telelink
BUSINESS SERVICES

Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

July 2021

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

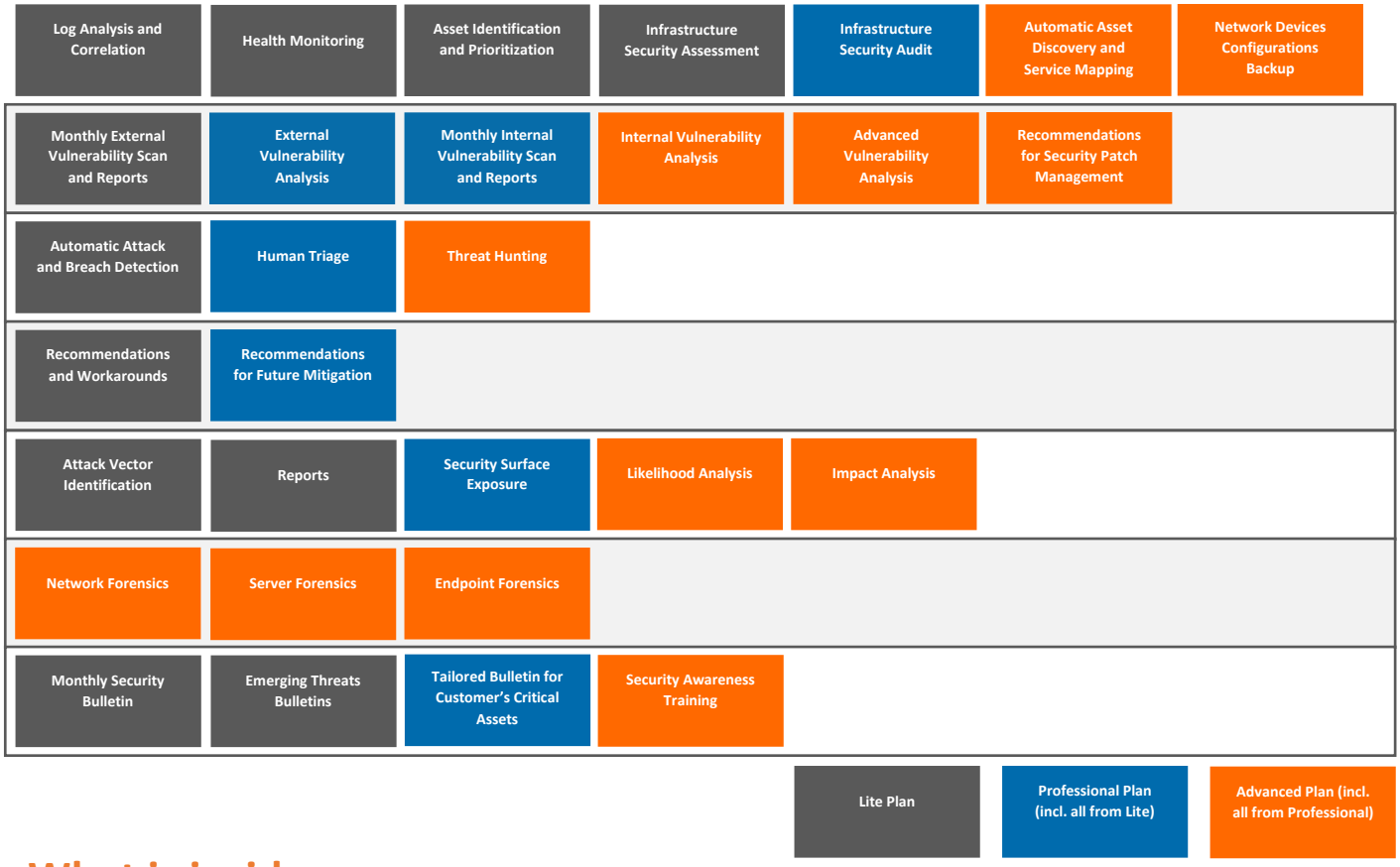
Start to mitigate cyber threats and minimize the risk!

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!



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. Cyber Extortion: What You Need to Know in 2021

Over the years, the term ransomware has taken on a new meaning for many businesses and local governments. This used to be considered a relatively new and emerging form of malware. Now, attackers have transformed it into a sophisticated and aggressive form of cyber extortion. Businesses feel the impact of ransomware globally. Their leaders need to be ready for how this cybercrime will surely advance in the next year.

Read on to discover different types of ransomware and how ransomware has evolved over the years. In addition, learn the common risk factors and how you can implement best practices.

Examples of a Ransomware Attack

Ransomware first came onto the scene in the late 1980s. It made waves as a disruptive, yet crude virus designed to corrupt computer data files to blackmail users. Since technology was more limited in those days, opportunities for ransomware to infect and spread were limited. However, cybercrime and the tools used to support it have advanced a lot over the years.

Below are just some examples of types of ransomware that have caused major damages to various businesses and government entities.

Ryuk Ransomware

Ryuk is a form of crypto-ransomware that infects systems and encrypts data belonging to organizations with little to no tolerance for downtime. Once run, Ryuk attempts to cease all antivirus and anti-malware related processes and disables system restore options.

Purelocker Ransomware

Purelocker is a ransomware-as-a-service (RaaS) attackers use against production servers of enterprises. This type of cyber extortion is sold and distributed on the dark web and uses Authenticated Lightweight Encryption (ALE) and Rivest–Shamir–Adleman (RSA) algorithms to encrypt user files.

Zeppelin

Zeppelin is a variant of Buran ransomware and was discovered in late 2019. Usually, victims download it through Microsoft Word attachments coded with malicious macros in phishing emails. The malware then encrypts web browsers, system boot files, user files and operating systems.

WannaCry

WannaCry ransomware has been available for several years now. Despite this, it is still one of the most well-known and financially devastating forms of malware. Security professionals consider this form of attack a ransomware worm that spreads rapidly across computer networks, infecting core system processes and encrypting data files. It impacted more than 200,000 computers across 150 countries in 2017.

Understanding Common Cyber Extortion Risk Factors

As entities continue to adapt their networks, supporting higher levels of growth potential and remote working arrangements for their employees, there are many risks to consider when defending against cyber extortion. Here are some of the common risk factors entities face in 2021.

Utilizing Legacy Systems Can Invite New Ransomware

Many entities still rely on outdated and unsupported systems to manage certain aspects of their business. However, since these systems no longer receive critical patches from their developers, malicious attackers can deploy wide open back doors for cyber extortion attackers to access and manipulate company data.

Lack of User Access Control

Since the COVID-19 pandemic started, more businesses worldwide have moved to remote workforces than ever before. While some entities have certainly seen benefits from reduced overhead expenses during this transition, this change can also be dangerous. As more remote employees access cloud-based business services and connect to business networks, a lack of secure access control protocols can lead to various risks, including ransomware attacks.

No Incident Response Plan for New Ransomware

Ransomware attacks almost always occur when victims least expect them. However, most of the damage occurs during the following days of an attack when business services are down for an extended period. Without an incident response plan, you may be left with an inevitable choice to pay a hefty ransom or completely rebuild your business systems from scratch. Both options can impact an entity severely. In fact, the U.S. Treasury now warns that companies may be punished for paying out the ransomware demands.

Keeping Your Business Safe from Cyber Extortion

For anyone who has asked themselves "Am I vulnerable to ransomware?" the answer is almost surely, "Yes." While most businesses invest in some form of a cybersecurity program, they deploy it without taking a more in-depth look at their digital attack surface.

Ransomware risk assessments are an essential aspect of ensuring your business is prepared to combat the latest threats. Using a mix of thorough database and network analysis, phishing resistance tests and client and server evaluations, risk assessments can identify the critical gaps in your security while providing you with a roadmap for security improvement.

While taking proactive steps with employees and systems to prevent a ransomware attack is important, entities should still prepare for the possibility of falling victim to an attack. By doing so, they can ensure they have adequate threat repair systems in place while also having effective incident response systems to recover from any attacks that occur quickly.

Checklist for Cyber Extortion Readiness

Some useful strategies businesses can deploy now to minimize their ransomware attack surfaces are:

- Adopt newer systems that support modern patches and updates.
- Segment network access to distinct users and validate credentials.
- Train employees on best security practices whether working on-premise or remotely.
- Back up your business data often using third-party solutions and services.
- Change passwords across all networks and devices often.
- Utilize active threat monitoring solutions to recognize ransomware signatures before they deploy in your systems.
- Use penetration testing methods through ethical hacking groups to discover hidden vulnerabilities that antivirus and anti-malware platforms may have missed.
- Develop an extensive incident response plan.

Ransomware is quickly evolving and has become one of the most common forms of digital attack today. To ensure your business is protected from cyber extortion now and in the future, it's essential for your organization to evolve its systems and process along with it. By conducting thorough ransomware risk assessments and building a path for network and security system hardening, you can ensure your business stays protected in 2021 and beyond.

The post Cyber Extortion: What You Need to Know in 2021 appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/cyber-extortion-what-you-need-to-know-in-2021/

2. School Cybersecurity: How Awareness Training Removes Attackers' Options

Keeping student data safe and maintaining information security in education are part of living in today's world for educators. Why is it important to include data security in their work? Find an example of how to set up a school cybersecurity policy and more below.

School Cyberattacks on the Rise

There's no sign that digital attacks are slowing down in this sector. On the contrary, schools suffered a combined total of 348 publicly disclosed malware infections, phishing scams, denial-of-service attacks and other attacks in 2019. That's more than triple the number of attacks in the sector a year earlier.

Things didn't get better in 2020. In April, the FBI's Internet Crime Complaint Center (IC3) warned that threat actors could take advantage of the world's rapid transition to remote learning to undermine students' safety and privacy online. A summer 2020 report found that the weekly number of digital attacks per school had risen from 368 in May and June to 608 in July and August. Many of those digital attacks consisted of distributed denial-of-service (DDoS) attacks.

But that wasn't the only problem. In the months that followed, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert in which it revealed that threat actors were targeting K-12 schools to steal information, disrupt distance learning services and install ransomware. Threat actors assumed all kinds of disguises to boost their chances of success. In one attack, they even pretended to be parents in an attempt to target teachers with crypto-malware.

Why This Rise in School Cybersecurity Attacks?

Running on public funding could make it difficult for schools to find the money for consistent cybersecurity investments from year to year. At the same time, schools need to make their networks open to everyone they serve. That includes teachers, administrators, students, staff and parents — all of whom have varying levels of security awareness.

Take teachers, for example. Another report said nearly half (44%) of K-12 and college educators had not received even basic security awareness training around the digital threats facing them. Another 8% said that they weren't even sure if they had received

training. These results help to explain why so many aren't familiar with some of today's common digital threats.

That being said, a rise in digital attacks is what happens when schools also spend years thinking that they don't have anything worth stealing. If there's nothing worth stealing, then there's no threat. And if there's no threat, there's no need to invest in school cybersecurity measures.

That's a problem, given the speed with which schools are adding video conferencing apps and other remote access tools. These tools could provide attackers with a means to infiltrate schools' networks and deploy malware. They can also gain access to sensitive data and use it to conduct phishing scams, identity theft and other attacks.

How to Improve School Cybersecurity

One of the best ways to boost school cybersecurity is to create an incident response plan. This lets personnel use defined roles to delegate essential response functions. It also enables them to test those processes so that they're prepared in the event of a problem. That plan needs to work not only within the school's workforce but also with external groups, including local law enforcement and the FBI.

Schools can also try to prevent an incident from occurring in the first place. They can do that by creating an effective security awareness training program. It should consist of the following three components:

- leaders prepared for real-world digital attacks,
- robust digital security skills, and
- training by roles to keep the group protected against targeted attacks.

That last point is important. Teachers face different threats than students do, and those threats aren't the same as those confronting parents and administration. Therefore, schools need to create a program that provides training to all of their different groups. It should let people know the exact actions they can take and focus on relevant security topics. It needs to go beyond just email.

School Cybersecurity Training for Students

Schools can concentrate the content of their security awareness training programs on threats that affect their teachers and staff. But they need a different strategy for students, more so those in K-12 facilities. Just as they cultivate students' language, reading, writing and other skills, so too should they foster their pupils' digital hygiene.

One of the most effective means to do this is to make it hands-on and fun. The Center for Internet Security and the Multi-State Information Sharing & Analysis Center hosts the National Kids Safe Online Poster Contest every year, in which kids create posters that

educate their peers about staying safe online, including password hygiene, safe web browsing habits and identity theft. With programs like this, kids can be one of the many defenses against attacks on school cybersecurity.

The post School Cybersecurity: How Awareness Training Removes Attackers' Options appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/how-awareness-training-improves-school-cybersecurity/

3. The What, Why, and How of AI and Threat Detection

There are more online users now than ever before, thanks to the availability of network-capable devices and online services. The internet population in Canada is the highest it has been, topping the charts at 33 million. That number is only expected to increase through the upcoming years. However, this growing number and continued adoption of online services pose increasing cybersecurity risks as cybercriminals take advantage of more online users and exploit vulnerabilities in online infrastructure. This is why we need AI-backed software to provide advanced protection for online users.

The nature of these online threats is ever-changing, making it difficult for legacy threat detection systems to monitor threat behavior and detect new malicious code. Fortunately, threat detection systems such as McAfee's Antivirus and Threat Detection Defense adapt to incorporate the latest threat intelligence and artificial intelligence (AI) driven behavioral analysis. Here's how AI impacts cybersecurity to go beyond traditional methods to protect online users.

What is AI?

Most of today's antivirus and threat detection software leverages behavioral heuristic-based detection based on machine learning models to detect known malicious *behavior*. Traditional methods rely on data analytics to detect known threat *signatures* or footprints with incredible accuracy. However, these conventional methods do not account for new malicious code, otherwise known as zero-day malware, for which there is no known information available. AI is mission-critical to cybersecurity since it enables security software and providers to take a more intelligent approach to virus and malware detection. Unlike AI–backed software, traditional methods rely solely on signature-based software and data analytics.

Similar to human-like reasoning, machine learning models follow a three-stage process to gather input, process it, and generate an output in the form of threat leads. Threat detection software can gather information from threat intelligence to understand

known malware using these models. It then processes this data, stores it, and uses it to draw inferences and make decisions and predictions. Behavioral heuristic-based detection leverages multiple facets of machine learning, one of which is deep learning.

Deep learning employs neural networks to emulate the function of neurons in the human brain. This architecture uses validation algorithms for crosschecking data and complex mathematical equations, which applies an "if this, then that" approach to reasoning. It looks at what occurred in the past and analyzes current and predictive data to reach a conclusion. As the numerous layers in this framework process more data, the more accurate the prediction becomes.

Many antivirus and detection systems also use ensemble learning. This process takes a layered approach by applying multiple learning models to create one that is more robust and comprehensive. Ensemble learning can boost detection performance with fewer errors for a more accurate conclusion.

Additionally, today's detection software leverages supervised learning techniques by taking a "learn by example" approach. This process strives to develop an algorithm by understanding the relationship between a given input and the desired output.

Machine learning is only a piece of an effective antivirus and threat detection framework. A proper framework combines new data types with machine learning and cognitive reasoning to develop a highly advanced analytical framework. This framework will allow for advanced threat detection, prevention, and remediation.

How Can AI Help Cybersecurity?

Online threats are increasing at a staggering pace. McAfee Labs observed an average of 588 malware threats per minute. These risks exist and are often exacerbated for several reasons, one of which is the complexity and connectivity of today's world. Threat detection analysts are unable to detect new malware manually due to their high volume. However, AI can identify and categorize new malware based on malicious behavior before they get a chance to affect online users. AI–enabled software can also detect mutated malware that attempts to avoid detection by legacy antivirus systems.

Today, there are more interconnected devices and online usage ingrained into people's everyday lives. However, the growing number of digital devices creates a broader attack surface. In other words, hackers will have a higher chance of infiltrating a device and those connected to it.

Additionally, mobile usage is putting online users at significant risk. Over 85% of the Canadian population owns a smartphone. Hackers are noticing the rising number of mobile users and are rapidly taking advantage of the fact to target users with mobile-specific malware.

The increased online connectivity through various devices also means that more information is being stored and processed online. Nowadays, more people are placing their data and privacy in the hands of corporations that have a critical responsibility to safeguard their users' data. The fact of the matter is that not all companies can guarantee the safeguards required to uphold this promise, ultimately resulting in data and privacy breaches.

In response to these risks and the rising sophistication of the online landscape, security companies combine AI, threat intelligence, and data science to analyze and resolve new and complex cyber threats. AI-backed threat protection identifies and learns about new malware using machine learning models. This enables AI-backed antivirus software to protect online users more efficiently and reliably than ever before.

Top 3 Benefits of AI-backed Threat Detection Software

AI addresses numerous challenges posed by increasing malware complexity and volume, making it critical for online security and privacy protection. Here are the top 3 ways AI enhances cybersecurity to better protect online users.

1. Effective threat detection

The most significant difference between traditional signature-based threat detection methods and advanced AI-backed methods is the capability to detect zero-day malware. Functioning exclusively from either of these two methods will not result in an adequate level of protection. However, combining them results in a greater probability of detecting more threats with higher precision. Each method will ultimately play on the other's strengths for a maximum level of protection.

2. Enhanced vulnerability management

AI enables threat detection software to think like a hacker. It can help software identify vulnerabilities that cybercriminals would typically exploit and flag them to the user. It also enables threat detection software to better pinpoint weaknesses in user devices before a threat has even occurred, unlike conventional methods. AI-backed security advances past traditional methods to better predict what a hacker would consider a vulnerability.

2. Better security recommendations

AI can help users understand the risks they face daily. An advanced threat detection software backed by AI can provide a more prescriptive solution to identifying risks and how to handle them. A better explanation results in a better understanding of the issue. As a result, users are more aware of how to mitigate the incident or vulnerability in the future.

Take a Smarter Approach to Security

AI and machine learning are only a piece of an effective threat detection framework. A proper threat detection framework combines new data types with the latest machine learning capabilities to develop a highly advanced analytical framework. This framework will allow for better threat cyber threat detection, prevention, and remediation.

Source: *https://www.mcafee.com/blogs/consumer/consumer-cyber-awareness/the-what-why-and-how-of-ai-and-threat-detection/*

4. Google fined €220 million for abusing dominant role in online ads

The French competition authority has fined Google €220 million for abusing its dominant position in online advertising and favoring its services to the disadvantage of its publishers and competitors.

The investigation into Google's unfair digital advertising practices started after a complaint from News Corp Inc., Le Figaro group (which withdrew its complaint in November), and the Rossel La Voix group.

According to the French regulator, Google favored its Google Ad Manager tech used to operate the DFP ad server and the SSP AdX sales platform, which allow publishers to sell ad space on their sites and auction impressions to advertisers, respectively.

Google did not dispute the French watchdog's allegations and settled the antitrust case agreeing to pay the fine and promising to "improve the interoperability of Google Ad Manager services with third-party ad server and advertising space sales platform solutions and end provisions that favor Google."

"These very serious practices penalized competition in the emerging online advertising market and allowed Google not only to maintain but also to increase its dominant position," said Isabelle de Silva, president of France's competition regulator.

"This sanction and these commitments will make it possible to re-establish a level playing field for all players, and the ability for publishers to make the most of their advertising space."

Google promises to do better

Google has responded to the €220 million (roughly $267 million) fine by promising to increase access to data, flexibility, and transparency.

"While we believe we offer valuable services and compete on the merits, we are committed to working proactively with regulators everywhere to make improvements to our products," said Maria Gomri, Legal Director at Google France.

"That's why, as part of an overall resolution of the FCA's investigation, we have agreed on a set of commitments to make it easier for publishers to make use of data and use our tools with other ad technologies.

"We will be testing and developing these changes over the coming months before rolling them out more broadly, including some globally."

The French competition authority has accepted Google's commitments making them binding as part of its decision in the case.

It also underlined that Google's dominant position in digital advertising also comes with the "particular responsibility [..] to an effective and undistorted competition."

The European Commission previously fined Google $1.7 billion in March 2019 for abusing market dominance to block advertising competitors from displaying search ads on publishers' search results pages.

One year earlier, in June 2017, the European Commission hit Google with another record fine of $2.72 billion for abusing its dominant market position to tweak search results favoring the Google Shopping service to the detriment of direct competitors.

Source: https://www.bleepingcomputer.com/news/google/google-fined-220-million-for-abusing-dominant-role-in-online-ads/

5. Critical Business Operations Are At Risk, and Companies Are Not Making This a Priority

Many companies around the world with industrial operations environments, commonly referred to as operational technology (OT) environments, do not invest the same resources to protect OT systems as they do to secure their corporate enterprise environments. Yet, these same companies are investing significantly to transform these environments with modern technologies and techniques to improve productivity, become more efficient, increase worker collaboration through increased data analytics and achieve other benefits that will make the company more competitive through higher quality and cost-effective products.

Some of these new industrial process improvements include reduced latency through edge computing and 5G technologies, autonomous vehicles, robotics, cloud computing, industrial Internet of things (IIoT) devices, remote access and more. Yet, the age-old problem continues to exist whereby insufficient cybersecurity controls make these

environments easy targets for cybercriminals and nation-state cyberattacks. The industrial OT environments are critical to a company's financial well-being and, depending on what the company produces, may be essential for the functioning of the broader society and economy. A recent example is the semiconductor shortage that has impacted many companies that produce all types of electronic products, mobile phones and cars. The risk and impact of an OT attack are much higher than a cyberattack on these same companies' corporate enterprise environment where they invest significantly today.

Most companies are taking shortcuts by looking for easy and cheap ways to protect their OT environments. This typically involves the purchase of OT intrusion detection system (IDS) technology that can help with device discovery, network visualization, some type of signature-based malware detection and device vulnerabilities. This is a good start, but this type of solution is far from a comprehensive security program that is required to mitigate the company's risk from a broad set of OT threats.

In the corporate enterprise environment where companies have been investing in mature cybersecurity programs, a one-tool approach would be considered laughable and certainly would fail any compliance audit. So why are companies reluctant to invest in protecting their critical OT environments?

- **Lack of governance:** Companies have not established the roles and responsibilities for OT security. This is a critical step, and the trend is to assign the chief information security officer (CISO) this responsibility. This is because the CISO understands what a good security program requires. The CISO may not understand the OT environment, but this has not proven to be a significant issue.
- **Lack of a quantitative risk assessment:** Why quantitative? Because the business stakeholders will quickly support the need to invest in a cybersecurity program once they realize the financial impact to the business should they be unlucky enough to be attacked.
- **Document "current state":** OT IDS products help with this activity but will not do it all. What type of insight do you need? You need a perspective on:
    a. People: Who needs access to the OT environment? Who already has access? How is this access managed? Is remote access common?
    b. Process: What are the industrial operations processes? What technologies support these processes? What processes are changing due to new digital transformation strategies?
    c. Technologies: Which devices support which industrial processes? Are there OT assets that are not connected to an IP network? How will these be protected? This inventory will be valuable for lots more than just security. For example, consideration should be given to integrating the OT device details into the company's asset management system.

d. Network Architecture: How is the network designed? Are leading practice security principles incorporated into the design? Many companies are digitally transforming their network infrastructure and leveraging 5G and WiFi. With OT original equipment vendors adding more industrial IoT capabilities to their new products, this should be a consideration and included in the security strategy.

e. Threat Assessment: Which threats are relevant, and which are not? It is very important to identify the threats that are relevant so that an effective and efficient security program can be developed to mitigate the risks.

f. Vulnerability Assessment: What vulnerabilities exist currently? Are there associated controls in place to prevent the vulnerability from being exploited in a cyberattack?

g. Data Discovery and Classification: What data is being produced and transmitted from the industrial environment? If you do not know, then data discovery, classification and protection must be added to the strategy and plan.

- **Lack of an OT security strategy and plan:** Once you understand the current environment, it is time to develop a cybersecurity strategy and plan to mitigate the risk of a cyberattack. This step seems logical, but it cannot be completed effectively without the first three steps. The quantitative risk assessment results establish the priorities. The plan should include techniques to continuously maintain visibility into all the areas referenced in step 3. It must have preventative controls put into place to protect known vulnerabilities. Finally, there must be solutions included to monitor the controls to make sure they are operating effectively. If they are not, there must be solutions to identify when a cyberattack is exploiting a vulnerability so that you can quickly respond to mitigate any impact to the business and quickly return to business as usual.

It is time that companies with OT environments start investing in their OT security programs. It will not be cheap or easy, so you should consider leveraging a trusted systems integrator with OT security experience.

The post Critical Business Operations Are At Risk, and Companies Are Not Making This a Priority appeared first on Security Intelligence.

Source: https://securityintelligence.com/posts/ot-security-critical-business-operations-at-risk/

6. Steam Gaming Platform Hosting Malware

Emerging malware is lurking in Steam profile images.

Look out for SteamHide, an emerging malware that disguises itself inside profile images on the gaming platform Steam, which researchers think is being developed for a wide-scale campaign.

The Steam platform merely serves as a vehicle which hosts the malicious file, according to research from G Data: "The heavy lifting in the shape of downloading, unpacking and executing a malicious payload fetched by the loader is handled by an external component, which accesses the malicious profile image on one Steam profile. This external payload can be distributed via crafted emails to compromised websites."

The technique is called steganography and it's not new — but Steam profiles being used as attacker-controlled hosting sites, is.

"While hiding malware in an image file's metadata is not a new phenomenon, using a gaming platform such as Steam is previously unheard of," G Data analyst Karsteen Hahn said about SteamHide in a new disclosure report, which builds on the original find by @miltinh0c on Twitter:

Reference:

https://twitter.com/miltinh0c/status/1392944896760238080

The malware downloader is hiding in the Steam profile image's metadata, specifically in the International Color Consortium (ICC) profile, a standardized set of data to control color output for printing. Attackers hide their malware in benign images commonly shared online, including memes like "blinking white guy" used in the G Data analysis example.

"The low-quality image shows three frames of the 'white guy blinking' meme alongside the words January, a black screen, and September," Hahn added.

Victims of the malware don't have to be on Steam or have any gaming platform installed, G Data's researchers found. The profile image data only hosts the malware — to make it onto a victim's machine, it must be fetched by a loader that's been loaded onto a compromised device, the report explained.

Attackers Have Big Plans for SteamHide

Once executed on a victim machine, the malware terminates any security protections and checks for administration rights, the researchers found, then copies itself to "LOCALAPPDATA" folder and persists by creating a key in a registry that G Data identified as "\Software\Microsoft\Windows\CurrentVersion\Run\BroMal."

For now, that's all it does. But G Data said the developers of SteamHide have hidden tools inside their malware that aren't currently being used but could be dangerous later; including checking if Teams is installed on the infected machine, and a method stub named "ChangeHash" that indicates developers are working on increasingly complex iterations of the existing malware. There's also a tool that enables the malware to send and receive commands over Twitter.

There could be new versions soon: Updating the malware only requires uploading a new profile pic.

"I am confident that we will see this malware emerge soon in the wild just like it happened with other in-development families that we covered, e.g., StrRAT and SectopRAT," according to researchers.

It's hard to say how easy the malware and attacker-controlled profiles would be to root out: Steam's most recent data said the platform has more than 20 million users playing games, including popular titles like Counter-Strike: Global Offensive, Dota 2 and Apex Legends. Steam's parent company Valve hasn't responded to Threatpost's request for comment on SteamHide.

This isn't the first time Steam has been hit with cybersecurity issues. For instance, last December, Steam had to fix critical bugs that allowed a remote attacker to crash another player's game, take over the computer and hijack all the computers connected to a third-party server.

Source: https://threatpost.com/steam-gaming-delivering-malware/166784/

7. IKEA Fined $1.2M for Elaborate 'Spying System'

A French court fined the furniture giant for illegal surveillance on 400 customers and staff.

KEA's French subsidiary was just hit with a $1.2 million fine after it was found guilty of a creepy systematic snooping scheme targeting customers, employees and even prospective hires.

Prosecutors said in all, the company illegally surveilled about 400 people in total, according to the BBC.

IKEA France's former chief executive, Jean-Louis Baillot, was also personally fined €50,000 (around $60,200 at press time) for "storing personal data," according to Deutsche Welle, and given a two-year suspended sentence by the French court.

More than a dozen others were on trial for the spy scheme, including four police officers accused of handing over confidential records and an additional former CEO of IKEA France, Stefan Vanoverbeke, DW reported.

The furniture seller subsidiary was found guilty of running the illegal operations between 2009 and 2012 that involved hiring a private security firm, Eirspace, to dig up dirt on their employees and perceived adversaries, according to reports. In one instance, the company investigated an employee to find out why they could afford a BMW on their salary.

Another former IKEA France employee, who is also involved in union activism, was accused by the company of robbing a bank after they hired cops to hand over police records, DW said. The employee hadn't broken any laws, just shared a name with a bank robber.

One store manager, Patrick Soavi, described to the court how he asked a police-officer cousin to "cast an eye" on 49 job applicants, BBC reported. Later he sent on another 68 names over for illegal background checks.

"I recognize that I was very naïve and rather over-zealous, but we were being asked to carry out these checks, and once I'd put a foot inside this system it was too late," Soavi testified.

Ikea France Denies 'Generalized Espionage'

Last spring, the former head of IKEA France's risk-management operations, Jean-Francois Paris, testified that he budgeted between $633,000 and $753,000 every year to outside security firm Eispace for these kinds of investigations.

Eirspace chief Jean-Pierre Fourès was also given a suspended two-year sentence and €20,000 fine ($24,000) by the French court.

In response, IKEA France's legal team said there wasn't "generalized espionage" within the organization and that the subsidiary issued the statement that it "takes the protection of its employees' and customers' data very seriously," DW reported.

IKEA France has not responded to Threatpost's request for comment on the ruling.

Investigative journalists with Canard Enchaine first uncovered the illegal scheme, and a union has also filed a formal complaint against IKEA France.

Source: https://threatpost.com/ikea-fined-spying-system/166991/

8. Dell SupportAssist bugs put over 30 million PCs at risk

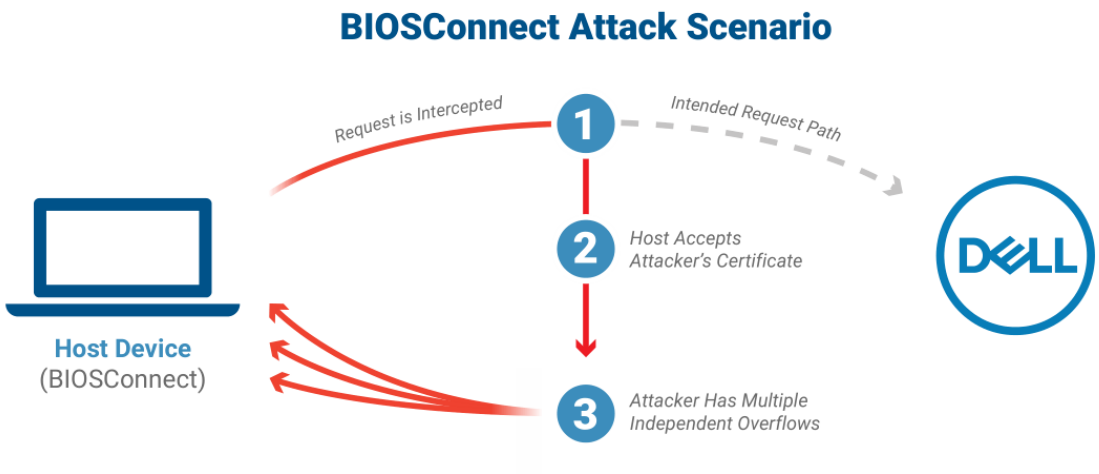
Security researchers have found four major security vulnerabilities in the BIOSConnect feature of Dell SupportAssist, allowing attackers to remotely execute code within the BIOS of impacted devices.

According to Dell's website, the SupportAssist software is "preinstalled on most Dell devices running Windows operating system," while BIOSConnect provides remote firmware update and OS recovery features.

The chain of flaws discovered by Eclypsium researchers comes with a CVSS base score of 8.3/10 and enables privileged remote attackers to impersonate Dell.com and take control of the target device's boot process to break OS-level security controls.

"Such an attack would enable adversaries to control the device's boot process and subvert the operating system and higher-layer security controls," Eclypsium researchers explain in a report shared in advance with BleepingComputer.

"The issue affects 129 Dell models of consumer and business laptops, desktops, and tablets, including devices protected by Secure Boot and Dell Secured-core PCs," with roughly 30 million individual devices exposed to attacks.



The researchers identified one issue leading to an insecure TLS connection from BIOS to Dell (tracked as CVE-2021-21571) and three overflow vulnerabilities (CVE-2021-21572, CVE-2021-21573, and CVE-2021-21574).

Two of the overflow security flaws "affect the OS recovery process, while the other affects the firmware update process," Eclypsium says. "All three vulnerabilities are independent, and each one could lead to arbitrary code execution in BIOS."

Additional info on the vulnerabilities can be found in Eclypsium's report and the complete list of affected device models in Dell's advisory.

Users advised not to use BIOSConnect for updating their BIOS

According to Eclypsium, users will have to update the system BIOS/UEFI for all affected systems. The researchers also recommend using an alternate method other than the SupportAssist's BIOSConnect feature to apply BIOS updates on their devices.

Dell is providing BIOS/UEFI updates for impacted systems and updates to affected executables on Dell.com.

CVE-2021-21573 and CVE-2021-21574 don't require require additional customer action as they were addressed server side on May 28, 2021. However, the CVE-2021-21571 and CVE-2021-21572 vulnerabilities require Dell Client BIOS updates to be fully addressed.

Users who cannot immediately update their systems can disable BIOSConnect from the BIOS setup page or using the Dell Command | Configure (DCC)'s Remote System Management tool.

"The specific vulnerabilities covered here allow an attacker to remotely exploit the UEFI firmware of a host and gain control over the most privileged code on the device," the researchers concluded.

"This combination of remote exploitability and high privileges will likely make remote update functionality an alluring target for attackers in the future, and organizations should make sure to monitor and update their devices accordingly."

Dell software plagued by critical flaws

This is not the first-time owners of Dell computers have been exposed to attacks by security vulnerabilities found in the SupportAssist software.

Two years ago, in May 2019, the company patched another high-severity SupportAssist remote code execution (RCE) vulnerability caused by an improper origin validation weakness and reported by security researcher Bill Demirkapi in 2018.

This RCE allowed unauthenticated attackers on the same Network Access layer with targeted systems to remotely execute arbitrary executables on unpatched devices.

Security researcher Tom Forbes found a similar RCE flaw in the Dell System Detect software in 2015, allowing attackers to trigger the buggy program to download and execute arbitrary files without user interaction.

SupportAssist was again patched one year later, in February 2020, to address a security flaw due to a DLL search-order hijacking bug that enabled local attackers to execute arbitrary code with Administrator privileges on vulnerable devices.

Last but not least, last month Dell addressed a flaw making it possible to escalate privileges from non-admin users to kernel privileges, a bug found in the DBUtil driver that ships with tens of millions of Dell devices.

Source: https://www.bleepingcomputer.com/news/security/dell-supportassist-bugs-put-over-30-million-pcs-at-risk/

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.