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

# Monthly Security Bulletin

**March 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

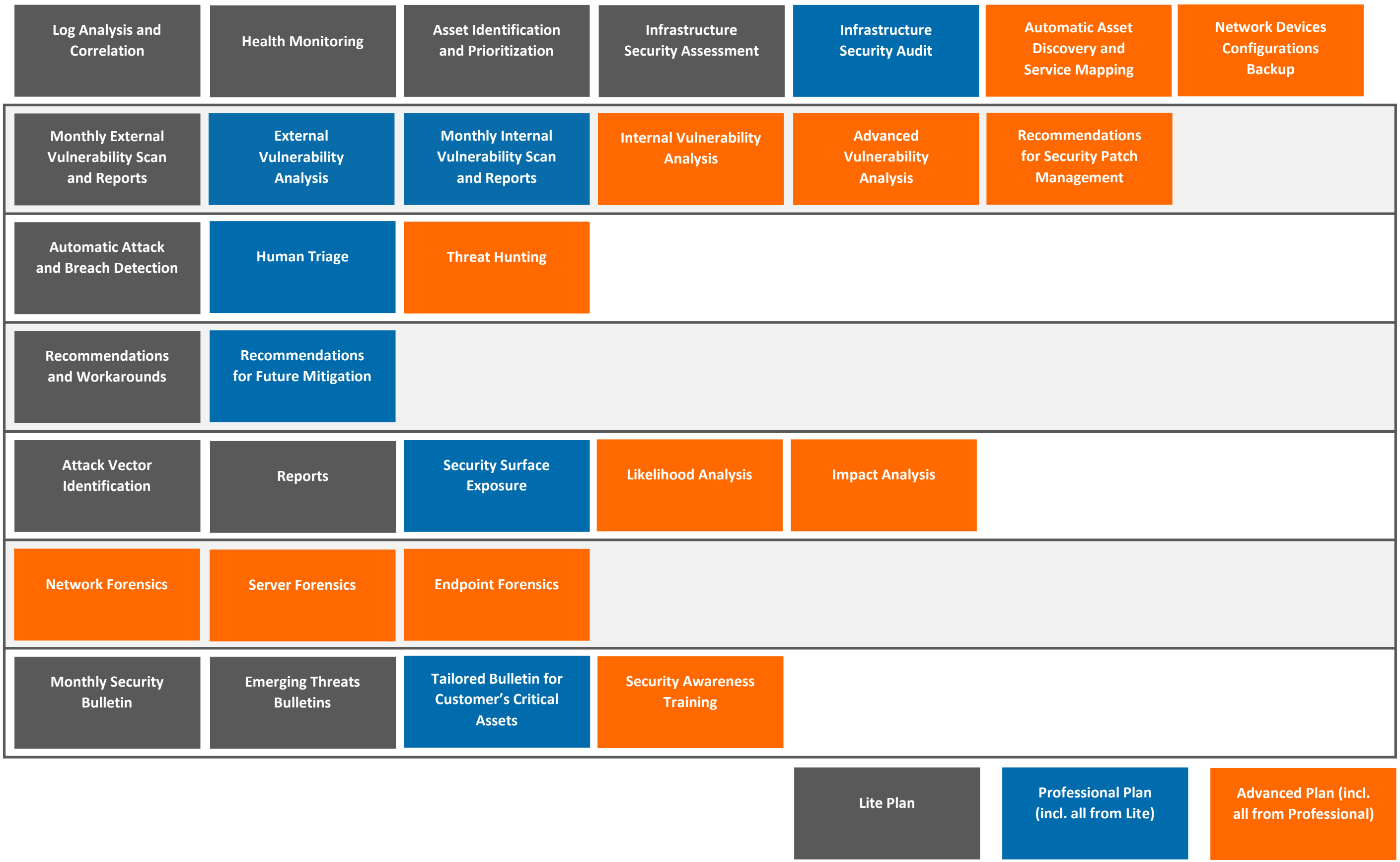
**Start to mitigate cyber threats and minimize the risk!**

## 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!**



| | | | | | | |
|---|---|---|---|---|---|---|
| ⬛ 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 Management | |
| ⬛ 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. US govt: Number of identity theft reports doubled last year

The U.S. Federal Trade Commission (FTC) said today that the number of identity theft reports has doubled during 2020 when compared to 2019, reaching a record 1.4 million reports within a single year.

Throughout last year, fraudsters have continuously targeted government funds reserved for people finding themselves in financial trouble due to the ongoing COVID-19 pandemic.

"2020's biggest surge in identity theft reports to the FTC related to the nationwide dip in employment," the FTC said.

"After the government expanded unemployment benefits to people left jobless by the pandemic, cybercriminals filed unemployment claims using other people's personal information."

For instance, the FTC received 394,280 reports regarding government benefits fraud attempts, the vast majority of them describing unemployment benefit identity theft fraud — compared with 12,900 reports filed in 2019.

The FTC also saw reports regarding cybercriminals using stolen business or personal information to illegally apply for government-sponsored small business loan programs.

"Last year, we had 99,650 reports of fraud involving business or personal loans, compared with 43,920 reports in 2019," the FTC added. "Not all of the new reports related to the government relief effort, but they were a big share of the increase."

IRS federal stimulus payments were also targeted by scammers and reported to the FTC as tax identity theft attempts, with 89,390 reports being filed last year compared to the 27,450 reports sent in 2019.

The Internal Revenue Service (IRS) has recently published taxpayer guidance on how to identify theft attempts involving unemployment benefits.

"The Internal Revenue Service today urged taxpayers who receive Forms 1099-G for unemployment benefits they did not actually get because of identity theft to contact their appropriate state agency for a corrected form," the US federal revenue service said.

"Additionally, if taxpayers are concerned that their personal information has been stolen and they want to protect their identity when filing their federal tax return, they can request an Identity Protection Pin (IP PIN) from the IRS."

The IRS announced in November 2020 that sensitive information will be masked on all business tax transcripts starting December to protect companies from identity theft.

The US Treasury Department bureau also warned of a surge in pandemic-related scams trying to harvest personal information using economic impact payments as a lure, with the stolen info to be later used for identity theft and tax-related fraud.

Source: *https://www.bleepingcomputer.com/news/security/us-govt-number-of-identity-theft-reports-doubled-last-year/*

## 2. New Linux malware steals SSH credentials from supercomputers

A new backdoor has been targeting supercomputers across the world, often stealing the credentials for secure network connections by using a trojanized version of the OpenSSH software.

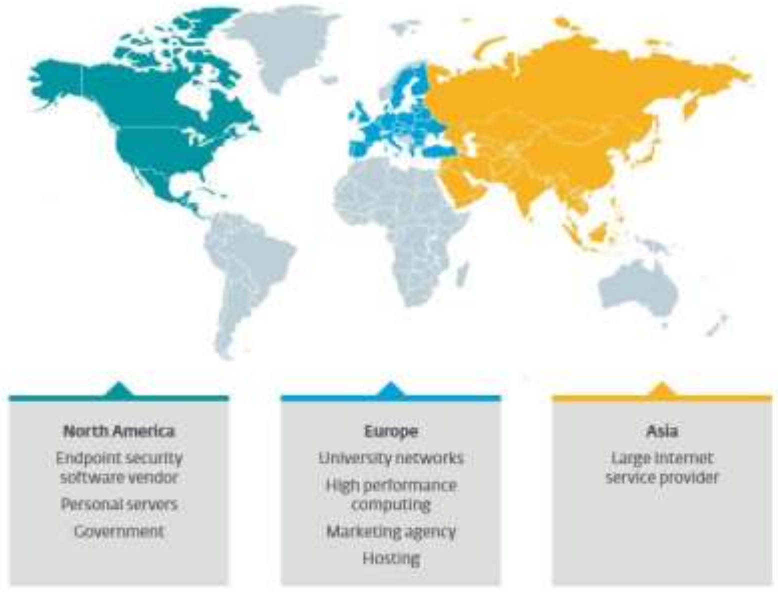
The malware is not widespread and appears to target mostly high-performance computers (HPC) and servers on academic and research networks.

### Multiplatform, high-profile targets

Security researchers at cybersecurity company ESET discovered the malware and named it Kobalos, after the misbehaving creature in Greek mythology.

They say that Kobalos has a small but complex codebase that can execute on other UNIX platforms (FreeBSD, Solaris). Some artifacts discovered during the analysis indicate that there may also be variants for AIX and Windows operating systems.

After creating a fingerprint for the threat, ESET ran internet-wide scans to find Kobalos victims. They discovered that many of the compromised systems were supercomputers and servers in the academic and research sector. Other victims include an endpoint of an undisclosed software security vendor in North America, a large ISP in Asia, marketing agencies, and hosting providers.



ESET could not establish the initial attack vector that allowed the hackers to gain administrative access to install Kobalos. However, some of the compromised systems "ran old, unsupported, or unpatched operating systems and software," so exploiting a known vulnerability is a likely scenario.

## Stealing SSH creds

Although the researchers spent months analyzing the malware, they could not determine its exact purpose because of the generic commands included and no specific payload.

Kobalos provides remote access to the file system and it can spawn terminal sessions, which lets the attackers run arbitrary commands. Some details are available, though.

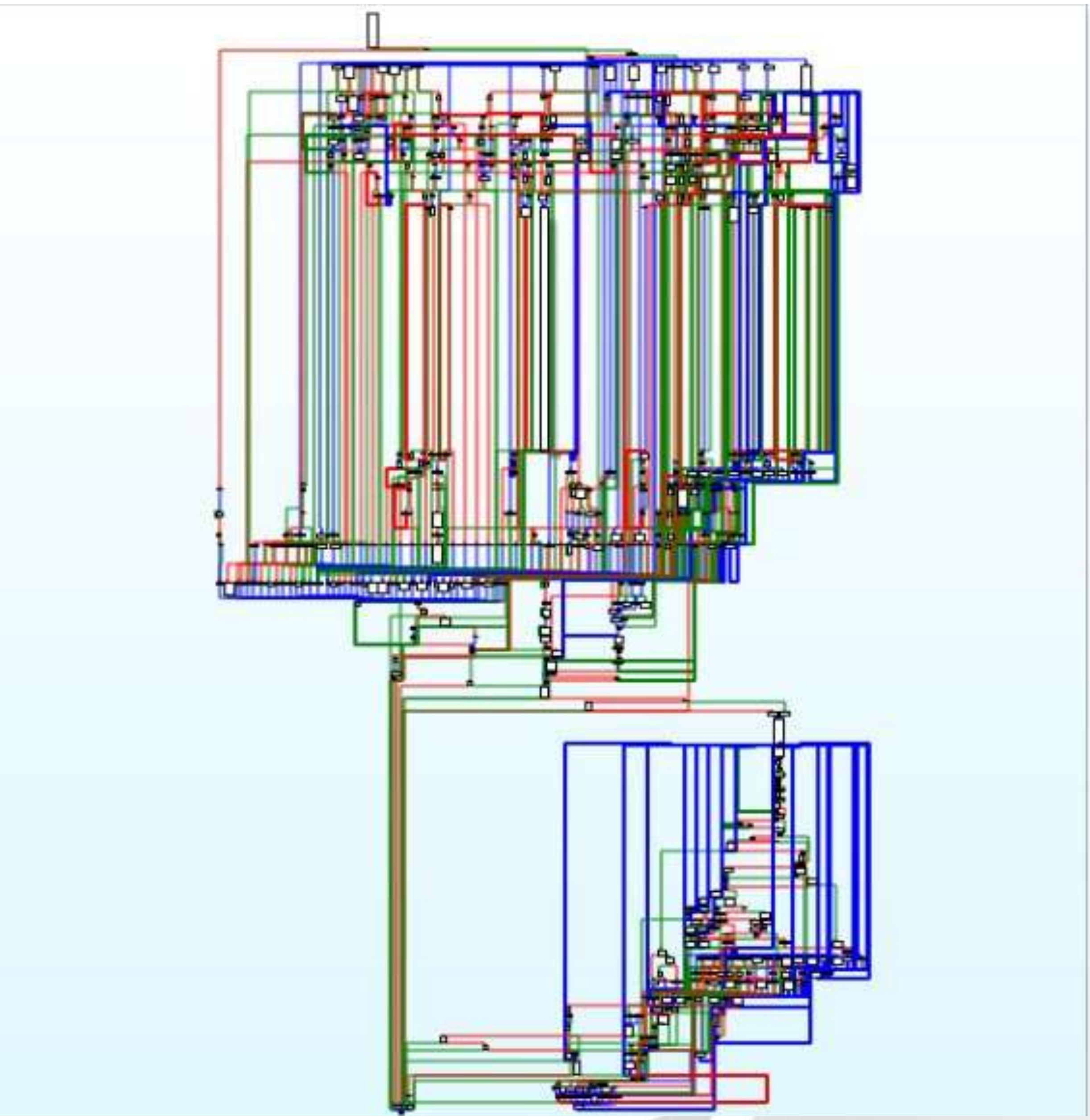
"On compromised machines whose system administrators were able to investigate further, we discovered that an SSH credential stealer was present in the form of a trojanized OpenSSH client. The /usr/bin/sshfile was replaced with a modified executable that recorded username, password and target hostname, and wrote them to an encrypted file" – ESET

The researchers believe that credential theft could explain how the malware spreads to other systems on the same network or other networks in the academic sector since students and researchers from multiple universities may have SSH access to supercomputer clusters.

## Tiny, complex backdoor

Despite being lightweight, only 24KB for 32/64-bit samples, Kobalos is a complex piece of malware with custom obfuscation and anti-forensics techniques that hinder its analysis, and with plenty of features for its small size.

An interesting feature that sets Kobalos apart is that its code is bundled into a single function and there is only one call from the legitimate OpenSSH code to it. It has a non-linear control flow, though, recursively calling that function to perform subtasks - supports a total of 37 actions, one of which can turn any compromised machine into a command and control (C2) server for others.



The researchers discovered that remote operators have three options to connect to Kobalos:

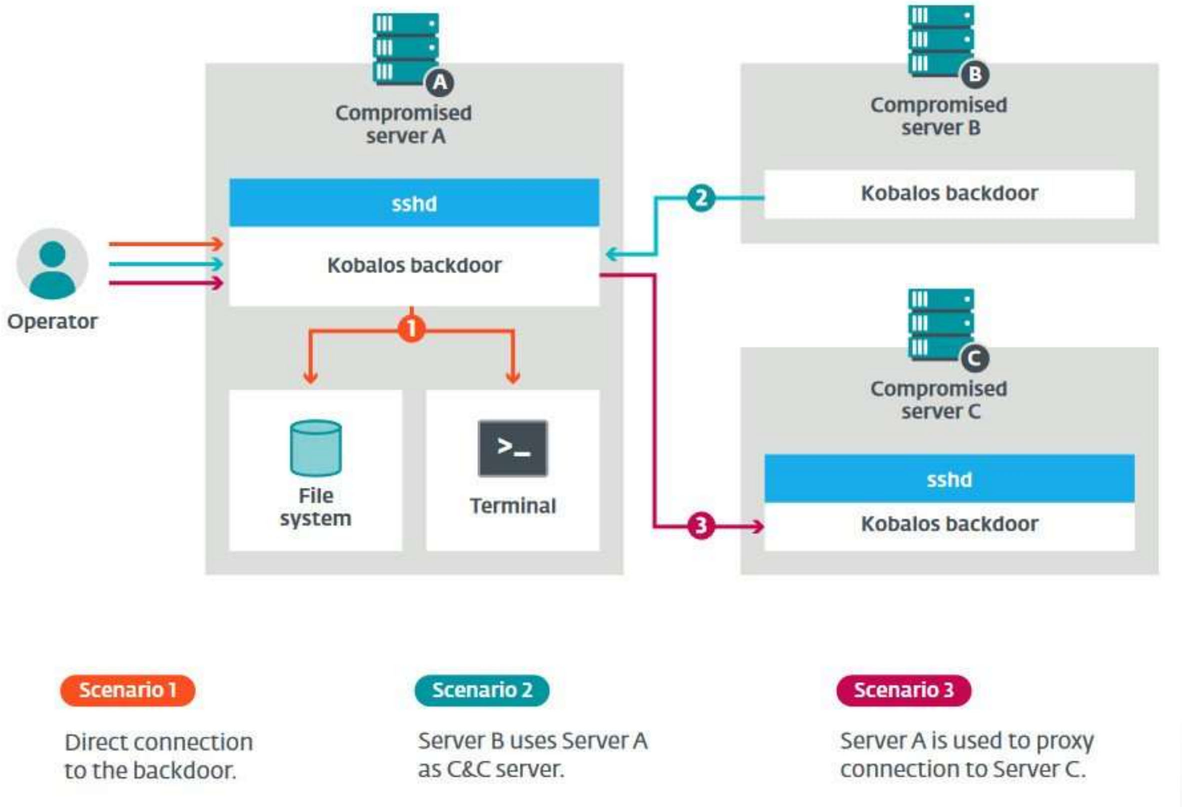
- open a TCP port and waiting for an incoming connection (sometimes called a passive backdoor)

- connect to another instance of Kobalos configured to run as a C2 server

- wait for connections to an already running, legitimate service but coming from a specific TCP source port (trojanize the running OpenSSH server)

Kobalos also encrypts the traffic to and from the attackers. To achieve this, clients need to authenticate using an RSA-512 key and a password. The key generates and encrypts two 16-byte keys that encrypt the communication using the RC4 stream cipher.

Furthermore, the backdoor can switch communication to an alternative port and act as a proxy (chainable) to reach other compromised servers.



Given the tiny codebase and the power it packs, ESET says that the sophistication of Kobalos "is only rarely seen in Linux malware," which indicates a developer with much better skills than the average Linux malware author.

While the complexity of the malware is undisputed, questions remain about the attacker's objective and the period Kobalos has been in use (some of the strings found relate to Windows 3.11 and Windows 95, which are more than 25 years old).

What is certain is that Kobalos is stealing SSH credentials from high-profile victims that include high-performance computer clusters and that it has been active before other attacks against supercomputers recorded since late 2019.

Furthermore, unlike the already reported incidents involving HPC networks, system administrators did not find any attempt to mine for cryptocurrency or run computationally expensive tasks in the case of Kobalos.

ESET notified all Kobalos victims they could identify and worked with them to remediate the infection. The researchers published a full technical analysis of Kobalos that includes indicators of compromise (IoCs) that can help potential victims detect the malware.

Source: *https://www.bleepingcomputer.com/news/security/new-linux-malware-steals-ssh-credentials-from-supercomputers/*

## 3. CISO Success: It's About More Than Tech Skills

The chief information security officer (CISO) is a relatively new position in the C-suite. It's about 25 years old or less, depending on whom you ask. But, it is only within the last 10 or so years that the role has taken on greater prominence, likely because of the increase in cyber breaches over the last decade. What does a CISO do, and what skills are required?

### Beyond Technology to Soft Skills

CISO roles and responsibilities are not as clear cut as some of the more established C-suite roles. This is in large part due to the overlap (or competition, some may say) with some other, similar roles. Chief security officer, chief information officer and even chief technology officer or chief information risk officer all could be competing roles. To complicate matters, there is no uniform reporting structure for the CISO position across the industry. In some cases the CISO reports directly to the CEO. In others they report to a CIO.

Some of this confusion may come from the idea that the role should be technology-based. In practice, managing information security is not a purely technological problem.

If it isn't all about tech, what do you need to be a CISO? To what degree are they technology-based? To what degree do they focus on business? On people? Do they require any special CISO soft skills and leadership techniques?

The skills required to be a successful CISO actually require a mixed bag of talents. They range from incident response, business resilience, intuitive thinking, tapping into your people, serving as the trusted advisor and being the voice of reason. That mixed bag of skills makes it a hard job to fill and succeed at.

## The Evolution — and Potential Revolution — of the CISO

All those challenges mean lots of responsibility and a big impact. A CISO with the right skills can overhaul how their group can handle both its security and business.

Let's take a quick look at the general history of the CISO. In the early stage of the title's existence (~1995-2005), CISOs focused on compliance and it was mostly an IT-related role. The middle stage (2005-2015) brought an increased focus on risk and more work on policies, procedures and frameworks. CISOs could make changes and adoptions for mobile technologies and handle and lead incident response. In the recent stage (2015-today), CISOs handle enforcement and leadership across a variety of platforms. These include, but are not limited to, cloud, mobile, identity and access management, mergers and acquisitions, strategy and business operations.

As the role evolves, the CISO takes on increased responsibility. At least, in theory, they should now have a more prominent role within the organization than they did in the 90s.

So, what does a CISO need to succeed today?

## Dispelling the Myth: The CISO Does Not Need to Be a Tech Whiz

It may seem obvious that a CISO needs to be amazing at handling tech, but that's not always what you need most to be successful in the role. Sure, it matters to be able to talk the talk with your technical staff. You need to understand what they are doing, but that is only one piece of a much larger puzzle.

Remember, this is a leadership role. The CISO needs to have sound knowledge of the field, but doesn't have to be the 'hands on keyboard' type. Success requires you have a larger bag of non-technical skills at hand.

## What it Takes to Be a CISO Today

A more refined list of skills a CISO should have include:

An understanding of business operations and what makes the organization tick.

Superior communication skills with a variety of stakeholders, especially with the C-suite.

A strong knowledge of security operations, including changing or even creating them if needed. This goes beyond just virtual security into physical security, as well.

Program management skills, if for no other reason than that this position has so many moving parts and requires someone who can juggle.

Cybersecurity knowledge, so they can appropriately manage issues of threat intelligence, identity and access management, data loss and prevention, investigations and forensics and monitoring and automation technology, such as SIEM and SOAR.

Enough of an IT and security architecture background that they can navigate the financial and maintenance needs of any information security program.

Disaster recovery and business continuity skills, both for pre- and post- event planning.

A strong knowledge of governance, risk and compliance issues and even legal issues, which will come in very handy for policy and procedure creation and maintenance.

Human resource management, which can be very important for education and training.

That's a pretty impressive and expansive list, but here's the kicker: You could find somebody who has all these skills, and they might fail in their role if they do not possess a couple more.

## It's About Culture

In a 2019 PwC and Harvard Business Review Analytic Services survey, 63% of respondents said culture will be among the top five responsibilities for the CISO within three years. That means a CISO will probably spend less time on technology-related matters and more time employing their soft skills. First, they'll need to try to sway the board into making cybersecurity investments. Secondly, they'll figure out what the best change management techniques will be.

A successful information security program will require two things: buy-in from executive leadership and buy-in from the rest of the team. So, how would you go about getting that buy-in?

When it comes to executive leadership, you need to speak their language. You need to convey how your decisions help the business, and more recently, how they affect risk and resilience. If your approach to winning over these people is a litany of threat intelligence reports, vulnerability assessments and industry warnings, don't expect to get too far. The key to your success with this stakeholder group rests solely on the CISO's talent to translate those reports, assessments and warnings into actions. That means you need to show how your work will save the group money (such as through a risk mitigation strategy) or generate a return on investment.

If you can demonstrate tangible value to the executive group, they'll be more likely to support your efforts.

But winning over the board and the rest of the C-suite is the easier job out of the two buy-in groups. Winning over the rest requires some serious skills in the field of change management.

## Getting Buy-In for the CISO and the Plan

Change management is tough. Entire courses and textbooks are devoted to the subject. All types of teams, both small and large, grapple with how to implement it in practice. Here's the first thing you should know about change management: there's no foolproof way to do it. So much of it depends on the existing culture and what the intended vision is. But there are a few solid principles that can be followed.

First and foremost, do not get lost in the details out of the gate. With that said, don't forget planning, either. If you want to make changes, you actually need to know the details. It's just a matter of when to focus in on them. Have them ready in your back pocket out of the gate, as best you can. Somebody may ask you what those details are, and if you're not ready, you may find yourself stumbling in a way it's hard to recover from.

## Back Up Words With Actions

But, what should a CISO first focus on to be successful? Well, it has nothing to do with technology. It has everything to do with psychology and emotional intelligence. And most of all: it all starts from the top. If there is some sort of culture change coming down the pipeline, people will be looking to the CISO. If employees see words and not actions, there will be a profound impact; except, that impact won't be the type the CISO is looking for. Cognitive dissonance is a real thing that can erase your best laid plans.

Put simply, cognitive dissonance means people become uncomfortable when their beliefs don't match their actions or with the actions they are asked to carry out. That means if, as a leader, you ask someone to do something they do not agree with, expect some form of pushback. This is particularly important in the cybersecurity space because employees are most often the weakest link in the security chain.

## The CISO as the Master of Connection

Getting past cognitive dissonance (which can also happen in the board and C-suite; nobody is immune to it) is more than just presenting your reasons for doing something. Once a person enters a state of cognitive dissonance, the only way to break free from it is by going deeper, showing the stakeholder that the new behavior will have a positive effect on both personal growth and the state of the group. Show some value that they can buy into, like savings and growth. In the end, what you are looking for is an emotional connection. This is why it is vital for the CISO to be able to answer the following questions, with specificity:

- What is being done?

- Why it is being done?

- What is the result of not doing it?

- How does it impact the business?

- How does it impact employees?

Therefore, before the CISO makes any security-program related plans, they need to first identify sources of resistance, including their own. They should also keep in mind the four dimensions of emotional intelligence: self-awareness, self-management, social awareness and social management.

### How the CISO Becomes the Premier Cybersecurity Executive

Being a good CISO requires talents that go well beyond the technical arena. In this dynamic field, the CISO must be dynamic and diverse in their skills as well. The CISO wears so many hats, and so many more than they would have had even just a few years ago. One-trick ponies need not apply.

Technical skills are important and may get you the job, but if you want to be successful, be ready to go out of your comfort zone.

Remember soft skills, even more so when you have the technical prowess to back them up. If you can employ some of the suggestions above and round out your game in the business and personal arenas, your next job title after CISO may be CEO.

Source: *https://securityintelligence.com/articles/ciso-success-more-than-tech-skills/*

## 4. Ransomware Attacks Hit Major Utilities

Eletrobras, the largest power company in Latin America, faces a temporary suspension of some operations.

Two state-owned utility companies in Brazil suffered separate ransomware attacks in the past week, forcing them to shut down some operations and services temporarily, In one case, sensitive data was stolen and dumped online, including network access logins and engineering plans.

Centrais Eletricas Brasileiras (Eletrobras) and Companhia Paranaense de Energia (Copel) both reported attacks, the latter of which appears to be the work of Darkside, which flogged data stolen from the attack online, according to a published report.

Darkside is a technically innovative ransomware group that's tried to brand itself as an altruistic, digital Robin Hood by making charitable donations with the Bitcoin it's stolen from victims.

In this case, the group said it stole more than 1,000 gigabytes of Copel data in the attack, including sensitive information allowing for access to key infrastructure, personally identifiable information (PII) of top management and customers, and detailed engineering plans of the company's network, according to the report, which included a snapshot of an ad for the data from a hacker forum.

Both utilities are state-owned and have a significant presence in the country. Eletrobras is the largest utility in Latin America and owner of Eletronuclear, which constructs and operates nuclear power plants. Copel is the largest utility provider in the Brazilian state of Parana.

## Eletrobras Cyberattack Impacts Nuclear Plant Subsidiary

It's not clear at this time who is behind the Eletrobras attack, which the company acknowledged in a press release posted earlier this week. The attack hit the administrative network of its Eletronuclear subsidiary, which runs two nuclear power plants—Angra1 and Angra 2.

In the case of the attack on Eletronuclear, the company had to suspend some of its systems to protect the integrity of data, the company said.

However, the administrative network is not connected to the operational technology (OT) systems that run the nuclear power plants, which are isolated from that network for security reasons, according to the release. Because of this, there was no impact on safety or the operation of the Almirante Álvaro Alberto Nuclear Power Station (CNAAA), nor damage to the supply of electricity to the National Interconnected System, according to Electrobras.

The company did not provide details on whether any data was stolen in the attack, and if there is any indication of who the culprit may be. Eletrobras has reported the attack to the appropriate authorities and is continuing to investigate, it said.

## Reams of Data Stolen from Copel Utility

The Copel attack was not publicly disclosed but mentioned in an SEC filing on Monday, according to Bleeping Computer, which appears to have had contact with Darkside about its hand in the attack.

Hackers said they gained access to the company's CyberArk cloud security solution for privileged access management and exfiltrated plaintext passwords across Copel's local and internet infrastructure, according to the report.

Specifically, attackers said the 1,000 GB cache of data they pilfered includes: Data from CyberArk storage with clear-text passwords from all local and internet infrastructure; network maps and diagrams; backup schemes and schedules; domain zones for cope.com and copel.nt domains; a database that stores ActiveDirectory data; phone numbers, emails and ID and other personal data of employers and customers, including top management; and NDAs, finances and contract info; and detailed engineering schemes, plans and network switches.

## Ransomware Remains a Top Cyberthreat

Ransomware continues to be one of the top threats plaguing organizations, spurred by gangs' success in extorting large sums of money from victims. 2020 went down as a banner year for this type of cybercrime, which hit less lucrative organizations such as hospitals particularly hard due to the COVID-19 pandemic.

Ransomware gangs don't appear to be letting up in 2021 either, with new variants of ransomware already detected — such as Babuk Locker, which is targeting corporations.

That said, there has been some promising news for potential ransomware victims this year thanks to global efforts to take down the criminal gangs behind major malware distribution schemes. Last week, an international law-enforcement consortium disrupted one of the most prolific malware strains, Emotet, by dismantling servers and infections. The malware is often used as a gateway infection to distributing ransomware.

And in an unrelated effort, authorities in Canada charged a suspect believed to be responsible for NetWalker ransomware attacks, and seized $454,500 in cryptocurrency from ransom payments made by three separate victims.

Source: *https://threatpost.com/ransomware-attacks-major-utilities/163687/*

# 5. Hacker Tries to Poison Water Supply of Florida Town

A threat actor remotely accessed the IT system of the water treatment facility of Oldsmar and raised the levels of sodium hydroxide in the water, an action that was quickly noticed and remediated.

A threat actor hacked into the computer system of the water treatment facility in Oldsmar, Fla., and tried to poison the town's water supply by raising the levels of sodium hydroxide, or lye, in the water supply. The attack happened just two days before NFL's Super Bowl LV was held nearby in Tampa Bay, according to local authorities.

An operator at the plant first noticed a brief intrusion Friday, Feb. 5, around 8:00 a.m., Pinellas County Sheriff Bob Gualtieri said in a press conference about the incident Monday. Someone remotely accessed the computer system the operator was monitoring that controls chemical levels in the water as well as other operations, he said.

At first the operator "didn't think much of it" because it's normal for his supervisors to use the remote access feature to monitor his computer screen at times, Gualtieri said. However, around 1:30 p.m. someone again remotely accessed the computer system and the operator observed the mouse moving around on the screen to access various systems that control the water being treated, he said.

## Lye Levels Raised at Water Treatment Plant

During the second intrusion, which lasted three to five minutes, the intruder changed the level of sodium hydroxide in the water from 100 parts per million to 11,100 parts per million, "a significant and potentially dangerous increase," Gualtieri said.

"Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners," he said. "It is used to control water acidity and remove metals from drinking water in water-treatment plants."

Fortunately, the operator quickly changed the level back to normal after the intrusion and alerted supervisors, who then contacted the Pinellas County Sheriff's Office. Gualtieri said his team notified the FBI and U.S. Secret Service and worked with them over the weekend to investigate and try to discover who was behind the attack.

At this time authorities have leads but have not identified a suspect, nor do they know if the attack came from inside the United States or outside the country, he said.

## Motive Behind Hack Remains Elusive

They also do not have a motive for the attack, although it did occur just before the Super Bowl was held in Tampa Bay on Sunday. The event can typically draw upwards of 150,000 visitors to the region but this year only about 22,000 live spectators were allowed to attend the game due to the COVID-19 pandemic.

Still, Gualtieri asked all critical infrastructure operators in the Tampa Bay area to check to ensure that their systems have the latest security protocols in place. He also stressed that despite the seriousness of the Oldsmar incident, "at no time was there a significant adverse effect on the water being treated."

"Importantly, the public was never in danger," Gualtieri said.

Even if the operator hadn't so quickly noticed the nefarious activity, he said it would have taken 24 to 36 hours for the tainted water to hit the water supply, and redundancies in the system would have tested it before then and caught the high levels of sodium hydroxide.

## At Risk: Critical Infrastructure

Still, the incident is a dire reminder of the potential catastrophic effect an attack on critical infrastructure can have on public safety, making the security of these systems a top concern, security experts said.

“With so much emphasis recently placed on hacks for the health care and financial services industry, an infrastructure hack such as this tends to hit much closer to home as it regards our physical safety,” noted Tom Garrubba, CISO of Shared Assessments, in an email to Threatpost.

Indeed, given past attacks on the U.S. critical infrastructure such as the power grid, water systems and nuclear plants, organizations in control of these systems should take the latest attack in Florida as a call to action, observed Hitesh Sheth, president and CEO at Vectra, a San Jose, Calif.-based provider of AI for detecting cyberattacks, in an e-mail to Threatpost.

“Protecting these critical facilities, and upgrading their cyber defenses, should be a far higher priority,” he said.

Some experts cited the COVID-19 pandemic for putting critical infrastructure at higher risk due to the necessity of putting remote access capabilities in place sooner than operators of these systems expected for employees forced to work remotely due to pandemic restrictions.

“Many organizations have previously felt protected by traditional perimeter security such as firewalls and VPNs,” observed Kevin Dunne, president at Greenlight, a Flemington, New Jersey-based integrated risk management firm, in an e-mail to Threatpost. “However, the new shift to work from anywhere has reduced the efficacy of many of these methods and even rendered some of them useless.”

Rather than use VPNs to secure networks, Dunne suggested that the most effective way to secure remote access is to monitor identity and access “to know exactly who is access critical systems and what they are doing with that access,” he said.

Source: *https://threatpost.com/hacker-tries-to-poison-water-supply-of-florida-town/163761/*

# 6. Yandex Data Breach Exposes 4K+ Email Accounts

In a security notice, Yandex said an employee had been providing unauthorized access to users' email accounts "for personal gain."

Yandex – one of Europe's largest internet companies – is warning of a data breach that compromised 4,887 email accounts. The breach stems from an insider threat.

Yandex is the most-used search engine in Russia – and the fifth most-popular search engine worldwide. Beyond its search engine, Yandex's internet product lineup includes email services, online advertising, app analytics and more.

The company found that a Yandex employee had been providing unauthorized access to users' mailboxes "for personal gain." This employee was one of three system administrators, who had the access privileges to provide technical support for mailboxes, said Yandex.

"A thorough internal investigation of the incident is under way, and Yandex will be making changes to administrative access procedures," said Yandex's Friday security advisory. "This will help minimize the potential for individuals to compromise the security of user data in future. The company has also contacted law enforcement."

## Yandex Internally Discovers Data Breach

Threatpost has reached out to Yandex for further comment on the timeline of the data breach – including when the unauthorized access to email accounts began, when the breach was discovered, and who was able to access the compromised accounts.

The company discovered the breach during a routine screening by its security team. Yandex stressed, no payment details were compromised, and it has already blocked the unauthorized access to the compromised mailboxes.

"We have contacted the mailbox owners to alert them about the breach and they have been informed of the need to change their account passwords," the company said.

## What is a Cybersecurity Insider Threat?

The data breach is reflective of an insider threat. This is a type of threat that comes from within an organization – whether it's an employee, former employee, contractor or otherwise. Insider threats can be non-malicious – such as a mistake by an employee (like a cloud misconfiguration) that leads personal data being exposed, for instance. Or, as in this incident, they can be malicious, where an employee purposefully gives access (or is persuaded to give access) to internal systems or records.

According to Verizon's 2020 Data Breach Investigations Report (DBIR), internal actors were behind 30 percent of breaches (with the majority, or 70 percent, coming from external actors).

## Insider Threats Have Plagued ADT, Cisco and Amazon

An insider threat could leave companies spiraling from financial or brand damage – but also a lack of subsequent trust from customers.

In a recent January case, for instance, a former ADT employee was caught adding his personal email address to the accounts of attractive women, so he could have around-the-clock access to their most private moments.

In December, a former Cisco Systems employee was sentenced to two years in jail, after hacking into the networking company's cloud infrastructure and deleting 16,000 Webex Teams accounts in 2018. And in October, Amazon fired an employee who shared customers' names and email addresses with a third party.

Brandon Hoffman, chief information security officer at Netenrich, said this incident highlights the ongoing concern related to insider threats.

"Employees are always a prime target for adversaries, whether it is targeting them to leverage their machine or identity or recruiting them actively on a closed source (dark web) forum," said Hoffman. "There has been several cases where we have seen a disgruntled employee posting messages on the dark web aiming to make a contact where they can 'cash out' their leverage as an employee. Considering this happened in Russia, a known hotspot (or even the primary hub) of cybercrime, the fact that it was an intentional insider is not all that surprising."

Source: *https://threatpost.com/yandex-data-breach-email-accounts/163960/*

# 7. Egregor ransomware affiliates arrested by Ukrainian, French police

A joint operation between French and Ukrainian law enforcement has reportedly led to the arrests of several members of the Egregor ransomware operation in Ukraine.

As reported first by France Inter, on Tuesday, law enforcement made the arrests after French authorities could trace ransom payments to individuals located in Ukraine.

The arrested individuals are thought to be Egregor affiliates whose job was to hack into corporate networks and deploy the ransomware. France Inter also reports some individuals provided logistical and financial support.

Over this past year, Egregor has attacked numerous French organizations, including Ubisoft, Ouest France, and, more recently Gefko.

The operation was reported launched through an investigation opened last fall by the Tribunal de grande instance de Paris after receiving complaints about the ransomware gang.

At this time, Egregor's Tor websites are offline, including the payment site and the operation's data leak site. With the Tor payment site inaccessible, victims are unable to contact the ransomware gang, pay a ransom, or download decryptors for previously paid ransoms.

It is not known if the problems with the ransomware gang's infrastructure are related to the law enforcement operation.

BleepingComputer.com has contacted French law enforcement but has not heard back.

## Rise and fall of Egregor

Egregor operates as a ransomware-as-a-service (RaaS) where affiliates partner with the ransomware developers to conduct attacks and split the ransom payments.

In partnerships like this, the ransomware developers are responsible for developing the malware and running the payment site. At the same time, the affiliates are responsible for hacking into victims' networks and deploying the ransomware.

As part of this arrangement, developers earn between 20-30% of a ransom payment, while affiliates make the other 70-80%.

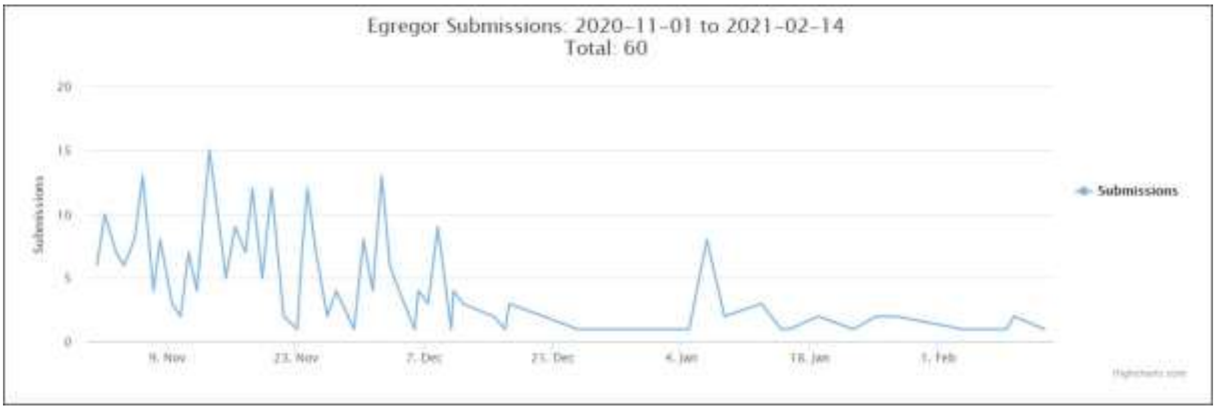
Egregor launched in the middle of September, just as one of the largest groups known as Maze began shutting down its operation.

At the time, threat actors told BleepingComputer that Maze affiliates moved to the Egregor RaaS, allowing the new ransomware operation to launch with experienced and skilled hackers.

In November, the ransomware gang partnered with the Qbot malware to gain access to victims' networks, increasing the volume of attacks even further.

Due to Egregor growing so quickly in a relatively short period, victims had to wait in a queue to negotiate a ransomware payment.

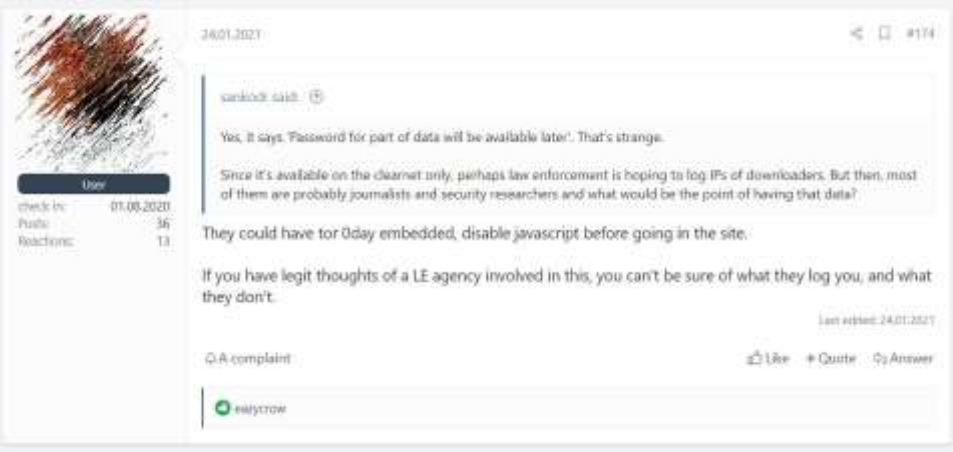
In early December, Egregor suddenly started slowing down with far fewer attacks conducted by the operation. You can see this dramatic decrease beginning on December 9th, 2020, in the graph below of Egregor submissions to ID Ransomware.



*ID-Ransomware submission stats showing a huge decline*

Last month, Bill Siegel, CEO of ransom negotiation firm Coveware, told BleepingComputer that they too had seen a decline in Egregor attacks and told us affiliates might have moved to another RaaS.

In January, Egregor's data leak site went offline for approximately two weeks, and when it came online again, there were issues with the site. This unusual activity led other threat actors to become suspicious that Egregor was hacked or breached by aw enforcement.



sankodr said:

Yes, it says 'Password for part of data will be available later'. That's strange.

Since it's available on the clearnet only, perhaps law enforcement is hoping to log IPs of downloaders. But then, most of them are probably journalists and security researchers and what would be the point of having that data?

They could have tor 0day embedded, disable javascript before going in the site.

If you have legit thoughts of a LE agency involved in this, you can't be sure of what they log you, and what they don't.

Last edited: 24.01.2021

*Hackers concerned*

Whether the decline of Egregor activity is law enforcement related or simply the ebbs and flows of ransomware operations is not currently known.

In a new report released last week by cybersecurity firm Kivu, researchers state that Egregor has amassed over 200 victims since it launched, and is comprised of 10-12 core members and 20-25 semi-exclusively vetted members.

Some of the well-known companies that have been attacked by Egregor include Barnes and Noble, Kmart, Cencosud, Randstad, Vancouver's TransLink metro system, and Crytek.

Source: *https://www.bleepingcomputer.com/news/security/egregor-ransomware-affiliates-arrested-by-ukrainian-french-police/*

## 8. Android App with 1 Billion Downloads Threatens Spying, Malware

Attackers can exploit SHAREit permissions to execute malicious code through vulnerabilities that remain unpatched three months after app makers were informed.

An Android app that's been downloaded more than 1 billion times is riddled with flaws that can let attackers hijack app features or overwrite existing files to execute malicious code, or launch man-in-the-disk (MiTD) attacks on people's devices, researchers discovered.

The flaws exist in an app called SHAREit, which allows Android app users to share files between friends or devices. They were identified and reported to the app maker three months ago by researchers at Trend Micro. However, the flaws remain unpatched, according to a report posted online Monday.

"We decided to disclose our research three months after reporting this since many users might be affected by this attack, because the attacker can steal sensitive data and do anything with the apps' permission," Echo Duan, a mobile threats analyst for Trend Micro, wrote in the report. "It is also not easily detectable."

Trend Micro also notified Google of the app's issues, which lie in several flaws in its code that too easily give third parties permissions to take over legitimate app features, overwrite existing app files or even take over Android storage shared by multiple apps to execute malicious code, he said.

## SHAREit’s Bevy of Security Bugs

“We delved into the app’s code and found that it declares the broadcast receiver as ‘com.lenovo.anyshare.app.DefaultReceiver,'” Duan explained in the post. “It receives the action ‘com.ushareit.package.action.install_completed’ and Extra Intent then calls the startActivity() function.”

Researchers built a simple proof of concept (PoC) and found that “any app can invoke this broadcast component,” he said. “This shows arbitrary activities, including SHAREit’s internal (non-public) and external app activities.”

Moreover, third-parties also can gain temporary read/write access to the content provider’s data through a flaw in its FileProvider, Duan wrote. “Even worse, the developer specified a wide storage area root path,” he wrote. “In this case, all files in the /data/data/<package> folder can be freely accessed.”

In Trend Micro’s PoC, researchers included code that reads WebView cookies, which was used to write any files in the SHAREit app’s data folder. “In other words, it can be used to overwrite existing files in the SHAREit app,” Duan said of the attack.

In this way malicious apps installed on a device running SHAREit can run take over the app to run custom code or install third-party apps without the user knowing, researchers found.

## Man-in-the-Disk Mobile Threat

SHAREit also is susceptible to an MiTD attack, a variation on a man-in-the-middle attack identified by Check Point in 2018 that arises from the way the Android OS uses two types of storage—internal and external, the latter of which uses a removable SD card and is shared across the OS and all apps.

This type of attack allows someone to intercept and potentially alter data as it moves between Android external storage and an installed app, and is possible using SHAREit “because when a user downloads the app in the download center, it goes to the directory,” Duan wrote. “The folder is an external directory, which means any app can access it with SDcard write permission.”

Researchers illustrated this action in their POC by manually copying Twitter.apk in the code to replace it with a fake file of the same name. As a result, a pop-up of the fake Twitter app appeared on the main screen of the SHAREit app, Duan wrote. Reopening SHAREit caused the fake Twitter app to appear on the screen again, prompting the user to install it, an action that is successful, according to the post.

Trend Micro’s discovery isn’t the first time serious flaws were found in SHAREit. Two years ago researchers discovered two high-severity flaws in the app that allowed an attacker to bypass the file transfer application's device authentication mechanism and ultimately download content and arbitrary files from the victim's device.

Duan recommended that people regularly update and patch mobile operating systems and the apps themselves to maintain security on their devices, as well as "keep themselves informed by reading reviews and articles about the apps they download."

Source: *https://threatpost.com/unpatched-android-app-billion-downloads-malware/163976/*

## 9. Malformed URL Prefix Phishing Attacks Spike 6,000%

Sneaky attackers are flipping backslashes in phishing email URLs to evade protections, researchers said.

Researchers from GreatHorn report they have observed a nearly 6,000-percent jump in attacks using "malformed URL prefixes" to evade protections and deliver phishing emails that look legit. They look legit, that is, unless you look closely at the symbols used in the prefix before the URL.

"The URLs are malformed, not utilizing the normal URL protocols, such as http:// or https://," researchers said in a blog post about their findings. "Instead, they use http:/\ in their URL prefix."

The slashes in the address are largely superfluous, the GreatHorn report explained, so browsers and many scanners don't even look at them.

Typosquatting is a common phishing email tactic where everyday business names are mispelled, like "amozon.com" — to try and trick unobservant users into clicking. But these days, researchers explained, most people know to look for these kinds of email scams, so threat actors have had to evolve too.

### Email Protections Ignore Backslashes in URL Prefix

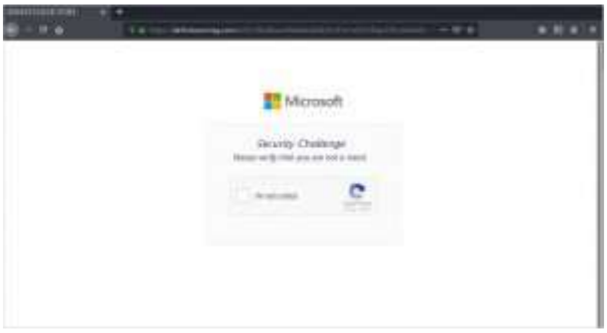
"The URLs don't fit the 'known bad' profiles developed by simple email scanning programs, allowing them to slip through undetected," researchers said. "They may also slip past human eyes that aren't accustomed to looking in the prefix for signs of suspicious activity."

The researchers reported they first noticed this new tactic last October, and said that it has been quickly gaining momentum ever since — with attacks between January and early February spiking by 5,933 percent, they said.

## What Does a Malformed URL Attack Look Like?

GreatHorn provided an example of a malformed URL phishing email with the address: “http:/\brent.johnson.australiasnationalskincheckday.org.au//exr/brent.johnson@impacteddomain.com”

The phishing email appears to be sent from a voicemail service; the researchers explained. The email contains a link to play the voice message “Play Audi Date.wav” which redirects to a malicious site, the team reported.

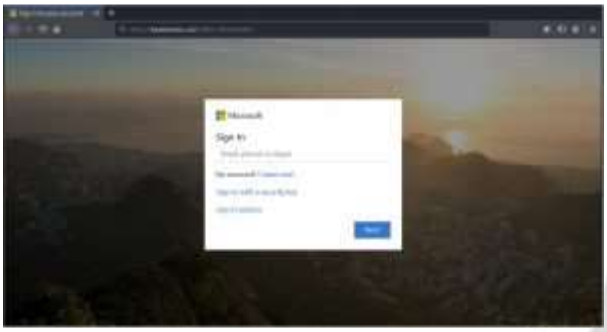


*A phishing page with a ReCAPTCHA. Source: GreatHorn.*

“The website even includes a reCAPTCHA, a common security feature of legitimate websites, showing the sophistication and subtlety of the attempted attack,” they explained.

The next page looks like an Office login page and asks for a username and password, the report said. Once entered, the attackers have control of the account credentials.

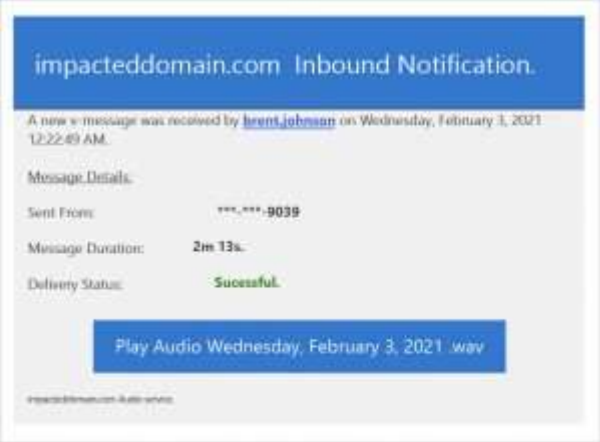
Office 365 users were far more likely to experience this type of breach, the report added, at a “much higher rate than organizations running Google Workspace as their cloud email environment.”



*A fake Microsoft sign-in page. Source: GreatHorn.*

The attackers using these malformed URLs have engaged in a variety of tactics to deliver their malware, including using a spoofed display name to impersonate the user's company internal email system; avoiding scanners searching for "known bad" domains by sending from an address with no established relationship with the business; embedding a link in phishing emails which opens a redirector domain; and using language to give the user a sense of "urgency" in the message, the report explained.

The report recommended "that security teams search their organizational email for messages containing URLs that match the threat pattern (http:/\) and remove any matches," to keep their systems protected.



impacteddomain.com Inbound Notification.

A new v-message was received by brent.johnson on Wednesday, February 3, 2021 12:22:49 AM.

Message Details.

Sent From: ***-***-9039

Message Duration: 2m 13s.

Delivery Status: Sucessful.

impacteddomain.com Audio service

*An example of an email with an "audio message" alert. Source: GreatHorn.*

Kevin O'Brien, CEO and co-founder of GreatHorn, told Threatpost that these malformed URL attacks could be mitigated through third-party solutions able to perform more nuanced analysis.

"There are a variety of API-native solutions that have come into the market in the last five years," O'Brien said. "Many of these solutions are designed to specifically address the kinds of threats that both legacy secure email gateways and platforms are incapable of analyzing or identifying, providing robust remediation options, and highlighting to users when they're about to go somewhere they don't need to go to, such as what we saw in this attack."

## Email Phishing Scams More Common, More Expensive

The report drops amid a particularly lucrative period for phishing scams. Proofpoint's recent 2020 State of the Phish showed a 14 percent jump in U.S. phishing attacks over the past year.

"Threat actors worldwide are continuing to target people with agile, relevant and sophisticated communications—most notably through the email channel, which remains the top threat vector," Alan LeFort, senior vice president and general manager of Security Awareness Training for Proofpoint said. "Ensuring users understand how to spot and report attempted cyberattacks is undeniably business-critical, especially as users continue to work remotely — often in a less secured environment. While many organizations say they are delivering security awareness training to their employees, our data shows most are not doing enough."

Source: [https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/](https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/)

-

## 10. Russian hackers linked to attack targeting Ukrainian government

The National Security and Defense Council of Ukraine (NSDC) has linked Russian-backed hackers to attempts to breach state agencies after compromising the government's document management system.

The System of Electronic Interaction of Executive Bodies (SEI EB) hacked in this attack is used by most public authorities to share documents, as the country's national security and defense agency explained.

"The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies," an advisory published earlier today says.

"The methods and means of carrying out this cyberattack allow to connect it with one of the hacker spy groups from the Russian Federation."

The Russian-linked threat actors attempted to use the document sharing system "to disseminate malicious documents," with the end goal of infecting systems belonging to Ukrainian public authorities.

Malicious documents uploaded to the SEI EB system by the attackers bundled macros designed to silently download and deploy a malware payload onto the targets' computers.

Once it infected the systems, the malware would've allowed the threat actors to control the victims' machines remotely.

"According to the scenario, the attack belongs to the so-called supply chain attacks," the NSDC added.

"It is an attack in which attackers try to gain access to the target organization not directly, but through the vulnerabilities in the tools and services it uses."

While the Ukrainian cybersecurity agency did not attribute this attack to a specific Russian APT group, it did provide indicators of compromise (IOCs) to allow security admins to detect and block future attacks using the same infrastructure.

### DDoS attacks also linked to Russian actors

On Monday, the NSDC also accused threat actors with Russian-ties of launching DDoS attacks on Ukrainian government sites, including those of the Security Service of Ukraine, and the National Security and Defense Council of Ukraine.

It is believed that Egregor threat actors launched the attacks in retaliation to arrests of alleged Egregor ransomware operation members two weeks ago.

One day after the Security Service of Ukraine (SBU) published a press release on the Egregor arrests, the SBU's website was hit by a DDoS attack and became inaccessible.

Source: *https://www.bleepingcomputer.com/news/security/russian-hackers-linked-to-attack-targeting-ukrainian-government/*

## 11. North Korean hackers target defense industry with custom malware

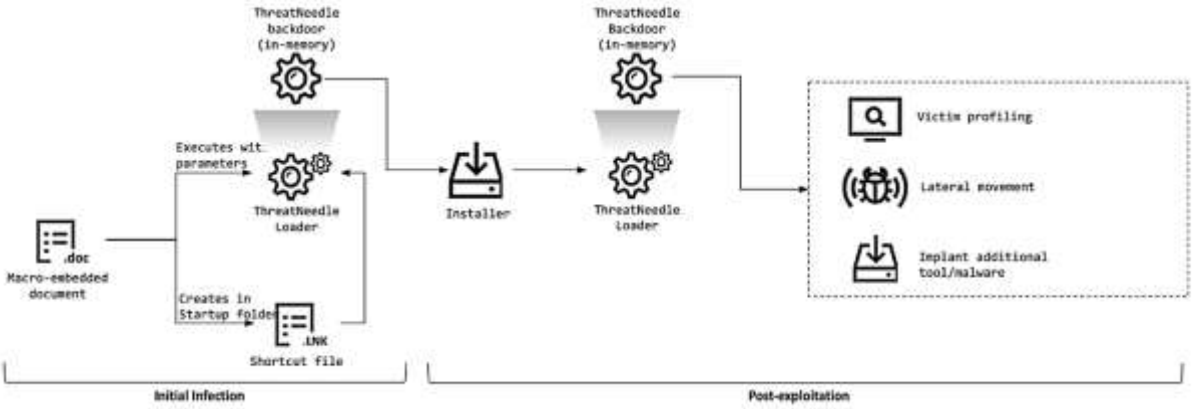
A North Korean-backed hacking group has targeted the defense industry with custom backdoor malware dubbed ThreatNeedle since early 2020 with the end goal of collecting highly sensitive information.

This espionage campaign affected organizations from more than a dozen countries and was coordinated by DPRK-backed state hackers tracked as Lazarus Group.

The attackers used COVID19-themed spear-phishing emails with malicious attachments or links as the initial access vector to the companies' enterprise network.

After the initial compromise, they installed the group's custom-made ThreatNeedle backdoor malware first used in 2018 in attacks targeting cryptocurrency businesses.

"Once installed, ThreatNeedle is able to obtain full control of the victim’s device, meaning it can do everything from manipulating files to executing received commands," Kaspersky security researchers said earlier today.



*Attack flow (Kaspersky)*

ThreatNeedle helped the Lazarus hackers to move laterally throughout the defense orgs' networks and harvest sensitive info that got exfiltrated to attacker-controlled servers using a custom tunneling tool via SSH tunnels to remote compromised South Korean servers.

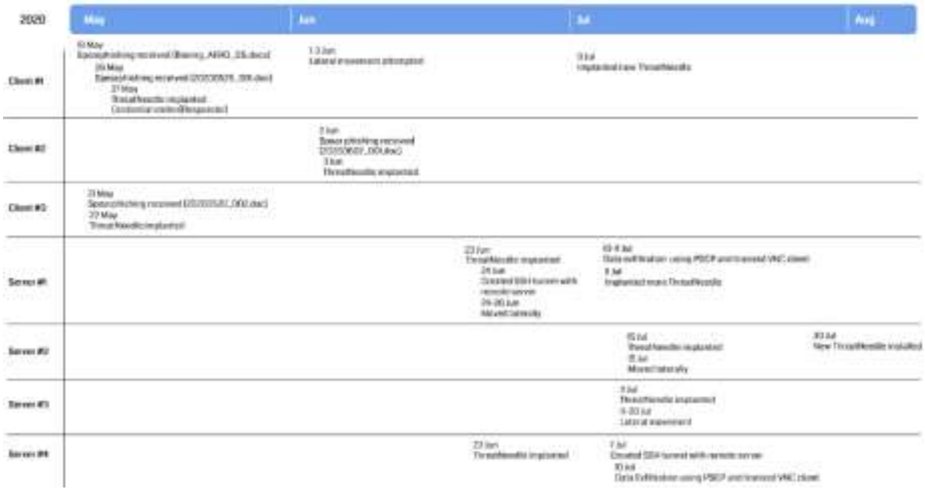
The backdoor also allowed them to bypass network segmentation and access restricted networks with mission-critical devices that didn't have Internet access.

"After gaining an initial foothold, the attackers gathered credentials and moved laterally, seeking crucial assets in the victim environment," Kaspersky added.

"We observed how they overcame network segmentation by gaining access to an internal router machine and configuring it as a proxy server, allowing them to exfiltrate stolen data from the intranet network to their remote server."

Throughout their attacks, the hackers were also seen stealing documents and data from both office IT networks (from devices used for storing business and customer info) and from restricted networks (commonly used for storing and managing highly sensitive data).

The Lazarus operators took control of administrators' workstations which later allowed them to set up malicious gateways that provided them with access to the restricted networks.


2020
May
Jun
Jul
Aug
Client #1
12 May
Spearphishing received (Boeing_AERO_SS.docx)
26 May
Spearphishing received (20200526_XXX.docx)
27 May
ThreatNeedle implanted
Credential stealer (Responder)
1-3 Jun
Lateral movement attempted
3 Jul
Implanted new ThreatNeedle
Client #2
2 Jun
Spear phishing received (20200602_XXX.docx)
3 Jun
ThreatNeedle implanted
Client #3
21 May
Spearphishing received (20200521_XXX.docx)
27 May
ThreatNeedle implanted
Server #1
23 Jun
ThreatNeedle implanted
24 Jun
Created SSH tunnel with remote server
24-30 Jun
Moved laterally
10-11 Jul
Data exfiltration using PSCP and trojanized VNC client
11 Jul
Implanted more ThreatNeedle
Server #2
15 Jul
ThreatNeedle implanted
15 Jul
Moved laterally
30 Jul
New ThreatNeedle installed
Server #3
11 Jul
ThreatNeedle implanted
11-20 Jul
Lateral movement
Server #4
23 Jun
ThreatNeedle implanted
7 Jul
Created SSH tunnel with remote server
10 Jul
Data Exfiltration using PSCP and trojanized VNC client

*Campaign timeline (Kaspersky)*

While the Lazarus Group has been known for focusing its efforts mainly on targeting worldwide financial institutions, starting with early 2020 when this campaign began, they switched their focus on "aggressively attacking" defense industry organizations.

After this move, the Lazarus hackers repurposed their ThreatNeedle malware for stealing sensitive information as part of targeted espionage attacks.

"Lazarus was perhaps the most active threat actor of 2020, and it doesn't appear that this will change anytime soon," said Kaspersky GReAT senior security researcher Seongsu Park.

"In fact, already in January of this year, Google's Threat Analysis Team reported that Lazarus had been seen using this same backdoor to target security researchers. We expect to see more of ThreatNeedle in the future, and we will be keeping an eye out."

The Lazarus hackers are also tracked as HIDDEN COBRA by the United States Intelligence Community).

They are a well-known financially motivated cybercrime group as shown by their campaigns — they hacked Sony Films as part of Operation Blockbuster in 2014 and were behind the 2017 global WannaCry ransomware campaign.

Source: [https://www.bleepingcomputer.com/news/security/north-korean-hackers-target-defense-industry-with-custom-malware/](https://www.bleepingcomputer.com/news/security/north-korean-hackers-target-defense-industry-with-custom-malware/)

# 12. T-Mobile discloses data breach after SIM swapping attacks

American telecommunications provider T-Mobile has disclosed a data breach after an unknown number of customers were apparently affected by SIM swap attacks.

SIM swap fraud (or SIM hijacking) allows scammers to take control of targets' phone numbers after porting them using social engineering or after bribing mobile operator employees to a SIM controlled by the fraudsters.

Subsequently, they receive the victims' messages and calls which allows for easily bypassing SMS-based multi-factor authentication (MFA), stealing user credentials, as well taking over the victims' online service accounts.

The criminals can then log into the victims' bank accounts to steal money, change account passwords, and even locking the victims out of their own accounts.

The FBI shared guidance on how to defend against SIM swapping following an increase in the number of SIM hijacking attacks targeting cryptocurrency adopters and investors.

## Undisclosed number of SIM swap attacks

In a data breach notice sent to impacted customers on February 9, 2021, and filed with US attorney generals' offices, T-Mobile revealed that an unknown attacker gained access to customers' account information, including personal info and personal identification numbers (PINs).

As the attackers were able to port numbers, it is not clear if they gained access to an employee's account or did it through the compromised users' accounts.

A T-Mobile spokesperson was not available for comment when contacted by BleepingComputer earlier today.

"[A]n unknown actor gained access to certain account information. It appears the actor may then have used this information to port your line to a different carrier without your authorization," T-Mobile said.

"T-Mobile identified this activity—terminated the unauthorized access, and implemented measures to protect against reoccurrence."

The information accessed by the hackers might have included customers' full names, addresses, email addresses, account numbers, social security numbers (SSNs), account personal identification numbers (PIN), account security questions and answers, date of birth, plan information, and the number of lines subscribed to their accounts.

"T-Mobile quickly identified and terminated the unauthorized activity; however we do recommend that you change your customer account PIN," the company also said.

Impacted T-Mobile customers are advised to change their account's password, PIN, as well as their security questions and answers.

T-Mobile is offering two years of free credit monitoring and identity theft detection services through Transunion's myTrueIdentity.

## Fifth data breach in four years

This is the fifth data breach disclosed by T-Mobile during the last four years, all of them being reported after hackers gained access to customers' data.

T-Mobile previously suffered from breaches in 2018 when millions of customers' info was accessed by hackers and in 2019 after exposing prepaid customers' data.

Last year, the company disclosed two more breaches, one of them in March 2020, when attackers gained access to customer and employee data.

In December 2020, T-Mobile's suffered another data breach after unknown threat actors again accessed customers' phone numbers and call records.

Update February 27, 02:44 EST: The attackers used an internal T-Mobile application to target up to 400 customers in SIM swap attack attempts, BleepingComputer has learned. No T-Mobile for Business customers were impacted during this incident.

BleepingComputer knows of at least one T-Mobile customer impacted by a SIM hijacking attack during the last month.

Source: *https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/*

# 13. Amazon Dismisses Claims Alexa 'Skills' Can Bypass Security Vetting Process

Researchers found a number of privacy and security issues in Amazon's Alexa skill vetting process, which could lead to attackers stealing data or launching phishing attacks.

Researchers warn Amazon's voice assistant Alexa is vulnerable to malicious third-party "skills" – voice assistant capabilities developed by third parties – that could leave smart-speaker owners vulnerable to a wide range of cyberattacks.

The security-threat claim is roundly dismissed by Amazon.

Researchers scrutinized 90,194 unique skills from Amazon's skill stores across seven countries. The report, presented at the Network and Distributed System Security Symposium 2021 this week, found widespread security issues that could lead to phishing attacks or the ability to trick Alexa users into revealing sensitive information.

"While skills expand Alexa's capabilities and functionalities, it also creates new security and privacy risks," said a group of researchers from North Carolina State University, the Ruhr-University Bochum and Google, in a research paper (PDF).

"We identify several gaps in the current ecosystem that can be exploited by an adversary to launch further attacks, including registration of arbitrary developer name, bypassing of permission APIs, and making backend code changes after approval to trigger dormant intents," they said.

An Amazon spokesperson told Threatpost that the company conducts security reviews as part of skill certification, and has systems in place to continually monitor live skills for potentially malicious behavior.

"The security of our devices and services is a top priority," said the Amazon spokesperson. "Any offending skills we identify are blocked during certification or quickly deactivated. We are constantly improving these mechanisms to further protect our customers. We appreciate the work of independent researchers who help bring potential issues to our attention."

## What is an Amazon Alexa Skill?

A skill is essentially an application for Alexa, made by third-party developers, which can be installed or uninstalled by users on their corresponding Alexa smartphone app. These skills have a variety of functionalities – from reading stories to children, to interacting with services like Spotify.

For developers to build a skill, they need the following elements:

- An invocation name identifying the skill

- A set of “intents,” which are the actions Alexa users must take to invoke the skill

- Specific words or phrases that users can utilize to invoke the desired intents

- A cloud-based service to accept requests and consequently act on them

- A configuration that brings the intents, invocation names and cloud-based service together, so Alexa can route the correct requests to the desired skill

Finally, before the skills can be actively made public to Alexa users, developers must submit their skills to be vetted and verified by Amazon. During this vetting process, Amazon ensures that the skills meet their policy guidelines.

For instance, Amazon makes sure that the privacy policy link for the skill is valid, and that the skill meets the security requirements needed for hosting services on external servers (by checking whether the server responds to requests that aren’t signed by an Amazon-approved certificate authority, for instance).

## Amazon’s Alexa Skill Vetting is Lacking

However, researchers said they found several glaring issues with Amazon’s skill vetting process. For one, developers can get away with registering skills that use some (but not others) well-known company names – such as Ring, Withings or Samsung. Bad actors could then leverage these fake skill brand names by sending phishing emails to users that link to the skill’s Amazon store webpage – ultimately adding an air of legitimacy to the phishing message and tricking users into handing over valuable information.

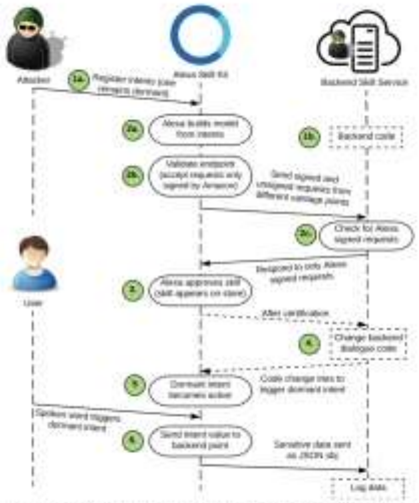

Attacker
1a. Register intents (one remains dormant)
Alexa Skill Kit
Backend Skill Service
2a. Alexa builds model from intents
1b. Backend code
2b. Validate endpoint (accept requests only signed by Amazon)
Send signed and unsigned requests from different vantage points
2c. Check for Alexa signed requests
Respond to only Alexa signed requests
3. Alexa approves skill (skill appears on store)
User
After certification
4. Change backend dialogue code
5. Dormant intent becomes active
Code change tries to trigger dormant intent
Spoken word triggers dormant intent
6. Send intent value to backend point
Sensitive data sent as JSON obj
Log data

**Fig. 5:** Workflow diagram for making backend code change to trigger a dormant intent which will contain sensitive information like phone number.

*Credit: Researchers with North Carolina State University, the Ruhr-University Bochum and Google*

Researchers said they found 9,948 skills in the U.S. skill store, for instance, that shared the same invocation name with at least one other skill – and across all skill stores, they found that only 36,055 (out of the 90,194) skills had a unique invocation name.

“This primarily happens because Amazon currently does not employ any automated approach to detect infringements for the use of third-party trademarks, and depends on manual vetting to catch such malevolent attempts which are prone to human error,” said researchers.

Another issue highlighted by researchers is that attackers can make code changes after their skills have been approved by Amazon, opening the door for various malicious intents. The issue here stems from the ability for developers to register various intents during the certificate process.

“Thus, an attacker can register dormant intents which are never triggered during the certification process to evade being flagged as suspicious,” said researchers. “However, after the certification process the attacker can change the backend code (e.g., change the dialogue to request for a specific information) to trigger dormant intents.”

In a real-world scenario, this could open the door for attackers to make code changes that could convince a user into revealing sensitive information – such as bank account details or otherwise.

## Issues With Alexa Privacy Policy Model

Researchers said that this requesting of sensitive information points to a larger overarching, conceptual (rather than technical implementation) issue.

Alexa skills can be configured to request permissions from users to access personal information from the Alexa account – such as the user’s address or contact information. However, researchers said that they uncovered instances where skills bypass the permission APIs and directly request such information from end users.

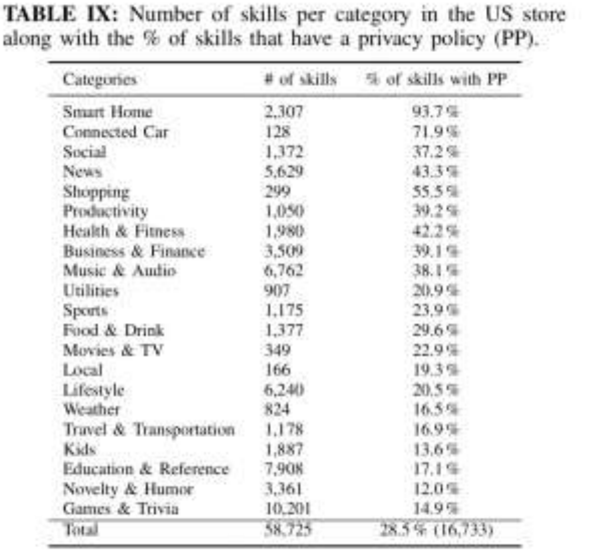


**TABLE IX:** Number of skills per category in the US store along with the % of skills that have a privacy policy (PP).

| Categories | # of skills | % of skills with PP |
|---|---|---|
| Smart Home | 2,307 | 93.7 % |
| Connected Car | 128 | 71.9 % |
| Social | 1,372 | 37.2 % |
| News | 5,629 | 43.3 % |
| Shopping | 299 | 55.5 % |
| Productivity | 1,050 | 39.2 % |
| Health & Fitness | 1,980 | 42.2 % |
| Business & Finance | 3,509 | 39.1 % |
| Music & Audio | 6,762 | 38.1 % |
| Utilities | 907 | 20.9 % |
| Sports | 1,175 | 23.9 % |
| Food & Drink | 1,377 | 29.6 % |
| Movies & TV | 349 | 22.9 % |
| Local | 166 | 19.3 % |
| Lifestyle | 6,240 | 20.5 % |
| Weather | 824 | 16.5 % |
| Travel & Transportation | 1,178 | 16.9 % |
| Kids | 1,887 | 13.6 % |
| Education & Reference | 7,908 | 17.1 % |
| Novelty & Humor | 3,361 | 12.0 % |
| Games & Trivia | 10,201 | 14.9 % |
| Total | 58,725 | 28.5 % (16,733) |

*Credit: Researchers with North Carolina State University, the Ruhr-University Bochum and Google*

Some skills, for instance, included the name of a user's specific locations as part of the invocation phrase. Researchers pointed to local news provider "Patch," which created 775 skills that include a city name. Such skills can potentially be used to track one's whereabouts, they argued.

"One could argue that this is not an issue as users explicitly provide their information, however, there may be a disconnect between how developers and users perceive the permission model," said researchers. "A user may not understand the difference between providing sensitive data through the permission APIs versus entering them verbally."

In another privacy issue, researchers found that 23.3 percent of the privacy policies viewed for skills were not fully disclosing the data types that were associated with permissions requested by a skill. For instance, 33 percent of skills accessing a user's full name did not disclose that type of data collection in their privacy policy.

## Amazon Alexa: Previous Skills Hacks

Alexa skills have come under scrutiny in the past, starting in 2018 when researchers created a proof-of-concept "rogue skill" that could eavesdrop on Alexa users – and automatically transcribe every word said.

In 2019, researchers said that vulnerabilities stemming from skills could enable what they called a "Smart Spies" hack, which allows for eavesdropping, voice-phishing, or using people's voice cues to determine passwords.

Amazon, for its part, in 2019 did make a few modifications to make this "Smart Spies" hack more difficult – However, researchers called the mitigations are "comically ineffective," saying that Amazon (and other voice assistant makers, such as Google) need to focus on weeding out malicious skills from the getgo, rather than after they are already live.

Finally, as recently as August, researchers disclosed flaws in Alexa that could allow attackers to access personal data and install skills on Echo devices.

"Our analysis shows that while Amazon restricts access to user data for skills and has put forth a number of rules, there is still room for malicious actors to exploit or circumvent some of these rules," said researchers this week. "This can enable an attacker to exploit the trust they have built with the system."

Source: *https://threatpost.com/amazon-dismisses-claims-alexa-skills-can-bypass-security-vetting/164316/*

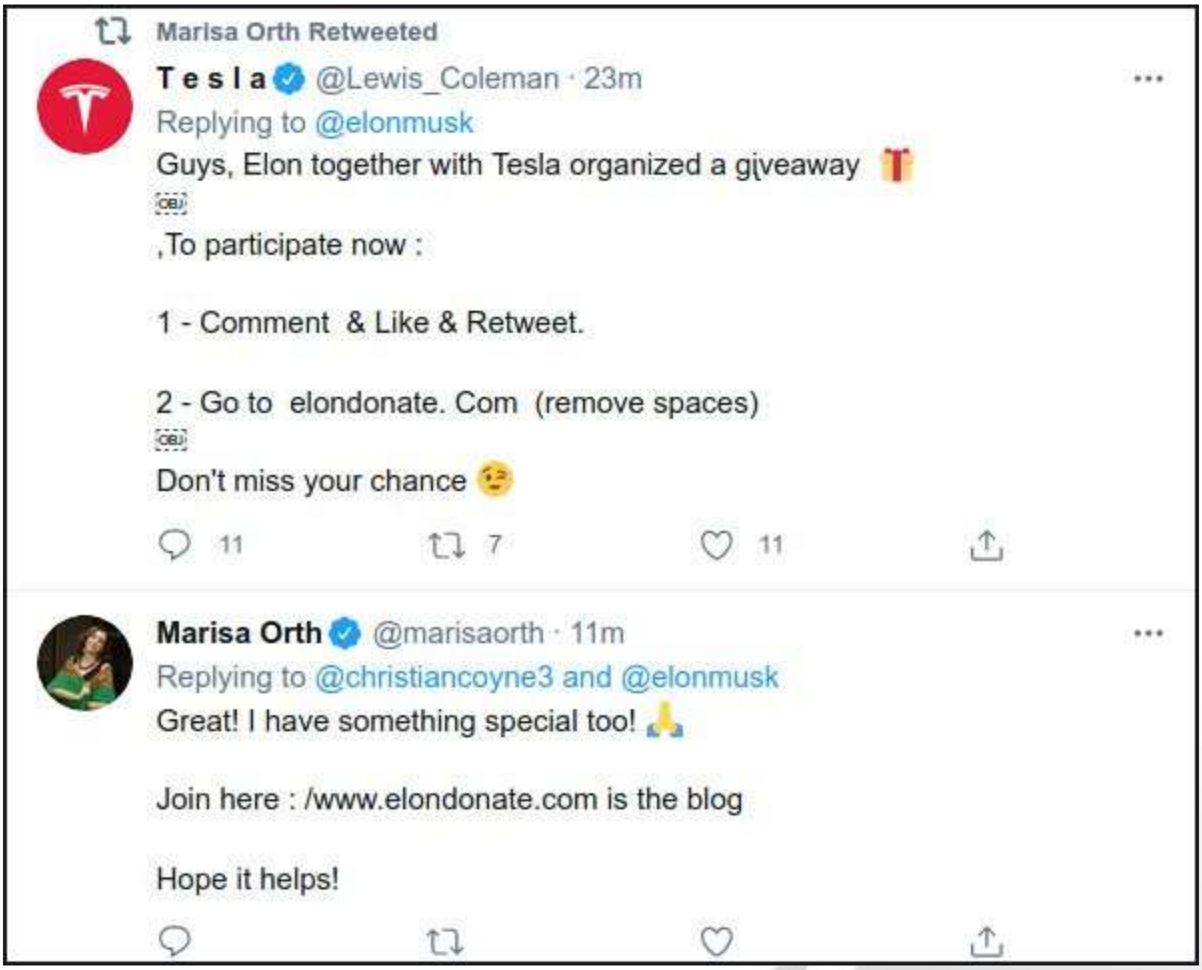
## 14. Twitter scammers earned over $145k in cryptocurrencies

Cryptocurrency scammers have made at least $145,000 this week by promoting fake giveaways through hacked verified Twitter accounts.

Last month, we reported an increasing trend where verified Twitter accounts are hacked to promote fake cryptocurrency giveaways. At the time, these scams pulled in a massive $580,000 in cryptocurrency over a one-week period.

The attackers target verified accounts with thousands, if not millions, of followers. They then tweet fake giveaway scams from well-known people or companies, such as Elon Musk, Tesla, Gemini Exchange, and more recently, Chamath Palihapitiya, and Social Capital.

When tweeting the scams, it is common to see different Twitter sock puppets talking to each other as they promote each other's tweets, as shown below.



Marisa Orth Retweeted

Tesla @Lewis_Coleman · 23m

Replying to @elonmusk

Guys, Elon together with Tesla organized a giveaway 🎁

,To participate now :

1 - Comment & Like & Retweet.

2 - Go to elondonate. Com (remove spaces)

Don't miss your chance 😉

Marisa Orth @marisaorth · 11m

Replying to @christiancoyne3 and @elonmusk

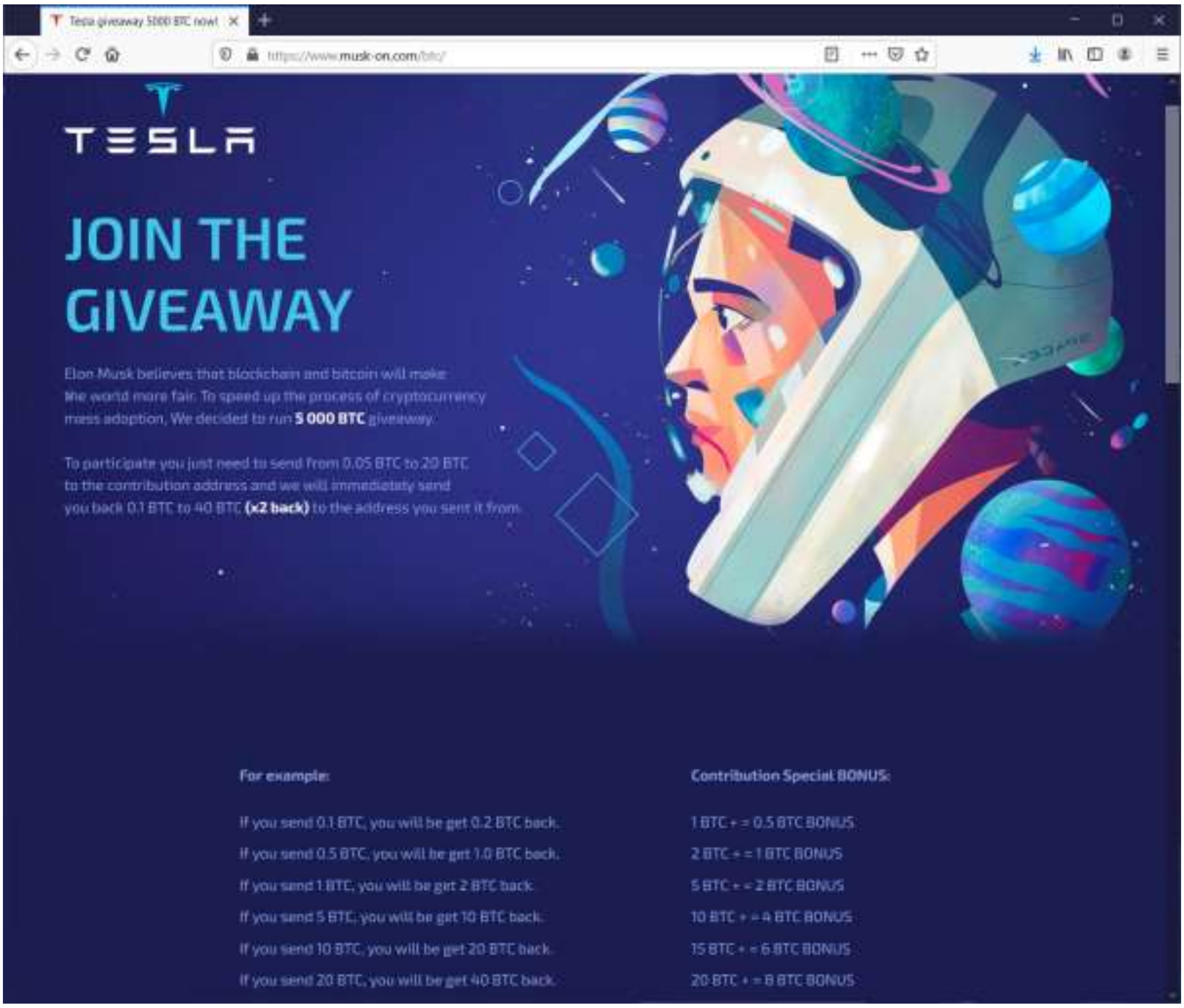
Great! I have something special too! 🙏

Join here : /www.elondonate.com is the blog

Hope it helps!

*A tweet promoting a fake Elon Musk giveaway*

Embedded in the tweets are links to sites that redirect to sites pretending to be Medium posts that promote the giveaway and include further links to the actual giveaway site, as shown below.



JOIN THE GIVEAWAY

Elon Musk believes that blockchain and bitcoin will make the world more fair. To speed up the process of cryptocurrency mass adoption, We decided to run **5 000 BTC** giveaway.

To participate you just need to send from 0.05 BTC to 20 BTC to the contribution address and we will immediately send you back 0.1 BTC to 40 BTC **(x2 back)** to the address you sent it from.

| For example: | Contribution Special BONUS: |
|---|---|
| If you send 0.1 BTC, you will be get 0.2 BTC back. | 1 BTC + = 0.5 BTC BONUS |
| If you send 0.5 BTC, you will be get 1.0 BTC back. | 2 BTC + = 1 BTC BONUS |
| If you send 1 BTC, you will be get 2 BTC back. | 5 BTC + = 2 BTC BONUS |
| If you send 5 BTC, you will be get 10 BTC back. | 10 BTC + = 4 BTC BONUS |
| If you send 10 BTC, you will be get 20 BTC back. | 15 BTC + = 6 BTC BONUS |
| If you send 20 BTC, you will be get 40 BTC back. | 20 BTC + = 8 BTC BONUS |

*Fake Tesla cryptocurrency giveaway site*

These sites tell visitors to send cryptocurrency to the listed address, and the site will send back double the amount you sent.

People continue to fall for these scams

Unfortunately, no matter how much BleepingComputer and other reporters cover these scams, people continue to fall for them.

MalwareHunterTeam, who has been monitoring these scams, has told BleepingComputer that the scammers continue to hack verified Twitter accounts with no sign of letting up.

From the list of examples MalwareHunter shared with BleepingComputer, we have determined that the scammers have made at least $145,000 this week alone.

These earnings include 1.49094148 bitcoins, with at today's high prices is equal to $70,382.16.

| Bitcoin address | Amount | USD amount |
|---|---|---|
| 1L2dzTrwrA15ZbTVWeDfznMMxQ4d9shzPm | 0 | 0 |
| 1E9GwoiRbzzEgQXk32J5ksr9FbcfGcJXuZ | 0.77457775 | $36,565.12 |
| 1CLAbY5VwBgnECbi5SQc97URaE9p1AUsNj | 0.71636373 | $33,817.04 |
| 33J8sHT2mZ7wJ6vhTssRChU3hCniZrZ6ej | 0 | 0 |
| 1Jg4oyfZqMkDDmtLss5nyaPWghowP1BpFJ | 0 | 0 |

The Ethereum giveaway scams did well for the scammers too, earning them $51,758.61.

| | | |
|---|---|---|
| {"id":"7c08b1bd-fb6e-fe13-075f-9334004c0306" | azureTenantId:"8153d5b9-7993-4a88-9cda-69a07754949e" | azureSubscriptionId:"fcdbc9bf-4b06-4b24-b5ab-4f410d12c51f" |
| | | |
| | | |
| | | |
| | | |

Finally, Dogecoin, the newcomer in cryptocurrency giveaways, generated $26,004.94.

| Ethereum address | Amount | USD amount |
|---|---|---|
| D6KkJA616qq64czYfcSLYgYLskQMT5hfj2 | 289,710.01032007 | $14,619.06 |
| D8h7ghzJ9SiT97ZAzoFAvEU7wGdufGS6BA | 199,170.62 | $10,264.18 |
| DC822cesUE5drToEnKMSstBfj9Bph4wGuc | 19,436.28 | $1,121.70 |

As many of the sites associated with these scams switch to different URLs and cryptocurrency addresses, the scammers likely made much more this week.

As these scams generate an incredible amount of money for the threat actors, they are not going away any time soon.

Therefore, everyone needs to understand that the vast majority of cryptocurrency giveaways are scams.

It is safer to treat any cryptocurrency giveaway you see online as a scam and understand that anything you send will not produce anything in return.

Source: *https://www.bleepingcomputer.com/news/security/twitter-scammers-earned-over-145k-this-week-in-bitcoin-ethereum-doge/*

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.*