Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

October 2020

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

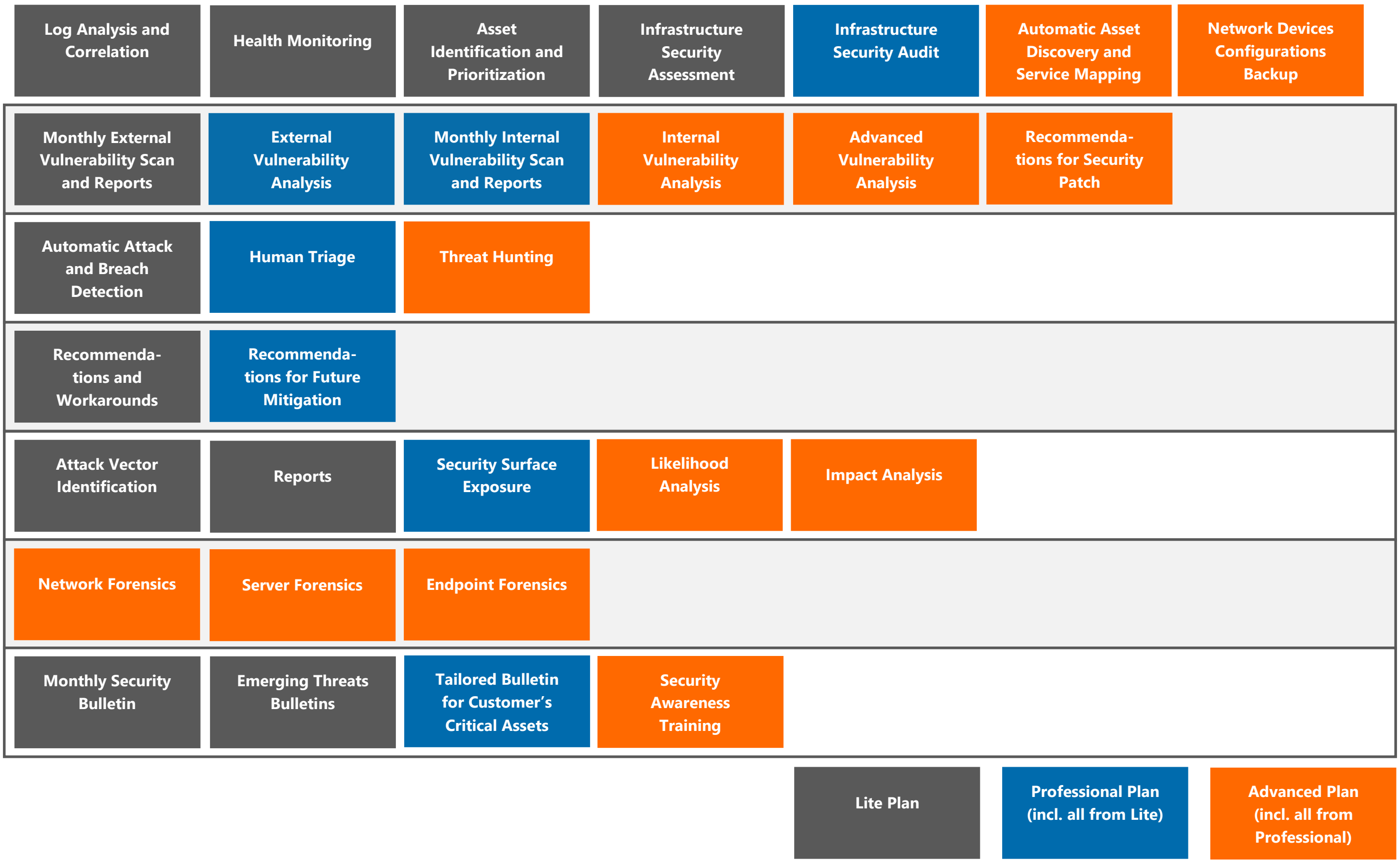
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!



Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Four Best Practices for Zero Trust for IoT

The Zero Trust security model is designed to encompass the expanding boundaries of an organization's network. Rooted in the principle of "never trust, always verify," it grants controlled access to authorized users and devices only on the basis of whether each can strictly authenticate their identity in order to be granted the privilege.

Above that, Zero Trust requires that user and device access privilege be continuously verified even after authentication. Privileged access to the organization's resources is limited to only those resources that the user and device absolutely need to perform their function. A user is not entitled to unrestricted access privileges, and the same goes for the device.

For these reasons, the identity awareness and application layer (Layer 7) control of every user and device becomes one of many critical factors in perpetuating the Zero Trust security model.

The Challenge Behind Implementing Zero Trust for IoT Devices

I've alluded to users and their IT devices in relation to Zero Trust. Now let's talk about IoT devices in a similar yet somewhat divergent context. When it comes to unmanaged IoT devices tethered to an organization's network, most enterprises find it difficult to adhere to standard Zero Trust principles. Why is this?

This is because, unlike users and their standard IT devices, IoT devices create a massive visibility challenge. As IoT picks up steam, for most enterprises undertaking IoT deployments, obtaining identity awareness of every such device connecting itself to the network is a problem. One of the main reasons for this is that most IoT devices don't support traditional enterprise authentication and authorization processes such as 802.1X or Single-Sign-On.

Approaches based on device fingerprinting don't work for IoT devices because of the sheer variety in operating protocols and standards. Besides, IoT devices are rarely assigned a unique hardware identifier (unlike IT devices) as a result of being manufactured in batches. Given this, most of these devices remain undiscovered and unaccounted for in an IT team's device inventory.

Since IoT devices are ultimately designed to connect to the wireless network, once connected, they roam and remain interspersed alongside IT devices, freely enjoying unfettered network access while remaining out of sight of vulnerability scans. As a result, these devices reduce risk levels to the lowest common denominator and greatly widen the threat surface, making the network gravely susceptible to lateral exploits.

Implementing Zero Trust for IoT Environments With Palo Alto Networks IoT Security

Palo Alto Networks IoT Security brings IoT devices into the fold of a Zero Trust security model by implementing four best practices that minimize IoT security risks and keep your network safe from cyber attacks. The cloud-delivered security service can be enabled on any of our Next Generation Firewalls for current customers, or delivered as a complete solution for non-Palo Alto Networks customers.

1. Our IoT Security makes enhanced visibility the foundation of your Zero Trust strategy for IoT security.

You can't secure what you can't see. To extend the principles of Zero Trust, it is important to first go beyond users and standard IT devices to include all unmanaged IoT devices in the network. Our agentless IoT security solution bypasses standard signature-based approaches to discover every connected IoT device in the network, including the never-seen-before ones that IT teams are unaware of.

Our IoT Security accurately matches each device's IP address with its type, vendor and model to surface a bundle of additional essential device attributes that completely profile the device. Accurate and granular device classification is a necessary prerequisite to differentiating unmanaged IoT devices from managed IT assets. Doing that enables enforcement of Zero Trust-driven security policies that only allow approved traffic in your IoT environment.

2. Our IoT Security continuously audits and validates devices against behavior anomalies and risk scores.

A core principle behind Zero Trust is that no devices – whether identified inside or outside the network – should be granted access to other devices and applications until assessed for risk and approved within the set parameters of normal behavior.

This principle applies perfectly to IoT devices since they have limited, stable and predictable behaviors by nature. Once identified, every IoT device should be verified against baselined behaviors before being granted access to other devices and applications in the network.

Our ML-based IoT Security automatically ascertains the device's identity and verifies "normal behaviors." Once "normal behaviors" are determined, the solution kicks in anomaly detection to uncover and prioritize any potential deviation from the baseline.

3. Our IoT Security microsegments IoT devices from IT devices to reduce the attack surface and risk radius of lateral exploits.

A Next-Generation Firewall enables microsegmentation of network perimeters and acts as border control within your organization. Our IoT Security takes a device profile-based microsegmentation approach that considers a number of factors (including device type, function, mission criticality and threat level) to enable sequestration. This significantly reduces the potential impact of cross-infection between IT and IoT devices. Seamlessly implemented on your Next-Generation Firewall, this approach restricts lateral movement between IT and IoT devices.

Partitioning away IoT devices ensures they have least-privileged access and connect to only required applications. It keeps them quarantined from guest and business networks, and minimizes operational downtime in critical IoT infrastructures by mitigating incompatibility issues cropping up between systems.

4. Our IoT Security automates Zero Trust policy enforcement using machine learning and Device-ID on the Next-Generation Firewall.

Zero Trust begins with "deny all." Zero Trust policies are then built and defined at Layer 7, based only on what is allowed. Next-Generation Firewalls utilize the concept of positive enablement, which makes Zero Trust-driven security policies easier to write.

Instead of manually translating normal versus suspicious device behavior into policies for enforcement, our IoT Security automatically generates and enforces Zero Trust policies using machine learning on your firewall. Our machine learning establishes a baseline of Layer 7 IoT device behaviors – for instance, application and network topology behaviors – discerning what is normal for a single device in order to make recommendations for device-level policies consistent with Zero Trust architecture.

The new Device-ID policy construct then tracks an individual device across your network, providing detailed information as context within the ML-Powered NGFW for any alert or incident that may occur – regardless of changes to the device's IP address or location. Policy rules and Layer 7 controls are automatically updated as the location and identified risks change.

Zero Trust Throughout Your Infrastructure

In the past, securing users, applications and devices identifiable inside the network perimeter was the obvious thing to do. The explosion of unmanaged IoT devices in enterprises with their ever-expanding network security perimeter sets a new paradigm. It is imperative for enterprises to now embrace a new approach to IoT security modeled steadfastly on Zero Trust best practices.

IoT security is one component of an enterprise Zero Trust strategy. Be sure to check out the rest of the blogs in our Zero Trust Throughout Your Infrastructure series. Or you can watch as Palo Alto Networks Founder and CTO Nir Zuk explains how it all fits together in this video.

To learn more on how you can put an IoT security lifecycle approach into action to secure your IoT investments, reference our buyer's guide on IoT Security or request a demo to see first hand how the solution delivers visibility and protection in the IoT security lifecycle.

This post is part of a series covering "Zero Trust Throughout Your Infrastructure."

The post 4 Best Practices for Zero Trust for IoT appeared first on Palo Alto Networks Blog.

Source: https://blog.paloaltonetworks.com/2020/09/zero-trust-for-iot/

2. Digital Education: The cyber-risks of the online classroom

This past spring, as the COVID-19 pandemic took hold, online learning became the new norm as universities and classrooms around the world were forced to close their doors. By April 29, 2020, more than 1.2 billion children across 186 countries were impacted by school closures.

Shortly after schools began to transition to emergency remote learning, it became clear that many were not ready for the kind of full-time, digital education now needed. Not all students had the technology that was required, from laptops to a stable Internet connection, and parents and instructors in countries like the United States worried students would inevitably fall behind academically. What is more, many educational institutions did not have proper cybersecurity measures in place, putting online classrooms at increased risks of cyberattacks.

In fact, in June, Microsoft Security Intelligence reported that the education industry accounted for 61 percent of the 7.7 million malware encounters experienced by enterprises in the previous 30 days – more than any other sector.

Apart from malware, educational institutions were also at increased risk of data breaches and violations of student privacy. It was this spring that "Zoombombing" became part of the general lexicon after pranksters and ill-intentioned individuals began taking advantage of Zoom's security weaknesses to break into private meetings. Among the victims were schools, with several reported incidents of online classrooms being interrupted by users making lewd comments or streaming pornography.

As fall approaches, digital learning will continue to be a necessity. In fact, half of all U.S. elementary and high school students will be entirely online. Even those that are reopening are deploying some kind of hybrid model, such as delivering large lectures online. What's more, the threat of a second coronavirus wave still remains, meaning that future large-scale school closures are still a possibility.

With this in mind, Kaspersky researchers took a closer look at the cyber risks faced by schools and universities, so that educators can be prepared moving forward – and take the necessary precautions to stay secure.

Methodology

This report examines several different types of threats – phishing pages and emails related to online learning platforms and video conferencing applications, threats disguised under the names of these same applications, and distributed denial of service (DDoS) attacks affecting the education industry.

Various threats disguised under popular online learning platforms/video conferencing applications

For this part, we utilized results from the Kaspersky Security Network (KSN) – a system for processing anonymous data related to cybersecurity threats shared voluntarily from Kaspersky users – for two different periods: January-June 2019 and January-June 2020.

Using KSN, we searched for files bundled with various threats that contained the name of one of the following platforms/applications during one of the two periods above:

– Moodle – the most popular learning management system (LMS) in the world. It is used by educators to build online courses, host classes and create activities.

– Blackboard – another popular LMS. It provides a virtual learning environment where educators can build entirely digital courses or create additional activities to supplement in-person instruction.

– Zoom – a highly popular online collaboration tool that provides free video conferencing capabilities. Many educators used Zoom to conduct online classes this past spring.

– Google Classroom – a web service designed specifically for educators to host classes, generate assignments and track students' progress.

– Coursera – a popular online learning platform that hosts a variety of open online courses, certificates and even degree programs.

– edX – a provider of open online courses available to users worldwide.

– Google Meet – a video communication service similar to Zoom, which can be used to host meetings and online classes

The results display those (PC and mobile) users that encountered various threats disguised as the above platforms/applications from January-June 2019 and January-June 2020.

Distributed denial of service (DDoS) attacks

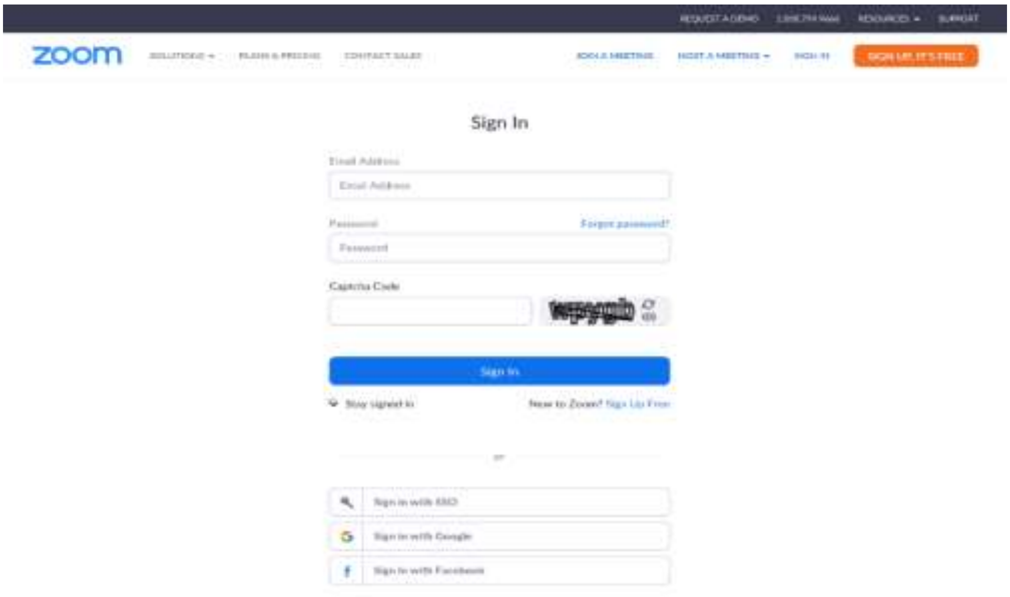
Kaspersky tracks DDoS (distributed denial of service) attacks using the Kaspersky DDoS Intelligence System. A part of Kaspersky DDoS Protection, the system intercepts and analyzes commands received by bots from C&C servers. The system is proactive, not reactive, meaning that it does not wait for the user device to get infected or a command to be executed. Each "unique target" represents a specific IP address that was attacked.

The following report displays the percentage of DDoS attacks that affected educational resources out of the total number of DDoS attacks registered by the Kaspersky DDoS Intelligence System for Q1 2019 and Q1 2020.

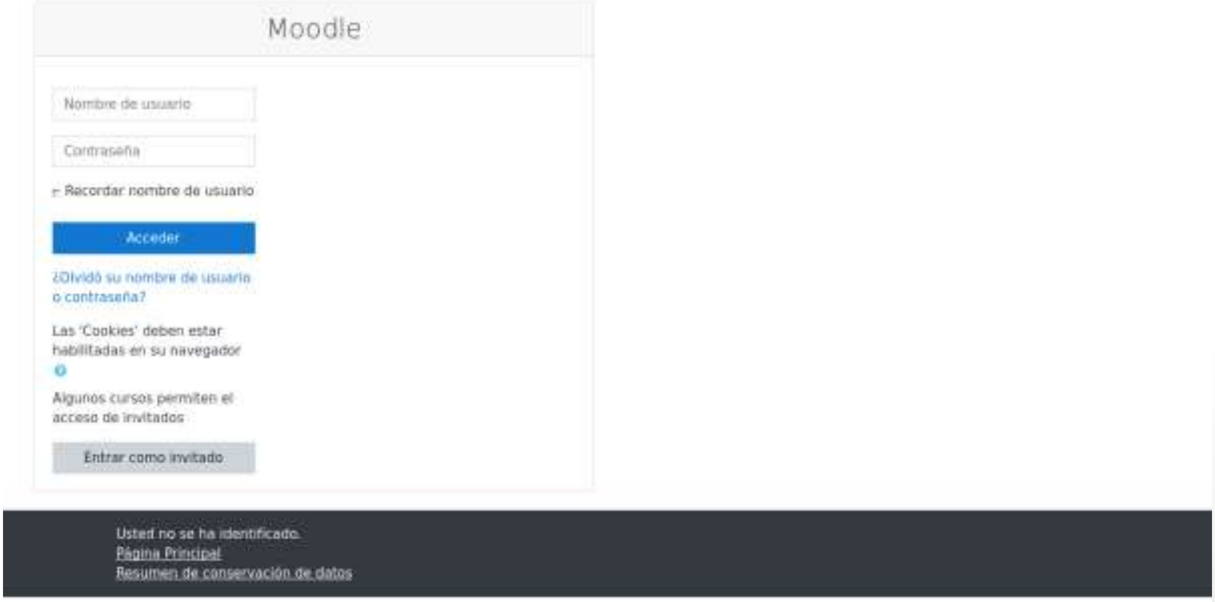
- Our Key Findings. The number of DDoS attacks affecting educational resources grew by **550%** in January 2020 when compared to January 2019.
- For each month from February to June, the number of DDoS attacks that affected educational resources out of the total number of attacks was **350-500%** greater in 2020 than in the corresponding month in 2019.
- From January to June 2020, the total number of unique users that encountered various threats distributed under the guise of popular online learning platforms/video conferencing applications was **168,550 – a 20,455% increase** when compared to the same period for 2019.
- From January to June 2020, the platform most commonly used as a lure was Zoom, with **5%** of the users that encountered various threats encountering them via files that contained the name Zoom. The second most common platform used as a lure was **Moodle**.
- By far the most common threats encountered in 2020 were downloaders and adware, which were encountered in 98.77% of the total registered infection attempts. Various classes of trojans followed adware.
- For threats distributed under the guise of popular platforms for conducting online classes in 2020, the highest infection rate was registered in Russia (**59 attempts per 1000 users)** followed by Germany (**39 infection attempts per 1000 users**).

Phishing risks of online learning platforms / video conferencing applications

It is not unexpected that phishing, one of the oldest and most popular forms of cybercrime, would reach educational organizations. In fact, a host of phishing websites for popular platforms like Google Classroom and Zoom began to pop up following the switch to distance learning. From the end of April to mid-June, Check Point Research discovered that 2,449 domains related to Zoom had been registered, 32 of which were malicious and 320 were "suspicious". Suspicious domains were also registered for Microsoft Teams and Google Meet. Users who land on these phishing pages are often tricked into clicking URLs that download malicious programs, or they might be tricked into inputting their login credentials, which would put these in the hands of the cybercriminals.



Fake login page for Zoom



¿Olvidó su nombre de usuario o contraseña?

Las 'Cookies' deben estar habilitadas en su navegador

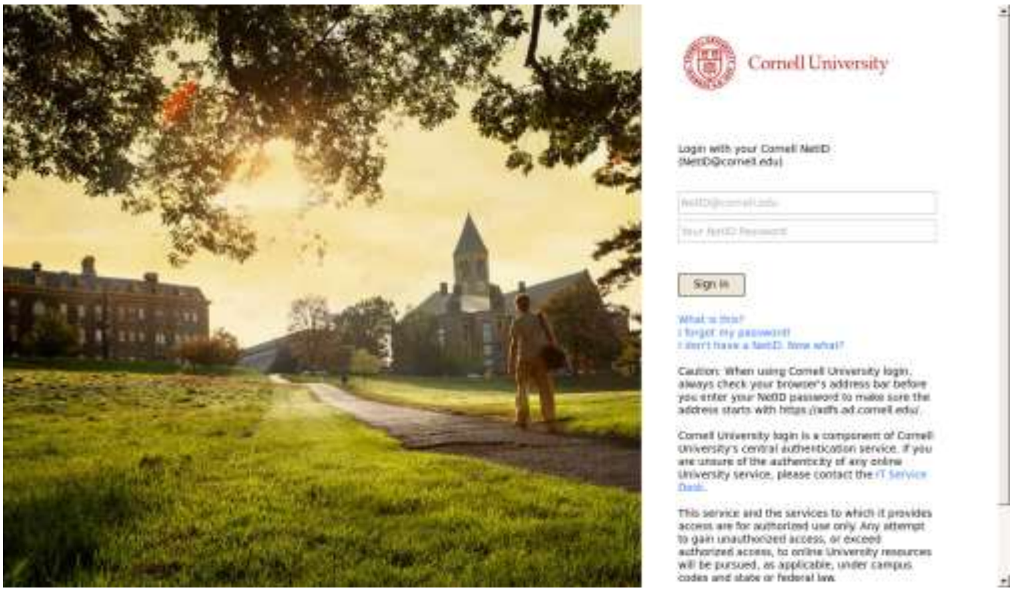
Algunos cursos permiten el acceso de invitados

Usted no se ha identificado.
Página Principal
Resumen de conservación de datos

Fake login page for Moodle

These criminals might not even be after access to your account. They can use your login credentials for various nefarious purposes: launching spam or phishing attacks, gaining access to your other accounts as people often reuse passwords, or collecting more personally identifiable information to be used in future attacks / attempts to steal funds.

Most universities also have their own platforms where students and faculty can login to access important resources and various academic services. This past spring, some attackers went so far as to target specific universities by creating phishing pages for their individual academic login pages.



Cornell University

Login with your Cornell NetID (NetID@cornell.edu)

NetID@cornell.edu

Your NetID Password

Sign in

What is this?
I forgot my password!
I don't have a NetID. Now what?

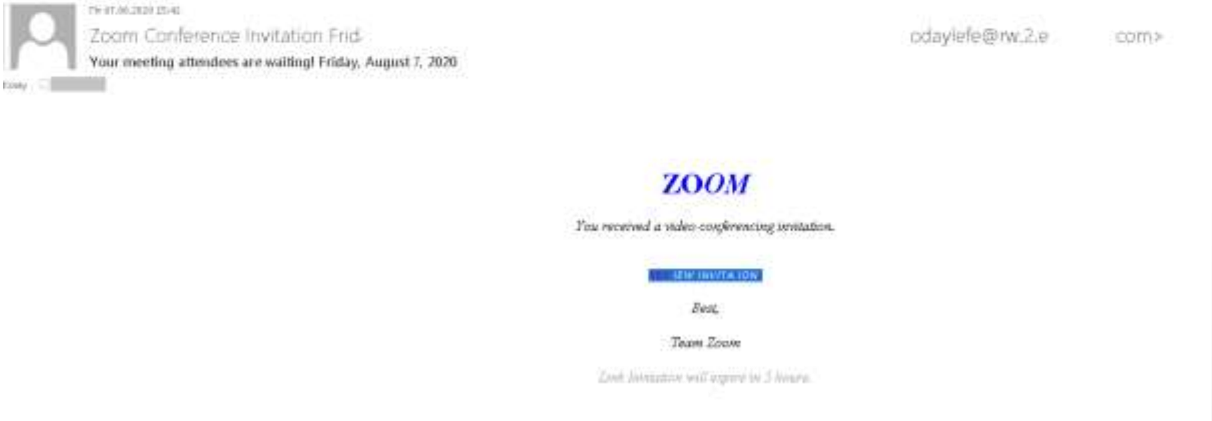
Caution: When using Cornell University login, always check your browser's address bar before you enter your NetID password to make sure the address starts with https://adfs.ad.cornell.edu/.

Cornell University login is a component of Cornell University's central authentication service. If you are unsure of the authenticity of any online University service, please contact the IT Service Desk.

This service and the services to which it provides access are for authorized use only. Any attempt to gain unauthorized access, or exceed authorized access, to online University resources will be pursued, as applicable, under campus codes and state or federal law.

Phishing page for Cornell University's academic login page

Apart from fake web pages, cybercriminals sent out an increasing number of phishing emails related to these same platforms. These told users they had missed a meeting, a class had been canceled, or it was time to activate their accounts. Of course, if they opened the email and clicked on any links, they were at risk of downloading various threats.



Fr 07.08.2020 15:40

Zoom Conference Invitation Frid

odaylefe@rw.2.e com>

Your meeting attendees are waiting! Friday, August 7, 2020

ZOOM

You received a video-conferencing invitation.

VIEW INVITATION

Best,

Team Zoom

Link Invitation will expire in 3 hours.

Phishing email supposedly from Zoom urging the user to review a new video conferencing invitation

The cyberthreats of online learning platforms

A common way to distribute threats disguised as popular video meeting apps and online course platforms is by bundling threats as legitimate application installers.

There are several ways users can encounter these malicious installers. One way is through phishing websites designed to look like the legitimate platforms, as seen above. Those users who inadvertently end up on the wrong page are then exposed to malware or adware when they attempt to download what they believe is the genuine application. Another common way is through phishing emails disguised as special offers or notifications from the platform. If users click the links in the email, then they are at risk of downloading unwanted files.

From January to June 2019, the number of unique users that encountered various threats distributed via the platforms specified in the methodology section of this report was **820**.

The number of unique users that encountered various threats disguised as popular online learning/video conferencing platforms, January – June 2019 (download)

The most popular lure was Moodle, with Blackboard and Zoom being the second most popular.

In 2020, however, the total number of users that encountered various threats disguised as popular online learning platforms jumped to **168,550, a 20,455% increase.**

The number of unique users that encountered various threats disguised as popular online learning/video conferencing platforms, January – June 2020 (download)

Zoom was far and away the platform most frequently used as a lure, with **99.5%** of users encountering various threats disguised under its name. This is not surprising given that Zoom became the go-to video conferencing platform. By February 2020, the platform had added more new users (2.22 million) than it had, in all of 2019 (1.99 million). As of April 30, the company claimed to have 300 million daily meeting participants. Given its immense popularity, it is only logical that it would be the preferred target for malicious actors. And, with millions of more users looking to download the application, the chances are high that at least some of these would come across fake installers or setup files.

A closer look at the 2020 threat landscape

Types of threats encountered

Percent distribution of different types of threats disguised as popular online learning / video conferencing platforms encountered by users, January – June 2020 (download)

By far the most common threats distributed under the guise of legitimate video conferencing/online learning platforms were not-a-virus **(99%).** Not-a-virus files are typically divided into two categories: riskware and adware. Adware bombards users with unwanted ads, while riskware consists of various files – from browser bars and download managers to remote administration tools – that may carry out various actions on your computer without your consent.

About **1%** of the infection attempts were various trojan families: malicious files that allow cybercriminals to do everything from deleting and blocking data to interrupting the performance of the computer. Some trojans encountered were password stealers, which are designed to steal your credentials, while others were droppers and downloaders, both of which can deliver further malicious programs on your device.

Other threats encountered were backdoors, which allow the attackers to take remote control over the device and perform any number of tasks; exploits, which take advantage of a vulnerability in an operating system or application to gain unauthorized access to/use of the latter; and DangerousObjects (non-specific malicious files).

A regional perspective

The five countries with the highest infection rate are as follows:

Russia	59 infection/1000 users
Germany	39 infection attempts/1000 users
Austria	27 infection attempts/1000 users
Isle of Man	13 infection attempts/1000 users
Switzerland	10 infection attempts/1000 users

came from Germany **(39 infection attempts/1000 users)**. Both countries closed schools early in mid-March, making remote learning the only option for millions of teachers and students. In addition, video conferencing has become incredibly popular in Germany, with more than half of Germans regularly using it as a tool for work or school. Given the overall global popularity of Zoom, a significant portion of Germans most likely use this platform and – given that Zoom is by far the most popular platform used as a lure – encountered various threats as a result.

Educational resources hit by DDoS attacks

In April, a large Turkish university was forced entirely offline for 40 minutes after it was hit with a DDoS attack on the morning of exams. In June, a major university in the northeastern United States had its exams disrupted after a DDoS attack affected its online test platforms. These are just two examples of a larger trend that began after schools were forced to transition to emergency remote learning: the rise of DDoS attacks against the education sector.

In general, the total number of DDoS attacks increased globally by 80% for Q1 2020 when compared to Q1 2019. And a large portion of that increase can be attributed to the growing number of attacks against distance e-learning services.

Percent of the total number of DDoS attacks that affected educational resources: Q1 2019 vs Q1 2020 (download)

When compared to Q1 2019, the percentage of DDoS attacks affecting educational resources out of all DDoS attacks increased steadily for each month of Q2 2020 (with the exception of March). When looking at the total number of DDoS attacks that occurred between January and June 2020, the number of DDoS attacks affecting educational resources increased by at least 350% when compared to the corresponding month in 2019.

January:	February:	March:	April:	May:	June:
550%	500%	350%	480%	357.14%	450%

The percent growth in the number of attacks on educational resources when compared to the same month in 2019

The more educational organizations rely on online resources to conduct their regular activities, the more of a target these networks become for cybercriminals looking to disrupt their operations.

Looking forward

Online learning is not a short-term response to a global pandemic. It is here to stay.

For one, the pandemic is not over. Many students are still studying virtually, at least part of the time, and some schools that decided to open have already decided to revert back to online classes only. The possibility of a second wave still looms, meaning educators have to be prepared for large-scale school closures in the future.

Even when the pandemic does end, most agree that online learning will not disappear altogether. A recent global survey by Pearson Education, an academic publishing company, found that nearly 90% of the 7,000 individuals surveyed expect online learning to continue to play a role at all education levels.

In fact, even before the pandemic, some universities had already developed blending curricula (a mix of offline experiences and online courses). More and more academic institutions are considering this as an option for future programs.

However, as long as online learning continues to grow in popularity, cybercriminals will attempt to exploit this fact for their own gain. That means educational organizations will continue to face a growing number of cyber risks – into this fall and beyond. Fortunately, engaging – and secure – online academic experiences are possible. Educational institutions just need to review their cybersecurity programs and adopt appropriate measures to better secure their online learning environments and resources.

The extended version of the report with security tips and additional materials from our partners: Ilya Zalessky, head of educational services at Yandex, Steven Furnell, professor of cyber security at the University of Nottingham, and Dr. Michael Littger, executive director of Deutschland sicher im Netz e.V, can be downloaded in PDF format.

Source: *https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/*

3. Ransomware Attacks: How to Protect your Data With Encryption

Cybercriminals are making headlines using ransomware to block organizations from accessing their own critical business data to extort ransoms.

Recently, the University of California San Francisco fell victim to a ransomware attack on key academic and research data (the institution is known to be working on a cure for COVID-19) and ended up paying over $1.14 million to gain back control of their data. It is unclear if the university had applied any data protection measures such as data encryption.

According to the 2020 Cost of a Data Breach report, ransomware attacks have grown more common and have a greater average cost of a breach than the overall average. This average comes out to nearly $4.44 million for a ransomware attack. These costs can be attributed to the monetary demands by the threat actor, but that's not the only problem. Other costs come from data recovery, systems downtime, reputational damage and so on.

No one solution available in the market today can completely protect against ransomware, but data encryption is key to any comprehensive data protection strategy. Data encryption software affords control over security policies that prevent malicious users and rogue processes from taking control of your sensitive data.

What is Ransomware?

A ransomware attack generally follows a known pattern. In one scenario, the threat actor does their homework by tracking down employee email addresses, which they use to orchestrate a phishing campaign that delivers ransomware via an email attachment.

An employee untrained to detect such schemes will open the email attachment, which is masquerading as something that looks trustworthy. Doing so opens the door to malware infecting their laptop and any known vulnerabilities. The ransomware goes on to take over sensitive files and databases by encrypting them. Only the threat actor will have the key to decrypt the data. To get the key, the victim has to pay the ransom.

It is imperative that employees be trained to recognize phishing. It only takes one person to make a mistake to allow ransomware to take hold of sensitive data. Organizations are also deploying additional measures such as securing email and web gateways, applying software patches to vulnerabilities and monitoring Domain Name System queries. However, these techniques are often ineffective against new and unknown strains of malware.

Application of Zero Trust security principles is a growing area of focus to embed technologies and processes that help mitigate ransomware attacks. As a failsafe, organizations should make sure to back up all critical business data, so that data restoration is possible without having to meet the demands of cybercriminals. Even with a backup, it’s possible the ransomware remains in the network, so any points of vulnerability will need to be fully addressed.

Consider Data Encryption to Block Ransomware

Organizations should consider a data protection solution with application whitelisting, access control and data encryption to effectively protect against ransomware. Application whitelisting is the process of specifying which software applications or executable files are allowed to run. This helps block malware from entering and executing within the network.

Access control is also key because it defines which users have access to which files or folders and what operations can be performed by the user on specific data. Oftentimes, malware attempts to gain privileges to access sensitive data. In the case of ransomware, once the threat actors have access to the system, they can encrypt sensitive data and hold it hostage until the ransom is paid. Fine-grained access control can prevent users from having more access than they should.

Data encryption protects data wherever it lives across the hybrid multicloud environment. Once data is encrypted and the encryption key is secured, the data becomes useless to any cybercriminal. If that data is already encrypted, that makes it much more difficult for the malware to detect it and attack.

A gold-standard data encryption solution will not only encrypt data across the technology stack, but will provide application whitelisting and fine-grained access control with consistent policy enforcement. By controlling access to trusted executables, limiting privileged access and obfuscating critical data, your organization will be much better positioned against ransomware attacks.

The post Ransomware Attacks: How to Protect your Data With Encryption appeared first on Security Intelligence.

Source: https://securityintelligence.com/posts/ransomware-attacks-how-to-protect-data-encryption/

4. SOC 2.0: A Guide to Building a Strong Security Ops Team

In a security operations center (SOC), your cybersecurity tools are only as good as the people using them and your SOC's culture. What are the critical SOC roles? What qualities should you look for when hiring for them? And, what should you expect from a cybersecurity career?

Learn more about why IBM was selected as a Global and European Leader in Managed Security Services.

Drawing from my experience working in IBM Security's Managed Security Services SOC, here are some insights on how SOCs around the world should staff and organize based on their needs.

Key Roles in a SOC

Making sure you have the right people in the right roles is crucial for the success of a modern-day SOC. The main roles found within a company's SOC depend on the program's maturity, company size and budget.

At IBM, I work with clients who have one or two security people who wear many hats within the organization. I also work with mature SOCs who have their own 24/7 operations and highly specific roles.

But, most of my clients are somewhere in the middle. They have full-time employees for some roles and supplement with service providers for others, such as to achieve 24/7 "eyes on glass" or for incident responders who can be kept "on retainer."

In general, roles are centered around key SOC functions: investigation and analysis, operations and maintenance, engineering and architecture, protection and defense, threat intelligence and oversight and governance.

Investigation and Analysis

These roles respond to a trigger, such as an alert or suspicious event. They can be separated based on technology, such as host, network-based or tiered-based on skill/scope, such as “Tier 1,” and “Tier 2.” They include:

- Security analyst
- Incident responder
- Incident manager

Operations and Maintenance

These roles are key to the day-to-day management of tools. Typical responsibilities include managing device health, troubleshooting, version management and policy management. They include:

- Device administrator (firewall, intrusion prevention system, endpoint agent, etc.)
- Security engineer

Engineering and Architecture

Architect and engineering roles are key to advancing and improving your security operations. They can be correlation engineers responsible for writing new use cases and collecting and operating new logs. This role can also be developers who write custom tools or integration architects who help to recommend and implement new tools. These roles include:

- Developer
- Security architect
- Security engineer

Protection and Defense

Roles in this category tend to be proactive in nature, helping to identify security gaps and improve security posture before a threat actor has the opportunity to exploit them. They include:

- Threat hunters
- Vulnerability manager
- Penetration tester

Threat Intelligence

Threat intelligence is a unique SOC function in some cases. In other cases, it is combined with other roles. Intel analysts are responsible for tracking the threat landscape, including actors and campaigns that may target the organization. In most cases, intelligence analysts work closely with engineers and architects to ensure the right detection tools are in place proactively.

- Threat intelligence analyst
- Threat research analyst

Oversight and Governance

These roles can include management positions to help drive strategy, manage security budgets and maintain compliance. They include:

- Compliance officer
- Security awareness and training professional
- SOC manager
- Chief information security officer

Changes to SOC Roles

The cybersecurity industry has evolved, and the roles needed within the SOC have changed. We're in the middle of a transition period where SOCs everywhere are seeking to move from a reactive, alert-driven approach to a proactive, "smart" approach — a step closer toward "SOC 2.0."

Alert fatigue is also a real driver among SOC employees. It contributes to chronic staffing and retention challenges, as well as hiring shortages. Time and time again, SOCs get stuck in a hire-train-replace cycle, constantly churning through analysts as they move on to bigger and better career options. It's a cycle that can't continue.

As a result, more and more companies are seeking to identify and automate routine tasks. SOAR (Security Orchestration, Automation and Response) platforms are becoming more popular, and many companies are introducing elements of machine learning for initial alert triage.

While automation takes over most of the previous "Level 1" analyst work, the remaining alerts will require in-depth analytical skills. This, in turn, leads to increasing specialization of roles within the SOC and drives demand for higher-value skills, introducing new opportunities for employee career growth and simultaneously contributing to overall SOC maturity.

Hiring for the SOC 2.0

As a hiring manager, I often look more for personality traits than skills, because skills can be taught. For example, when hiring analysts, I look for passionate and motivated individuals, who have an innate curiosity. This is more important to me than in-depth experience with a particular tool or platform, as it shows me that they will excel at analysis and investigations, regardless of the tool. I love tinkerers and experimenters — bonus points if they've set up a home lab for testing and playing with malware.

For more senior roles, I look for employees who have experience in and understand best-practice methodologies. If you want to be an intel analyst, for example, learn the intelligence lifecycle. Study industry frameworks, such as MITRE ATT&CK, so you can understand adversary tactics, techniques and procedures. Strive for highly technical certifications, such as the Offensive Security Certified Professional or GIAC Certified Incident Handler.

At the more senior levels, specialization is key. You should also be able to interact and effectively communicate with other stakeholders. Generally, the more senior the role, the more frequent is the customer interaction. Technical skill is a must, but team members must also be able to convey complex security information to clients in a way that makes sense and allows them to make the best decisions on how to use their limited resources to maximize their security posture.

Real-World Example: Maze Ransomware

Ultimately, the goal of any SOC is to detect, analyze and respond to security threats. Regardless of your role, everyone in an SOC has this key goal in mind at all times, so the environment must be highly collaborative.

This really starts to come to life when you look at recent threats our SOC has handled. One such example is the Maze ransomware. After responding to several engagements, our X-Force Incident Response Team started to learn about the ways the Maze actors exfiltrated data, deleted backups, encrypted files and held the exfiltrated data for ransom. The group would post some of the stolen data on their "Wall of Shame" to scare victims into paying.

As our incident response team saw more of this activity, our intelligence team learned more about the threat actors. They then passed their findings to our threat hunters, who started hunting proactively, and to our correlation engineers, who pushed out new detection tools, which then fed into our "eyes-on-glass" monitoring teams. It's the cyber threat circle of life.

The post SOC 2.0: A Guide to Building a Strong Security Ops Team appeared first on Security Intelligence.

Source: https://securityintelligence.com/posts/soc-2-cybersecurity-hiring

5. The Joys of Owning an 'OG' Email Account

When you own a short email address at a popular email provider, you are bound to get gobs of spam, and more than a few alerts about random people trying to seize control over the account. If your account name is short and desirable enough, this kind of activity can make the account less reliable for day-to-day communications because it tends to bury emails you do want to receive. But there is also a puzzling side to all this noise: Random people tend to use your account as if it were theirs, and often for some fairly sensitive services online.

About 16 years ago — back when you actually had to be invited by an existing Google Mail user in order to open a new Gmail account — I was able to get hold of a very short email address on the service that hadn't yet been reserved. Naming the address here would only invite more spam and account hijack attempts, but let's just say the account name has something to do with computer hacking.

Because it's a relatively short username, it is what's known as an "**OG**" or "**original gangster**" account. These account names tend to be highly prized among certain communities, who busy themselves with trying to hack them for personal use or resale. Hence, the constant account takeover requests.

What is endlessly fascinating is how many people think it's a good idea to sign up for important accounts online using my email address. Naturally, my account has been signed up involuntarily for nearly every dating and porn website there is. That is to be expected, I suppose.

But what still blows me away is the number of financial and other sensitive accounts I could access if I were of a devious mind. This particular email address has accounts that I never asked for at **H&R Block**, **Turbotax**, **TaxAct**, **iTunes**, **LastPass**, **Dashlane**,

MyPCBackup, and **Credit Karma**, to name just a few. I've lost count of the number of active bank, ISP and web hosting accounts I can tap into.

I'm perpetually amazed by how many other Gmail users and people on similarly-sized webmail providers have opted to pick my account as a backup address if they should ever lose access to their inbox. Almost certainly, these users just lazily picked my account name at random when asked for a backup email — apparently without fully realizing the potential ramifications of doing so. At last check, my account is listed as the backup for more than three dozen **Yahoo**, **Microsoft** and other Gmail accounts and their associated file-sharing services.

If for some reason I ever needed to order pet food or medications online, my phantom accounts at **Chewy**, **Coupaw** and **Petco** have me covered. If any of my **Weber** grill parts ever fail, I'm set for life on that front. The Weber emails I periodically receive remind me of a piece I wrote many years ago for *The Washington Post*, about companies sending email from [companynamehere]@donotreply.com, without considering that someone might own that domain. Someone did, and the results were often hilarious.

It's probably a good thing I'm not massively into computer games, because the online gaming (and gambling) profiles tied to my old Gmail account are innumerable.

For several years until recently, I was receiving the monthly statements intended for an older gentleman in India who had the bright idea of using my Gmail account to manage his substantial retirement holdings. Thankfully, after reaching out to him he finally removed my address from his profile, although he never responded to questions about how this might have happened.

On balance, I've learned it's better just not to ask. On multiple occasions, I'd spend a few minutes trying to figure out if the email addresses using my Gmail as a backup were created by real people or just spam bots of some sort. And then I'd send a polite note to those that fell into the former camp, explaining why this was a bad idea and ask what motivated them to do so.

Perhaps because my Gmail account name includes a hacking term, the few responses I've received have been less than cheerful. Despite my including detailed instructions on how to undo what she'd done, one woman in Florida screamed in an ALL CAPS reply that I was trying to phish her and that her husband was a police officer who would soon hunt me down. Alas, I still get notifications anytime she logs into her Yahoo account.

Probably for the same reason the Florida lady assumed I was a malicious hacker, my account constantly gets requests from random people who wish to hire me to hack into someone else's account. I never respond to those either, although I'll admit that sometimes when I'm procrastinating over something the temptation arises.

Losing access to your inbox can open you up to a cascading nightmare of other problems. Having a backup email address tied to your inbox is a good idea, but obviously only if you also control that backup address.

More importantly, make sure you're availing yourself of the most secure form of multi-factor authentication offered by the provider. These may range from authentication options like one-time codes sent via email, phone calls, SMS or mobile app, to more robust, true "2-factor authentication" or 2FA options (something you have and something you know), such as security keys or push-based 2FA such as Duo Security (an advertiser on this site and a service I have used for years).

Email, SMS and app-based one-time codes are considered less robust from a security perspective because they can be undermined by a variety of well-established attack scenarios, from SIM-swapping to mobile-based malware. So it makes sense to secure your accounts with the strongest form of MFA available. But please bear in mind that if the only added authentication options offered by a site you frequent are SMS and/or phone calls, this is still better than simply relying on a password to secure your account.

Maybe you've put off enabling multi-factor authentication for your important accounts, and if that describes you, please take a moment to visit twofactorauth.org and see whether you can harden your various accounts.

As I noted in June's story, Turn on MFA Before Crooks Do It For You, people who don't take advantage of these added safeguards may find it far more difficult to regain access when their account gets hacked, because increasingly thieves will enable multi-factor options and tie the account to a device they control.

Are you in possession of an OG email account? Feel free to sound off in the comments below about some of the more gonzo stuff that winds up in your inbox.

Source: https://krebsonsecurity.com/2020/09/the-joys-of-owning-an-og-email-account/

6. Fileless Malware Tops Critical Endpoint Threats for 1H 2020

When it comes to endpoint security, a handful of threats make up the bulk of the most serious attack tools and tactics.

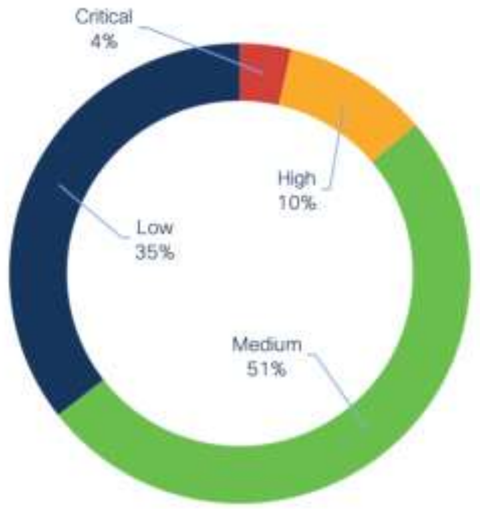
In the first half of 2020, the most common critical-severity cybersecurity threat to endpoints was fileless malware, according to a recent analysis of telemetry data from Cisco.

Fileless threats consist of malicious code that runs in memory after initial infection, instead of files being stored on the hard drive. Cisco flagged threats like Kovter, Poweliks, Divergent and LemonDuck as the most common fileless malware.

Another prevalent critical threat to endpoints in the first half was dual-use tools that are typically leveraged for both exploitation and post-exploitation tasks. Examples in circulation include PowerShell Empire, Cobalt Strike, Powersploit and Metasploit, according to Cisco.

“While these tools can very well be used for non-malicious activity, such as penetration testing, bad actors frequently utilize them,” wrote Ben Nahorney, researcher with Cisco, in a [blog posting]() on Monday.

Credential-dumping tools make up a third critical-severity threat category. The most commonly seen of these tools that malicious actors to scrape login credentials from a compromised computer in the first half of 2020 was Mimikatz, Cisco found.



Percentage of low, medium, high, and critical severity IoCs

IoC threats by severity level

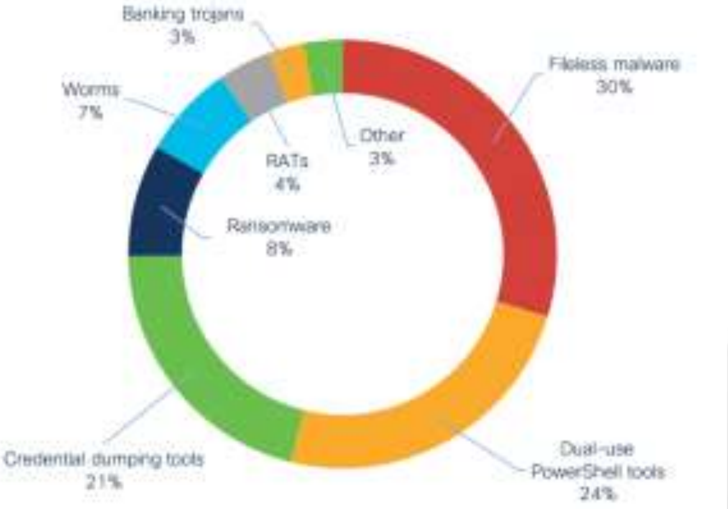
The activity appears to be extending into the rest of the year. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) said last week that threat actors have been spotted using the Cobalt Strike commercial penetration testing tool to target commercial and federal government networks; they have also seen the nation-states successfully deploying open-source tool Mimikatz to steal credentials.

These first three categories comprise 75 percent of the critical-severity indicators-of-compromise (IoC) seen in the analysis period; the remaining 25 percent is made up of a mix of different malwares, including ransomware (Ryuk, Maze, BitPaymer and others); worms (Ramnit and Qakbot); remote-access trojans (Corebot and Glupteba); banking trojans (Dridex, Dyre, Astaroth and Azorult); and various downloaders, wipers and rootkits.

Cisco also took a look at how threats were distributed across the MITRE ATT&CK framework of tactics.

Another way to look at the IoC data is by using the tactic categories laid out in the MITRE ATT&CK framework. Within Cisco's Endpoint Security solution, each IoC includes information about the MITRE ATT&CK tactics employed. These tactics can provide context on the objectives of different parts of an attack, such as moving laterally through a network or exfiltrating confidential information.

"Multiple tactics can…apply to a single IoC," the researcher explained. "For example, an IoC that covers a dual-use tool such as PowerShell Empire covers three tactics: Defense evasion (it can hide its activities from being detected); execution (it can run further modules to carry out malicious tasks); and credential access (it can load modules that steal credentials).



By far the most common tactic, defensive evasion appears in 57 percent of IoC alerts seen. Execution also appears frequently, at 41 percent, as bad actors often launch further malicious code during multi-stage attacks.

“For example, an attacker that has established persistence using a dual-use tool may follow up by downloading and executing a credential dumping tool or ransomware on the compromised computer,” Nahorney said, adding that execution is more common among critical severity IoCs than defense evasion.

Two tactics commonly used to gain a foothold, initial access and persistence, come in third and fourth, showing up 11 and 12 percent of the time, respectively. Persistence appears in 38 percent of critical IoCs, as opposed to 12 percent of IoCs overall.

And, communication through command-and-control rounds out the top five tactics, appearing in 10 percent of the IoCs seen.

“While these [critical issues] make up a small portion of the overall IoC alerts, they’re arguably the most destructive, requiring immediate attention if seen,” according to Nahorney. He added, “As you might expect, the vast majority of alerts fall into the low and medium categories, [and] there’s a wide variety of IoCs within these severities.”

Source: https://threatpost.com/fileless-malware-critical-ioc-threats-2020/159422/

7. 3 Biggest Factors in Data Breach Costs and How To Reduce Them

The cost of a data breach has increased slightly in the last six years on average. Costs are up 10% since 2014 to $3.86 million, according to the annual Cost of a Data Breach Report, published by IBM Security and based on research conducted by the Ponemon Institute.

Three areas in particular proved to have the biggest cost impact for organizations in the study. Take a look at steps organizations can take to mitigate data breach costs, from security automation and a well-trained incident response capability to securing cloud environments.

Behind the Numbers on Protecting Against a Data Breach

Specifically, the difference between costs for the least prepared organizations in the study and most prepared organizations — those with best practices for proactive, responsive security measures — has grown over the past few years.

The study, based on 524 recent global data breaches, found the average cost of a data breach went down slightly since 2019. This statistic hides a key connection. Organizations that had implemented an advanced security program faced significantly lower average data breach costs. Meanwhile, those without such programs struggled with much higher average costs.

In other words, the savings for investing in cybersecurity have increased.

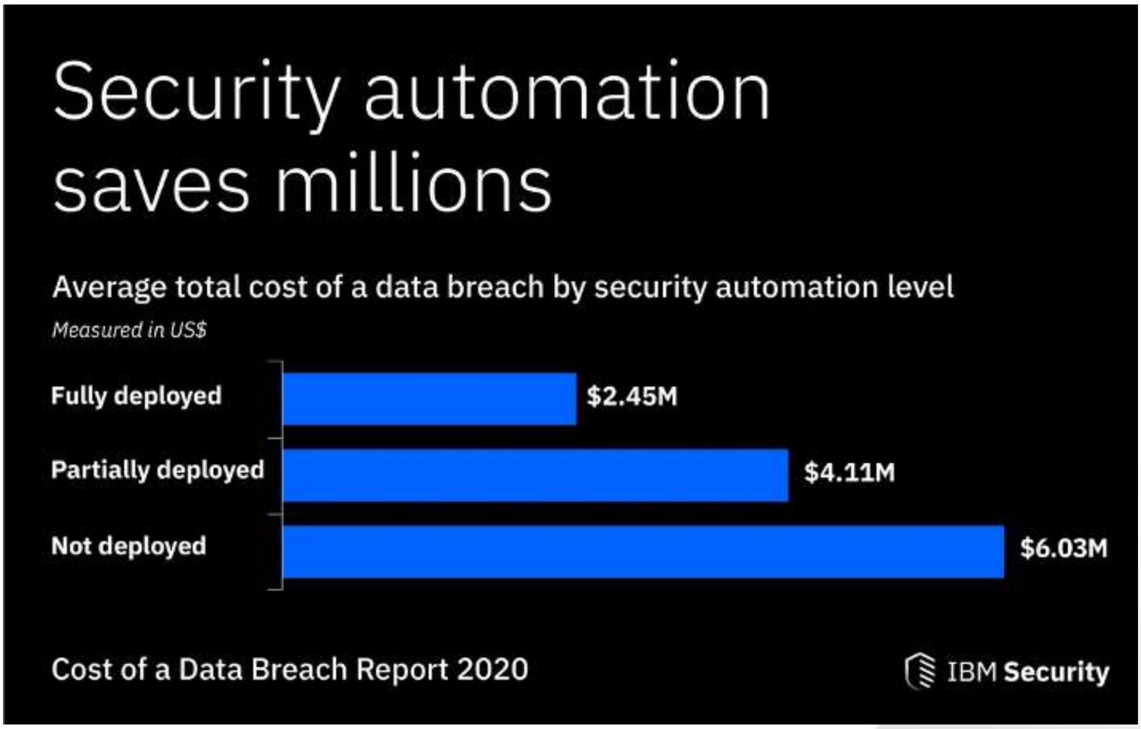
Here are three major factors that most affect the cost of a 2020 data breach.

Security Automation and Incident Response Work

First, the numbers in this year's report present compelling evidence that having effective, efficient security controls in place protecting against a data breach lower the cost of an attack.

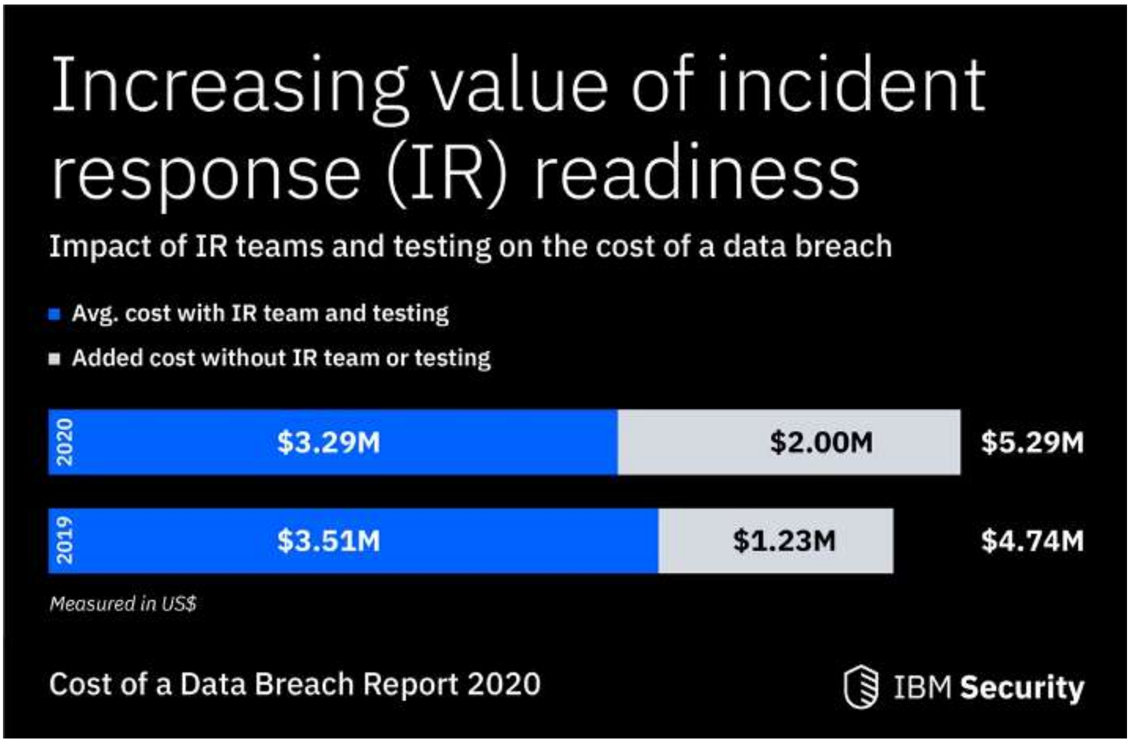
The report shows security automation has a massive impact on the average cost of a data breach. In this research, security automation means enabling security technologies that augment or replace what IT staff normally do. They include any security solution, such as SIEM tool, that uses artificial intelligence, machine learning, analytics and automated orchestration.

According to the report's findings, companies that did not deploy any form of security automation experienced much higher average breach costs and took much longer to identify and contain a breach than those with these technologies fully deployed. The average total cost of a data breach at organizations with fully deployed security automation was $2.45 million, compared with $6.03 million on average for organizations that had not deployed security automation — a difference of $3.58 million.



Incident response (IR) also remained a top cost saver, with trained and tested IR teams contributing to an average $2 million in data breach cost savings.

These benefits increased year over year. In the 2019 report, the cost difference between having no IR team or testing versus a trained and tested team was $1.23 million. The 2020 report's finding of a $2 million difference was a whopping 63% more than 2019.



Despite these findings, many organizations still don't have security automation fully deployed. Only one-fifth of organizations in the study had security automation fully deployed. But more and more companies are making the investment in automating their security. The number of organizations having fully deployed security automation increased from 16% in 2019 to 21% in 2020.

The percentage of companies with no security automation decreased from 48% in 2019 to 41% in 2020. Another 38% of organizations in the 2020 study said they had partially deployed security automation. This is an increase from 36% with security automation partially deployed in the 2019 study.

The vast majority of organizations can still take steps to deploy security automation in their organization. Speed up incident response time, and you might also reduce data breach costs.

Time is Still Money When it Comes to Data Breaches

Why are we seeing this increasing gap between lower cost and higher cost breaches? Time is a big factor. Data breach costs correlate to the amount of time it takes to identify and contain the breach (the data breach lifecycle). In 2020, a breach with a lifecycle of fewer than 200 days on average cost an organization only $3.21 million. But for a lifecycle greater than 200 days, the average cost jumps 30% to $4.33 million.

If longer breaches mean higher costs, it follows that speeding up the identification would lead to lower costs. Security automation, which was associated with much lower data breach costs on average, also sped up the detection and containment of breaches. Organizations with no security automation took more than two months longer to identify and contain a breach. (They took 308 days, compared with 234 days.)

Meanwhile, breach costs accrue over a long period of time. Losses from things like customer turnover and regulatory and legal fines can extend breach costs. Only 61% of breach costs occur in the first year on average. Therefore, organizations need to be ready to pay for data breaches for years, not months, after the event.

This changes for highly regulated organizations in industries such as finance and healthcare. In the 2020 study, those highly regulated organizations experienced 44% of costs in the first year and 21% of the cost more than two years later. In less regulated industries, 77% of breach costs accrued in the first year. These groups felt just 8% of costs more than two years after the breach.

Cloud-Based Expertise Pays Dividends

One other trend in this year's report shows that organizations need to be very aware of their cloud security. Cloud misconfigurations tied for the most frequent source of data breaches, accounting for 19% of the breaches caused by malicious attacks. In addition, organizations that suffered a data breach during a cloud transition had an average breach cost of $4.13 million, or $267,000 higher data breach costs on average.

Cloud environments provide organizations with a myriad of security benefits and can help reduce security system complexity. This, in turn, may speed up response times to incidents. Migrating to the cloud is an absolute win for many organizations, but this study also tells us that companies need to do cloud migration right. Using managed security services was one of the factors that can mitigate the average cost of a data breach.

Discover More in the Cost of a Data Breach Report

The Cost of a Data Breach Report can help you decide where to efficiently allocate your security spend to minimize the costs of a data breach. Register for the report to use interactive tools, explore the data and access key findings and recommendations.

The post 3 Biggest Factors in Data Breach Costs and How To Reduce Them appeared first on Security Intelligence.

Source: https://securityintelligence.com/posts/data-breach-three-biggest-factors-in-cost/

8. Universal Health Services Ransomware Attack Impacts Hospitals Nationwide

A ransomware attack has shut down Universal Health Services, a Fortune-500 owner of a nationwide network of hospitals.

The attack occurred in the wee hours of the morning on Monday, according to reports coming in from employees on Reddit and other platforms.

On Reddit, a discussion with hundreds of comments indicated that many UHS locations were indeed down and requiring a return to manual processes.

“It was an epic cluster working ‘old school’ last night with everything on paper downtime forms,” one posted said. “It is true about sending patients away (called EMS diversion) but our lab is functional along with landlines. We have no access to anything computer based including old labs, EKGs or radiology studies. We have no access to our PACS radiology system.”

Another wrote, “UHS psych Georgia we’re definitely down. We are having to handwrite everything! We’re not allowed to turn computers on either.”

Meanwhile, one person told TechCrunch that “Everyone was told to turn off all the computers and not to turn them on again,” the person said. “We were told it will be days before the computers are up again.”

In an official statement given out on Monday, UHS noted: “The IT Network across Universal Health Services (UHS) facilities is currently offline, due to an IT security issue. We implement extensive IT security protocols and are working diligently with our IT security partners to restore IT operations as quickly as possible. In the meantime, our facilities are using their established back-up processes including offline documentation methods. Patient care continues to be delivered safely and effectively.”

It added, “No patient or employee data appears to have been accessed, copied or otherwise compromised.”

While UHS didn’t mention what kind of attack it suffered, other information coming from workers seems to point to the Ryuk ransomware as the culprit. An employee told BleepingComputer for instance that encrypted files are being appended with the .RYK extension; and, a ransom note that showed up on all affected computers referenced the phrase “Shadow of the Universe,” which is known to be included in Ryuk ransom notes.

Threatpost reached out to UHS for further comment.

Some on Reddit floated the specter of patients dying because of a lack of care, with an original poster stating (without evidence) that “four people died” as a result of the attack, because patient care was delayed.

“One of the busiest hospitals in the region is currently sending away all ambulances to different smaller hospitals because of this, and they themselves are losing patients while they are waiting for lab results to be delivered by courier….four people died tonight alone due to the waiting on results from the lab to see what was going on,” the post reads.

This is a similar situation to an incident this month at a Dusseldorf University hospital, where a ransomware attack resulted in emergency room diversions to other hospitals. According to a report by the NRW Minister of Justice, a patient died who had to be taken to a more distant hospital in Wuppertal because of the attack on the clinic’s servers. An investigation has been opened.

Some employees said they wouldn’t be surprised if patient care were impacted, despite the hospital system’s assurances.

“No patients died tonight in our ED but I can surely see how this could happen in large centers due to delay in patient care,” one poster said.

Another wrote, “I work at a UHS facility in Tucson and our sh*t is definitely down. They won’t even let us turn the computers on for going on over 24 hours. We’re a psych hospital so no one is dying from not getting their lab results back in time, but if the same thing happening to us is going on at any of UHS’s medical facilities then I can well imagine people dying.”

Again, there’s no confirmation that patient safety was compromised, let alone deaths, but the news does come as ransomware continues to explode. A report out from IBM X-Force found that this month, one in four observed attacks have been caused by ransomware.

“It is sad to see that despite hackers’ claims to stop healthcare cyber-attacks during COVID-19 crisis, such attacks still take place,” said Ilia Sotnikov, vice president of product management, Netwrix. “Ransomware attacks are especially disastrous for healthcare as they block access to IT systems and patient data in hospitals, leading to inability to treat people, and might eventually cost lives. Yet, the recent Netwrix 2020 Cyber Threats Report has found that every third healthcare organization experienced a ransomware attack during the past few months, which is the highest result among all the verticals. Reason for such high rates is easy: healthcare sector is an easy target for hackers, giving the shortage of resources, legacy systems and the pressure that the sector faces in the current situation.”

Source: https://threatpost.com/universal-health-ransomware-hospitals-nationwide/159604/

9. Cybersecurity Awareness Month Helps Us All be #BeCyberSmart

Cybersecurity Awareness Month Helps Us All be #BeCyberSmart

October is Cybersecurity Awareness Month, which is led by the National Cyber Security Alliance (NCSA)—a national non-profit focused on cybersecurity education & awareness in conjunction with the U.S. government's Cybersecurity and Infrastructure Security Agency (CISA). McAfee is pleased to announce that we're a proud participant.

Cybersecurity Awareness Month

If there's ever a year to observe Cybersecurity Awareness Month, this is it.

As millions worked, schooled, and simply entertained themselves at home (and continue to do so) this year, internet usage increased by up to 70%. Not surprisingly, cybercriminals followed. Looking at our threat dashboard statistics for the year so far, you'll see:

- 113,000+ new malicious websites and URLS referencing COVID-19
- 5+ Million threats that exploit COVID-19
- A large spike in trojan-based attacks in April followed by a higher spike in July and August

And that doesn’t account for the millions of other online scams, ransomware, malicious sites, and malware out there in general—of which COVID-19-themed attacks are just a small percentage.

With such a high reliance on the internet right now, 2020 is an excellent year to observe Cybersecurity Awareness Month, along with its focus on what we can do collectively to stay safer together in light of today’s threats.

#BeCyberSmart

Unified under the hashtag *#BeCyberSmart*, Cybersecurity Awareness Month calls on individuals and organizations alike to take charge of protecting their slice of cyberspace. The aim, above making ourselves safer, is to make everyone safer by having us do our part to make the internet safer for all. In the words of the organizers, “If everyone does their part – implementing stronger security practices, raising community awareness, educating vulnerable audiences or training employees, our interconnected world will be safer and more resilient for everyone.”

Throughout October, we’re participating as well. Here in our blogs and across our broad and ongoing efforts to boost everyone’s awareness and expertise in cybersecurity and simply staying safe online, we’ll be supporting one key theme each week:

Week of October 5: If You Connect It, Protect It

If you’ve kept up with our blogs, this is a theme you’ll know well. The idea behind “If you connect it, protect it” is that the line between our lives online and offline gets blurrier every day. For starters, the average person worldwide spends nearly 7 hours a day online thanks in large part to mobile devices and the time we spend actively connected on our computers. However, we’re also connecting our homes with Internet of Things (IoT) devices—all for an average of 10 connected devices in our homes in the U.S. So even when we don’t have a device in our hand, we’re still connected.

With this increasing number of connections comes an increasing number of opportunities—and challenges. During this weel, we’ll take a look at how internet-connected devices have impacted our lives and how you can take steps that reduce your risk.

Week of October 12 (Week 2): Securing Devices at Home and Work

As we shared at the open of this article, this year saw a major disruption in the way we work, learn, and socialize online. There’s no question that our reliance on the internet, a safe internet, is greater than before. And that calls for a fresh look at the way people and businesses look at security.

This week of Cybersecurity Awareness Month will focus on steps users and organizations can take to protect internet connected devices for both personal and professional use, all in light of a whole new set of potential vulnerabilities that are taking root.

Week of October 19 (Week 3): Securing Internet-Connected Devices in Healthcare

Earlier this year, one of our articles on telemedicine reported that 39% of North Americans and Europeans consulted a doctor or health care provider online for the first time in 2020. stand as just one example of the many ways that the healthcare industry has embraced connected care. Another noteworthy example comes in the form of internet-connected medical devices, which are found inside care facilities and even worn by patients as they go about their day.

As this trend in medicine has introduced numerous benefits, such as digital health records, patient wellness apps, and more timely care, it's also exposed the industry to vulnerabilities that cyber criminals regularly attempt to exploit. Here we'll explore this topic and share what steps both can take do their part and #BeCyberSmart.

Week of October 26 (Week 4): The Future of Connected Devices

The growing trend of homeowners and businesses alike connecting all manner of things across the Internet of Things (IoT) continues. In our homes, we have smart assistants, smart security systems, smart door locks, and numerous other home IoT devices that all need to be protected. Businesses manage their fleets, optimize their supply chain, and run their HVAC systems with IoT devices, which also beg protection too as hackers employ new avenues of attack, such as GPS spoofing. And these are just a fraction of the applications that we can mention as the world races toward a predicted *50 billion* IoT devices by 2030.

As part of Cybersecurity Awareness Month, we'll look at the future of connected devices and how both people and businesses can protect themselves, their operations, and others.

Give yourself a security checkup

As Cybersecurity Awareness Month ramps up, it presents an opportunity for each of us to take a look at our habits and to get a refresher on things we can do right now to keep ourselves, and our internet, a safer place. This brief list should give you a great start, along with a catalog of articles on identity theft, family safety, mobile & IoT security, and our regularly updated consumer threat notices.

Use strong, unique passwords

Given the dozens of accounts you need to protect—from your social media accounts to your financial accounts—coming up with strong passwords can take both time and effort. Rather than keeping them on scraps of paper or in a notebook (and absolutely not on an unprotected file on your computer), consider using a password manager. It acts as a database for all your passwords and stores new codes as you create them. With just a single password, you can access all the tools your password manager offers.

Beware of messages from unknown users

Phishing scams like these are an old standard. If you receive an email or text from an unknown person or party that asks you to download software, share personal information, or take some kind of action, don't click on anything. This will steer you clear of any scams or malicious content.

However, more sophisticated phishing attacks can look like they're actually coming from a legitimate organization. Instead of clicking on a link within the email or text, it's best to go straight to the organization's website or contact customer service. Also, you can hover over the link and get a link preview. If the URL looks suspicious, delete the message and move on.

Use a VPN and a comprehensive security solution

Avoid hackers infiltrating your network by using a VPN, which allows you to send and receive data while encrypting – or scrambling – your information so others can't read it. By helping to protect your network, VPNs also prevent hackers from accessing other devices (work or personal) connected to your Wi-Fi.

In addition, use a robust security software like McAfee® Total Protection, which helps to defend your entire family from the latest threats and malware while providing safe web browsing.

Check your credit

At a time where data breaches occur and our identity is at risk of being stolen, checking your credit is a habit to get into. Aside from checking your existing accounts for false charges, checking your credit can spot if a fraudulent account has been opened in your name.

It's a relatively straightforward process. In the U.S., the Fair Credit Reporting Act (FCRA) requires credit reporting agencies to provide you with a free credit check at least once every 12 months. Get your free credit report here from the U.S. Federal Trade Commission (FTC). Other nations provide similar services, such as the free credit reports for UK customers.

Be aware of the latest threats

To track malicious pandemic-related campaigns, McAfee Advanced Programs Group (APG) has published a COVID-19 Threat Dashboard, which includes top threats leveraging the pandemic, most targeted verticals and countries, and most utilized threat types and volume over time. The dashboard is updated daily at 4pm ET.

Stay Updated

To stay updated on all things McAfee and for more resources on staying secure from home, follow @McAfee_Home on Twitter, listen to our podcast *Hackable?*, and 'Like' us on Facebook.

Source: https://www.mcafee.com/blogs/consumer/cybersecurity-awareness-month-helps-us-all-be-becybersmart/

10. Cybersecurity Risk Management: Protecting Our Most Valuable Currency

Cybersecurity risk management can be a unifying conversation throughout your organization. Few things are more challenging in the cybersecurity business than getting stakeholders to speak in the same language. The business planners are talking supply and demand; the IT department is talking bits and bytes; the HR department is talking wellness and productivity; the C-suite is talking dollars and cents; and the board of directors are talking governance and liability. All these competing challenges make discussions about endpoint solutions, monitoring systems and identity management systems difficult to have.

So how does one overcome the challenge? The answer comes in finding a common interest. And that common interest requires having a common language.

The History of Currency

The concept of currency goes back a while. Ancient China, the Mesopotamians and the Lydians, a group from western Anatolia who are likely the first to have used metal coins for exchange, all understood this concept well.

Medieval Europe gave rise to the merchant banks and letters of credit, where you could make a deposit in one place and use a letter of credit to make a withdrawal in another. Letters of credit provided an early form of security to those traveling between Europe and the Middle East. Because they did not need to carry their money, they were less likely to become targets for robbers.

You can bet your C-suite understands the concept of currency when they're deciding the next IT and cybersecurity budgets. In order to talk about how cybersecurity risk management fits into that budget, you need to speak the language of money. So who and what provides security for your data while it is deposited away somewhere or traveling along a network?

The 'War for Data'

Many wars are rooted in the desire to control more resources. You can make a strong argument that the most valuable resource in the 21st century is, in fact, data.

Why is it so valuable? Raw data, on its own, does have intrinsic value, just like many natural resources. But what makes data truly valuable nowadays is what you can do with it: collate it, interpret it, manipulate it, refine it, commercialize it and even abuse it.

Here's what makes information so unique: it gives you the ability to control what happens in the present and the future. That's why data, despite how readily available it is, should be treated as today's most valuable currency and not a commodity. That's why cybersecurity risk management is so important.

Turning Cybersecurity Risk Management Into a Shared Interest

The path to getting your cybersecurity risk management concerns addressed may all come down to communication and understanding. When you can translate your security and privacy concerns into wellness and productivity concerns, you're making progress. And if you can up your game by translating artificial intelligence monitoring and infrastructure design into governance and liability issues, then you're really on the road. This is how you make cybersecurity champions of your colleagues, because you are teaching them .

The way to do this is framing: making your colleagues understand that your data isn't just a bunch of information, but rather cold, hard cash.

Make Your Message Relatable

If your message is about artifacts and logs, you better be talking to your colleagues in the security and IT department. If you're not, you're likely to get a bunch of glossy looks, weird expressions, the ever so polite "mmhmm" or some mixture of them all. This may be a painful thing to hear, but non-security folks usually have about as much interest in cybersecurity as security folks have in non-security matters.

What bridges that gap?

People understand money. They can relate. That's where your discussion needs to start if you are trying to build allies within your organization. Trying to sell a risk management framework or a cybersecurity risk management assessment is hard on the best of days. Trying to sell that same framework and assessment through a business case or through what the calculable cost of attack would be makes it a whole lot easier.

If security professionals really want to make a change, they need to up their business acumen. Security professionals need to feel comfortable speaking about issues like reputational risk, stock value impact, financial risk, cost of business interruption, disclosure and regulatory penalties and liability payments.

If you *really* want to get attention, attach metrics to your discussion of cybersecurity risk management.

Back Your Discussion Up With Numbers

What do you think would happen if a chief financial officer walks into the boardroom and says “Someone has stolen millions of dollars from us”?

Jaws would drop. People would gasp and demand to know how something like this happened.

But would you get the same reaction if the chief information security officer walks into the boardroom and says, “There has been a theft: one of our main databases has been compromised”?

Would the “wow factor” be the same? Probably not.

This supports that data and metrics are key. If you’re not sure what metrics to use, a good place to start is the Ponemon Institute’s Cost of a Data Breach Report, published by IBM Security.

You can use the same or similar categories to make presentations to your colleagues.

Why You Should Treat Your Data Like Cash

The moment you really believe data is cold hard cash, you treat it differently. Cryptocurrency is a good example of this. Think about it: a cryptocurrency is just a bunch of 0s and 1s. Because those 0s and 1s are convertible into monetary value, those who own cryptocurrencies take great lengths to keep them secure.

Your intellectual property is also cash. Databases of personal information are cash. And your habits, all recorded in 0s and 1s, are cash.

Why? Because people can collate, interpret, manipulate, refine, commercialize and abuse data.

There is another major benefit of treating your data like cash: you can invest and secure it wisely. Finding solid numbers on the issue of cybersecurity risk management versus cybersecurity response costs are hard to come by, but you can tailor your solution to your need. You do this through risk management. This is where some good ol' fashioned math comes into play.

How To Talk About Cybersecurity Risk Management

Once you determine your risk tolerances, start crunching the numbers. The moment you have those calculations and metrics, you're armed with some serious statistics that can help back your case.

For example, you can walk into the boardroom and say, "These cybersecurity risk management measures will cost $100,000 per year. However, they will help us close a gap in our infrastructure that, if left unaddressed, could cost us millions of dollars if we are breached. The recovery costs will be bad, but the impact of such a breach will put our business operations in jeopardy due to regulatory penalties, reputational risk and loss of intellectual property. I value all of these costs to total upwards of $50 million dollars."

Show executives how valuable data is. For example, "We can afford $100,000 per year because our profit margins are x. Our balance sheet is in pretty good shape, so we can add some assets and depreciate them. The y amounts of costs are manageable year-over-year based on our current revenue stream."

If you have the data to back up a statement like that and you may find yourself with a few new cybersecurity risk management champions.

The post Cybersecurity Risk Management: Protecting Our Most Valuable Currency appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/risk-management-building-fort-around-worlds-most-valuable-currency/

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.sales@tbs.tech**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.