



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

Monthly Security Bulletin

May 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.	Prioritizing Security in a Remote Learning Environment.....	4
2.	FBI and CISA warn of state hackers attacking Fortinet FortiOS servers	6
3.	European Commission, other EU orgs recently hit by cyber-attack.....	8
4.	Have I Been Pwned adds search for leaked Facebook phone numbers.....	9
5.	Attackers Blowing Up Discord, Slack with Malware	11
6.	1.3M Clubhouse Users' Data Dumped in Hacker Forum for Free.....	14
7.	Don't Stop At 'Delete:' How Privacy Needs Are Shaping Data Destruction	17
8.	US government confirms Russian SVR behind the SolarWinds hack.....	20
9.	Hundreds of networks reportedly hacked in Codecov supply-chain attack	22
10.	The Value of Independent Testing to Assess Your Cybersecurity Posture.....	24
11.	Emotet malware nukes itself today from all infected computers worldwide	26
12.	FBI shares 4 million email addresses used by Emotet with Have I Been Pwned..	28
13.	New stealthy Linux malware used to backdoor systems for years.....	30
14.	Microsoft Office SharePoint Targeted With High-Risk Phish, Ransomware	
	Attacks.....	32

1. Prioritizing Security in a Remote Learning Environment

Learning environments are not what they used to be, and as educational institutions deploy new technology to facilitate a safe and effective remote learning environment, their cyber vulnerabilities also increase. [Canadian schools especially have seen a rise in ransomware attacks](#) with the transition to online learning, opening the door for hackers to exploit student data and sabotage academic research. To combat the rising cybersecurity concerns, educators need to implement new measures to uphold secure and efficient distance learning environments without allowing student data and privacy to hang in the balance.

Why Education Has a Target on Its Back

Limiting disruptions remains a high priority for educators as they discover how to manage their remote classrooms. Although many teachers are familiar with supplemental technologies such as tablets and online programs, it's another matter entirely to be completely dependent on them to support a fully virtual classroom. When investing in online learning tools, educational institutions should not allow their concern for efficiency to overshadow an equally important requirement: safety.

The education sector has seen its fair share of cybersecurity attacks since the widespread shift to remote classrooms. According to Microsoft, the [global education industry](#) has the most malware attacks, even more than prominent industries such as business, finance, and healthcare. K-12 schools especially have experienced an uptick in [ransomware and Distributed Denial of Service \(DDoS\)](#). Many [Canadian schools](#) are experiencing cyber security incidents, damaging the integrity of their student data and privacy. With hackers consistently seeking to take advantage of the [vulnerabilities in new technology](#), this prompts further discussion into why education is such a highly targeted industry.

The rapid shift to remote learning is an obvious culprit for the increasing threat level, but higher education institutions were already vulnerable before the pandemic. Many students simply lack the proper security awareness when using their online devices. In [Morphisec's CyberSecurity Threat Index](#), more than 30% of higher education breaches were caused by students falling victim to email scams, misusing social media, or other careless online activities. Budgetary constraints are also to blame for increasing online attacks, as many schools lack adequate funding to support a robust cybersecurity infrastructure. Cybercriminals recognize the vast amount of student data that schools have on record, and this incentivizes them further to infiltrate their systems.

Many of the new remote learning technologies introduced during the pandemic have exposed the risks associated with a lack of stringent security measures. For example, until recently, [Agora's](#) video conferencing software exhibited a vulnerability that would have

allowed hackers to spy on video and audio calls. With a growing number of students accessing remote learning technologies through their schools' networks, it's especially critical for schools to re-evaluate their security protocols to safeguard their students.

Safeguarding the Virtual Classroom

Schools at all levels need to proactively secure their digital technologies and safeguard their students' data integrity. With the right approach, students and educators can mitigate the risks of cyber threats. Here are four critical cybersecurity steps that schools should take immediately:

Enforce User Awareness Training

It only takes one person to allow a hacker to infiltrate a school system. Digital security training is a must to ensure that students and faculty can recognize and take the appropriate action for suspicious activities like phishing emails. For example, a common cyber threat is when hackers pose as school officials asking for important information such as tax information or identification information.

Since many of the learning technologies on the market are new to students and staff, it's especially critical to understand the implications of a security breach and the necessary steps to mitigate risks.

User Access Control

The principle of "least privilege" can also help avoid a cyber attack. This principle only allows users access to data and systems on a need-to-know basis and can mitigate data breaches that occur via unauthorized or unnecessary access. Hackers often try to infiltrate lower-level devices and accounts as a way to gain access to higher-value accounts and systems. Schools can take action by optimizing a list of what users have access to, which functions they have access to, and why. Ensuring that users have access to only what they need will limit attacks to smaller areas of the system and help protect the security ecosystem as a whole.

Update Security and Password Management Policies

An often overlooked but critical cybersecurity protocol is having a robust password management policy. These policies must also be in accordance with provincial and territorial legislation, which set guidelines and rules that govern how students and faculty use their devices and online learning technologies. Password management policies that encourage strong passwords and multi-factor authentication are essential to prevent password sharing and unrestricted access.

Third Party Vendor Management

Third-party technology vendors have become an integral component of distance learning, but they are also a vulnerability. Educational institutions need to ensure that they are properly managing their technology vendors so their students' safety is prioritized above all else. Undergoing a thorough vetting process to evaluate third-party technology, as well as vendors' terms and conditions, will help identify any security gaps that can create greater issues down the road.

Make Distance Learning Safe Learning

The ascendance of distance learning during the pandemic has given educators, students, and parents new insights into both the opportunities and challenges of not being in a physical classroom. One of the most critical is the importance of creating safe and secure virtual environments to ensure that students are safe. Despite the benefits that education technology provides, without proper training or technical safeguards in place, schools and students are left vulnerable to the dangers of external threats. By enhancing awareness of cyber threats and implementing a strong security strategy, educators and parents can start creating safer learning environments for students to thrive.

Source: <https://www.mcafee.com/blogs/consumer/prioritizing-security-in-a-remote-learning-environment/>

2. FBI and CISA warn of state hackers attacking Fortinet FortiOS servers

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) warn of advanced persistent threat (APT) actors targeting Fortinet FortiOS servers using multiple exploits.

In the Joint Cybersecurity Advisory (CSA) published today, the agencies warn admins and users that the state-sponsored hacking groups are "likely" exploiting Fortinet FortiOS vulnerabilities CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591.

The attackers are enumerating servers unpatched against CVE-2020-12812 and CVE-2019-5591, and scanning for CVE-2018-13379 vulnerable devices on ports 4443, 8443, and 10443.

Compromised servers may be used in future attacks

The APT group may use abuse these security bugs in the future to breach the networks of government, commercial, and technology services. Once they gain infiltrate the targets' networks, they might use this initial access for future attacks.

"The APT actors may be using any or all of these CVEs to gain access to networks across multiple critical infrastructure sectors to gain access to key networks as pre-positioning for follow-on data exfiltration or data encryption attacks," the joint advisory reads [PDF].

"APT actors may use other CVEs or common exploitation techniques—such as spearphishing—to gain access to critical infrastructure networks to pre-position for follow-on attacks."

"APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns."

The FBI and CISA have also shared mitigation measures to block compromise attempts in these ongoing state-sponsored attacks.

Fortinet exploits used to hack US election support systems

In November 2020, a threat actor shared a list of one-line CVE-2018-13379 exploits that could be used to steal VPN credentials from almost 50,000 Fortinet VPN servers, including governments and banks.

State hackers also abused the CVE-2018-13379 vulnerability in the Fortinet FortiOS Secure Socket Layer (SSL) VPN to compromise U.S. election support systems reachable over the Internet.

In September 2020, Microsoft warned of Russian, Chinese, and Iranian APT actors targeting the 2020 US elections.

Microsoft's report confirmed US govt intelligence shared last year on Russian, Iranian, and Chinese hackers trying to "compromise the private communications of U.S. political campaigns, candidates and other political targets."

Earlier this year, Fortinet fixed multiple severe vulnerabilities impacting its products, including Remote Code Execution (RCE), SQL Injection, and Denial of Service (DoS) bugs affecting FortiProxy SSL VPN and FortiWeb Web Application Firewall (WAF) products.

Source: <https://www.bleepingcomputer.com/news/security/fbi-and-cisa-warn-of-state-hackers-attacking-fortinet-fortios-servers/>

3. European Commission, other EU orgs recently hit by cyber-attack

The European Commission and several other European Union organizations were hit by a cyberattack in March, according to a European Commission spokesperson. As revealed by the spokesperson, the "IT security incident" impacted multiple EU institutions, bodies, or agencies' IT infrastructure.

"We are working closely with CERT-EU, the Computer Emergency Response Team for all EU institutions, bodies and agencies and the vendor of the affected IT solution," the spokesperson told BleepingComputer.

"The Commission has set up a 24/7 monitoring services and is actively taking mitigating measures."

No "major information breach" was detected so far, although forensic analysis of the intrusion attempts is still in the initial phase, and no conclusive information is available.

"Let me use this occasion to recall that we take cybersecurity very seriously and apply strict policies to protect our infrastructures and devices, the spokesperson added. "We investigate every incident."

No information is available at the moment about the nature of the incident or the identity of the attackers behind the attack.

Although not confirmed by the European Commission spokesperson, Bloomberg reported earlier that the attack hit the EU organizations last week.

Other EU orgs were also targeted – in last month, the European Banking Authority (EBA) had to take down all email systems after their Microsoft Exchange Servers were breached as part of the ongoing attacks targeting commercial and government organizations worldwide.

In January, the European Medicines Agency (EMA) said that Pfizer/BioNTech COVID-19 vaccine data stolen from its servers in December was leaked online.

In a subsequent update, EMA revealed that some of the vaccine candidate data was doctored by threat actors before being leaked online to undermine the public's trust in COVID-19 vaccines.

IBM X-Force researchers also warned in December of threat actors targeting organizations associated with the COVID-19 vaccine cold chain, including the European Commission's Directorate-General for Taxation and Customs Union.

Source: <https://www.bleepingcomputer.com/news/security/european-commission-other-eu-orgs-recently-hit-by-cyber-attack/>

4. Have I Been Pwned adds search for leaked Facebook phone numbers

Facebook users can now use the *Have I Been Pwned* data breach notification site to check if their phone number was exposed in the social site's recent data leak.

Last weekend, a threat actor released a data leak containing information for 533 million Facebook users. This information includes phone numbers and Facebook IDs for almost all exposed accounts and other optional information such as a member's name, gender, relationship status, location, occupation, date of birth, and email address.

This data was initially collected in 2019 and sold privately at the time. Over time, the data was traded and sold between different threat actors for lower and lower prices until it was eventually released for free on the hacker forum this weekend.

When it was released, the data was added to the *Have I Been Pwned* data breach notification service so that users can look up whether their emails were in the Facebook data leak.

However, this leak's main component is a Facebook user's phone number, rather than an email address, and thus *Have I Been Pwned* could not accurately alert a user if they were exposed in the breach.

"There's over 500M phone numbers but only a few million email addresses so >99% of people were getting a "miss" when they should have gotten a "hit," *Have I Been Pwned* creator Troy Hunt explained in a blog post.

To more accurately alert users, Hunt has updated *Have I Been Pwned* so that users can now search for their phone numbers on the site to determine if the leak exposed their Facebook info.

When searching for phone numbers, users must include their country code as that is how the data leak stored the number.

For example, if you wanted to check if your phone number was part of the Facebook data leak, you would need to use a search in the format '19175555555.' If you are in the UK, you would need to include your country code as well, so a searchable phone number format would be '+442071838750.'

Hunt states that the + symbol is optional and will be stripped when searching, as shown below.

1917/XXXXXX/XXXXXX
pwned?

Oh no — pwned!

Pwned in 1 data breach (subscribe to search sensitive breaches)

i

3 Steps to better security

[Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

f
t
b
p
[Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Facebook: In April 2021, a large data set of over 500 million Facebook users was made freely available for download. Encompassing approximately 20% of Facebook's subscribers, the data was allegedly obtained by exploiting a vulnerability Facebook advises they rectified in August 2019. The primary value of the data is the association of phone numbers to identities; whilst each record included phone, only 2.5 million contained an email address. Most records contained names and genders with many also including dates of birth, location, relationship status and employer.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, Names, Phone

With this new feature added, *Have I Been Pwned* has become a valuable tool for Facebook members to determine if the data leak exposed their data.

Unfortunately, when data leaks such as this one are released, it is common for other threat actors to use this information in their own attacks.

If your data was exposed, you should be on the lookout for Facebook phishing emails or smishing (phishing texts) attacks that attempt to harvest more information from you.

Source: <https://www.bleepingcomputer.com/news/security/have-i-been-pwned-adds-search-for-leaked-facebook-phone-numbers/>

5. Attackers Blowing Up Discord, Slack with Malware

One Discord network search turned up 20,000 virus results, researchers found.

Workflow and collaboration tools like Slack and Discord have been infiltrated by threat actors, who are abusing their legitimate functions to evade security and deliver info-stealers, remote-access trojans (RATs) and other malware.

The pandemic-induced shift to remote work drove business processes onto these collaboration platforms in 2020, and predictably, 2021 has ushered in a new level of cybercriminal expertise in attacking them.

Cisco's Talos cybersecurity team said in a report on collaboration app abuse this week that during the past year threat actors have increasingly used apps like Discord and Slack to trick users into opening malicious attachments and deploy various RATs and stealers, including Agent Tesla, AsyncRAT, Formbook and others.

"One of the key challenges associated with malware delivery is making sure that the files, domains or systems don't get taken down or blocked," Talos researchers explained in their report. "By leveraging these chat applications that are likely allowed, they are removing several of those hurdles and greatly increase the likelihood that the attachment reaches the end user."

Content Delivery Network Abuse

The researchers explained that Slack, Discord and other collaboration app platforms use content delivery networks (CDNs) to store the files shared back and forth within channels. As an example, Talos uses the Discord CDN, which is accessible by a hardcoded CDN URL from anywhere, by anyone on the internet.

"This functionality is not specific to Discord. Other collaboration platforms like Slack have similar features," Talos reported. "Files can be uploaded to Slack, and users can create external links that allow the files to be accessed, regardless of whether the recipient even has Slack installed."

The trick, the team said, is to get users to click on a malicious link. Once it has evaded detection by security, it's just a matter of getting the employee to think it's a genuine business communication, a task made easier within the confines of a collaboration app channel.

This also means attackers can deliver their malicious payload to the CDN over encrypted HTTPS, and that the files will be compressed, further disguising the content, according to Talos. Over the past year, they observed many common compression algorithms being used, including .ACE, .GZ, .TAR and .ZIP, and several less common types, like .LZH.

"In most cases, the [messages] themselves are consistent with what we have grown accustomed to seeing from malspam in recent years," Talos said. "Many of the [messages] purport to be associated with various financial transactions and contain links to files claiming to be invoices, purchase orders and other documents of interest to potential victims."

Messages were delivered by attackers in several languages, including English, Spanish, French, German and Portuguese, they added.

CDNs are also handy tools for cybercriminals to deliver additional bugs with multi-stage infection tactics. The researchers saw this behavior across malware, adding that one Discord CDN search turned up almost 20,000 results in VirusTotal.

"This technique was frequently used across malware distribution campaigns associated with RATs, stealers and other types of malware typically used to retrieve sensitive information from infected systems," the Talos team explained.

The team used this screenshot to illustrate this type of attack on Discord, showing a first-stage malware tasked with fetching an ASCII blob from a Discord CDN. The data from the Discord CDN is converted into the final malicious payload and injected remotely, the report said.

"As is common with Remcos infections, the malware communicated with a command-and-control server (C2) and exfiltrated data via an attacker-controlled DNS server," the report added. "The attackers achieved persistence through the creation of registry run entries to invoke the malware following system restarts."

In another campaign using AsyncRAT, the malware downloader looked like a blank Microsoft document, but when opened used macros to deliver the bug.

Discord API Used for C2 Communications

The Discord API has turned into an effective tool for attackers to exfiltrate data from the network. The C2 communications are enabled through webhooks, which the researchers explained were developed to send automated messages to a specific Discord server, which are frequently linked with additional services like GitHub or DataDog.

"Webhooks are essentially a URL that a client can send a message to, which in turn posts that message to the specified channel — all without using the actual Discord application," they said. The Discord domain helps attackers disguise the exfiltration of data by making it look like any other traffic coming across the network, they added.

"The versatility and accessibility of Discord webhooks makes them a clear choice for some threat actors, according to the analysis: "With merely a few stolen access tokens, an attacker can employ a truly effective malware campaign infrastructure with very little effort. The level of anonymity is too tempting for some threat actors to pass up."

This communication flow can also be used to alert attackers when there are new systems available to be hijacked, and delivers updated information about those they've already infiltrated, Talos said.

Ransomware and Discord

The team also observed campaigns associated with Pay2Decrypt LEAKGAP ransomware, which used the Discord API for C2, data exfiltration and bot registration, in addition to Discord webhooks for communications between attacker and systems.

"Following successful infection, the data stored on the system is no longer available to the victim and the following ransom note is displayed," the report said. They provided a screenshot of the ransom note received by users after infection:

Discord generates an alphanumeric string for each user, or access token, according to Talos, which attackers can steal to hijack accounts, they added they saw this frequently targeting online gaming.

"At the time of writing, Discord does not implement client verification to prevent impersonation by way of a stolen access token," according to Talos. "This has led to a large amount of Discord token-stealers being implemented and distributed on GitHub and other forums. In many cases, the token stealers pose as useful utilities related to online gaming, as Discord is one of the most prevalent chat and collaboration platforms in use in the gaming community."

These accounts are then used to anonymously deliver malware and for social-engineering purposes, they add.

How to Mitigate the Collaboration App Threat

The solutions, much like the threats themselves, need to be multi-faceted, according to experts. But the primary responsibility to put more security in place is on the platforms themselves, according to Oliver Tavakoli, CTO of Vectra.

"This trend will continue until suppliers of such collaboration tools put more effort into providing more policy controls to lock down the environment and add more telemetry to monitor it," Tavakoli told Threatpost. "It will also require security vendors to step up and use the telemetry to detect and block attacks within these communication channels."

On the business side, Mark Kedgley, CTO at New Net Technologies, recommends focusing on user privileges.

"To mitigate the risks, more focus on least privilege is needed, as it's still too common for users to run with local admin rights," Kedgley recommended. "Email and office applications provide a number of hardened settings to combat malware and phishing;

however, not enough organizations make use of them. Change control and vulnerability management as core security controls should be in place as well.”

But fundamentally, how can any business or any user be expected to stay on top of the glut of communications channels today’s workers are feverishly trying to maintain? Simplification is one way to narrow the attack surface and make it reasonable for users to be mindful of the security of their interactions, Chris Hazelton with Lookout advised.

“Most organizations have too many communication tools: email, collaboration and messaging platforms, web conferencing chats, and text messages on phones and tablets,” Hazelton said. “This means users are overwhelmed as they communicate with different or sometimes the same people across multiple platforms. This leads to lesser awareness of risks in sharing across collaboration platforms and other communications tools.”

Source: <https://threatpost.com/attackers-discord-slack-malware/165295/>

6. 1.3M Clubhouse Users’ Data Dumped in Hacker Forum for Free

Clubhouse, the startup invitation-only chat app, is the latest social-media platform to see mammoth troves of user data collected and posted in underground forums. An SQL file containing the personal data of 1.3 million Clubhouse users has been posted in a hacker forum for free.

Names, user IDs, photo URL, number of followers, Twitter and Instagram handles, dates that accounts were created and even the profile information of who invited them to the app are among the information contained in the database, according to CyberNews, giving threat actors key information which can be used against victims in phishing and other socially engineered scams.

For its part, Clubhouse said that its users’ data being public isn’t a bug, it’s just how the platform is built:

The company isn’t supplying any other details and Clubhouse didn’t respond to Threatpost’s request for additional comment.

Clubhouse followers on Twitter were quick to note the statement points out a difference without any distinction to its exposed users.

“I fail to see what is false ... ” user Benjamin Maynard responded to the Clubhouse statement.

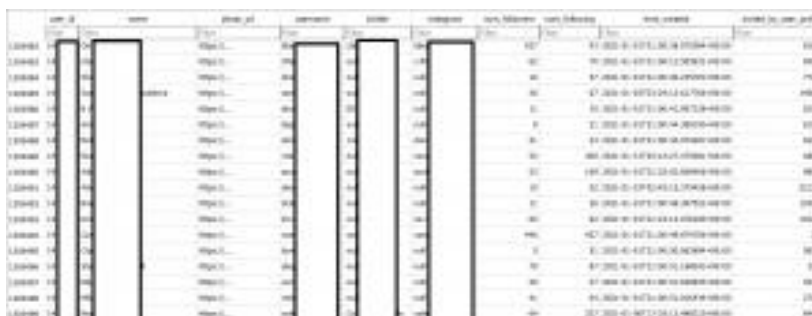
Leaky APIs Plague Social Media

Clubhouse’s terms of service prohibit data scraping, yet its API, by its own admission, is sitting online with no protection against it.

“Clubhouse has conflicting user policies – being an invite-only platform and at the same time free-for-all user data,” Setu Kulkarni, vice president with WhiteHat Security said. “All it takes is one user to figure out the API for such large data egress of the millions of users on the platform.”

Kulkarni added that these platforms need to shift to an API-first security strategy.

“Testing APIs in production is as if not more important than ever for not just vulnerabilities but also for business logic flaws that can result in unfettered access to user data,” he said.



user_id	name	phone_no	email	address	password	city	state	country	created_at	updated_at
1	John Doe	1234567890	john.doe@example.com	123 Main St	password123	New York	NY	USA	2020-01-01 12:00:00	2020-01-01 12:00:00
2	Jane Smith	9876543210	jane.smith@example.com	456 Elm St	password456	Los Angeles	CA	USA	2020-01-02 15:30:00	2020-01-02 15:30:00
3	Bob Johnson	5678901234	bob.johnson@example.com	789 Oak St	password789	Chicago	IL	USA	2020-01-03 09:15:00	2020-01-03 09:15:00
4	Alice Brown	2345678901	alice.brown@example.com	101 Pine St	password101	San Francisco	CA	USA	2020-01-04 18:45:00	2020-01-04 18:45:00
5	Charlie Davis	8901234567	charlie.davis@example.com	202 Cedar St	password202	Seattle	WA	USA	2020-01-05 11:20:00	2020-01-05 11:20:00

The Clubhouse database. Source: CyberNews.

CyberNews researcher Mantas Sasnauskas analyzed the Clubhouse data and said the privacy bug is built into the platform itself.

“The way the Clubhouse app is built lets anyone with a token, or via an API, to query the entire body of public Clubhouse user profile information, and it seems that token does not expire,” Sasnauskas said.

The CyberNews team added that the SQL file posted in the hacker forum only has Clubhouse-related information and doesn’t include “sensitive data like credit-card details or legal documents.”

Denying the Problem

In the past two weeks, 533 million Facebook users’ data was leaked, LinkedIn saw scraping of 500 million people’s data and now Clubhouse has given up the information on another 1.3 million people.

And as Politico Europe’s Nicholas Vinocur pointed out, they’ve all followed an eerily similar disclosure playbook: deny it ever happened.

Facebook was similarly vulnerable through their API, which Michael Isbitski from Salt Security told Threatpost is becoming more common.

“Content scraping is a common attack pattern,” Isbitski said in the wake of the Facebook leak. “Organizations often build or integrate APIs, without fully considering the abuse cases of the APIs.”

LinkedIn also out a statement in the wake of its incident, explaining the platform wasn’t technically “breached,” but that the information was public and scraped from the LinkedIn site.

To view the LinkedIn user data file in the hacker forum, it costs \$2 worth of forum credits. The full database was up for auction in the four-figures range.

“We have investigated an alleged set of LinkedIn data that has been posted for sale and have determined that it is actually an aggregation of data from a number of websites and companies” that includes “publicly viewable member-profile data that appears to have been scraped from LinkedIn,” the company said in a statement. “This was not a LinkedIn data breach, and no private member account data from LinkedIn was included in what we’ve been able to review.”

Data Scraping Fallout

“I don’t expect that this will be the last of these sort of scraping incidents,” Isbitski predicted. “APIs are regularly the vehicle for functionality and data. Social media companies inherently design their platforms to be consumable, powering much of it with APIs. Attackers know this, and they continue to target APIs in scraping attacks, repurposing publicly available data for malicious purposes”

Users of all three of these social media platforms should be aware they could be targeted by email phishing campaigns, so strong passwords and multi-factor authentication are important. CyberNews offers a personal data leak checker to help users figure out if their data was compromised.

Source: <https://threatpost.com/clubhouse-users-data-hacker-forum/165354/>

7. Don't Stop At 'Delete:' How Privacy Needs Are Shaping Data Destruction

It's just part of the job: at some point in a device's lifecycle, data must be destroyed. While deleting files may mean users and apps can't access them, simple deletion isn't enough to truly destroy the data. To be most effective, secure data destruction has to be complete. This is especially true when your organization needs to stay compliant with changing local and global [data privacy](#) regulations.

What is Data Destruction? It Isn't Always Common Sense

[ZDNet](#) reported 59% of hard drives sold used or refurbished on online marketplaces contained data from the previous owner, including data that had been 'deleted' and easily recovered. In some cases, the drive had been reformatted but data was still recoverable.

"The drives contained a wide array of data, from including employment and payroll records, family and holiday photos (along with intimate photos and sexualized content), business documents, visa applications, lists of passwords, passport and driver's license scans, tax documents, bank statements and lists of students attending senior high schools," the article reports.

This level of data recovery on retired or re-instituted electronic equipment is never acceptable. However, it is even less so in enterprise settings. This is especially true now that a growing list of data privacy regulations dictates the way organizations approach data storage, transmission, sharing and destruction. You need to know where all your data lives so nothing lingers for a potential breach. In addition, you should conduct an audit to ensure that data is not lingering on third-party systems when it is time for data destruction.

Knowing Your Data

Before you destroy your data, you need to know your data. Where are all of the possible places it lives? In addition, you need to know which pieces of data are the most sensitive for both the organization and customers.

With data privacy laws, consumers have more control over their personal data than organizations do. They get to decide if they want to be forgotten or how they want their data used. You have to be able to oblige. The right to be forgotten is now part of the data destruction process, making it vital that the cybersecurity team knows everywhere data is stored. Don't forget paper files, virtual formats or individual devices and drives.

Conducting a data audit will provide a clear picture of where your data is and how it is used. You are also responsible for any third party using your data, so the audit can help identify how spread out your information is.

Have a Data Destruction Policy in Place

Even as you destroy data, you are still responsible for protecting it from compromise or theft. Bringing hardware to the end of its lifecycle is just as important as onboarding devices. It requires careful planning and a clear process.

That process begins with any typical data compliance. Some regulations have restrictions on how long you can store data, so your data destruction may need to take place at regular intervals. This can include determination on whether just data is being eliminated or if the hardware is also at end of life.

Create a budget for end-of-life data and hardware. There are tools and software to assist with permanent data deletion and hardware destruction. This is not an area to try to save a few bucks; if the data is recoverable and breached, you will pay the penalty.

Have a team in charge of determining end-of-life for both data and hardware. Additionally, make it clear to employees what the process is. If employees are using personal devices to access company data that is going to be destroyed, their devices will have to be scrubbed. They can't just hit 'delete' and consider it done.

Staying Compliant

Once you know where all sensitive data is and your destruction processes are in place, the next step is to make sure you are following any data privacy compliance laws for your industry and location.

The European Union's General Data Protection Regulation (GDPR), for example, classifies data destruction as a method of data processing and requires organizations to follow certain steps before destroying anything. Owners of the data have the ultimate say over their data, even when it comes to destruction. Additionally, data on end-of-life devices [must be completely erased](#) and not just deleted. Destroy hardware in such a way that it can no longer be used (i.e., magnetic strips removed or devices physically destroyed or shredded).

Most — but not all — states have laws surrounding destruction of data.

According to the [National Conference of State Legislatures](#), "at least 35 states, D.C. and Puerto Rico have enacted laws that require either private or governmental entities or both to destroy, dispose, or otherwise make personal information unreadable or indecipherable."

Also, the [Federal Trade Commission](#) requires any business or individual that uses a consumer report for business purposes must dispose of that data under strict guidelines. Paper records, for instance, must be burned, pulverized or shredded, while electronic files must be erased or destroyed so the consumer data can't be read nor reconstructed.

Also, [industry compliance regulations](#) have their own sets of instructions for how data should be destroyed.

Failure to follow the correct procedures can result in a data breach, which results in financial consequences for the company and puts consumers at risk for identity theft and fraud.

Tools for Data Destruction

If you can afford the equipment, it is safer to keep the destruction process within the company. There are also companies that will outsource data and hardware destruction, but this adds risk of a data breach. You can acquire shredders to destroy hardware, or physically destroy a device with an old-fashioned hammer. Degaussing wipes clean magnetic strips, and degausser machines can be purchased for in-house use.

Data privacy regulations have put heightened attention on consumer information and how it is used — and how it is destroyed. Recognizing that destruction is simply part of the data protection process should keep the data secure through the entire lifecycle and keep your organization compliant.

Clients are responsible for ensuring their own compliance with various laws and regulations. IBM does not provide legal advice and does not represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Source: <https://securityintelligence.com/articles/data-destruction-beyond-delete-for-privacy-law-compliance/>

8. US government confirms Russian SVR behind the SolarWinds hack

The United States government is formally accusing the Russian government of the SolarWinds supply-chain attack that gave hackers access to the network of multiple U.S. agencies and private tech sector companies.

In a brief announcing sanctions on Russia for actions against the U.S. interests, the White House is naming the Cozy Bear group of advanced hackers as the author of the cyber espionage activity exploiting the SolarWinds Orion platform.

Loud and clear attribution

The press release from the White House confirms past media reports citing unofficial sources that the Russian Foreign Intelligence Service, the SVR, was behind the SolarWinds hack.

In early January, the Cyber Unified Coordination Group (UCG) attributed the attack to a Russian-backed hacker group, without giving a specific name.

Today, the White House officially blames the SVR for carrying out “the broad-scope cyber espionage campaign” through its hacking division commonly referred to as APT29, The Dukes, or Cozy Bear.

“The U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR,” notes the brief from the White House.

By compromising the SolarWinds software supply chain, the SVR had access to more than 16,000 computers across the world. However, the campaign targeted only select targets, such as companies in the cybersecurity sector (FireEye, Malwarebytes, Mimecast) and state and federal agencies in the U.S.

“The scope of this compromise is a national security and public safety concern. Moreover, it places an undue burden on the mostly private sector victims who must bear the unusually high cost of mitigating this incident” - the U.S. White House

In a joint cybersecurity advisory, the U.S. National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) are warning about the top five vulnerabilities the SVR is exploiting in attacks against the U.S. interests.

Organizations should heed the warning and take the necessary steps to identify and defend against malicious activity conducted by the SVR.

Russian companies sanctioned

President Biden has issued an executive order today on blocking property with regards to harmful activities from the government of the Russian Federation.

Using the Executive Order issued today by President Biden, the Treasury Department has issued sanctions against the following Russian technology companies for helping the SVR, Russia's Federal Security Service (FSB), and Russia's Main Intelligence Directorate (GRU) perform malicious cyber activities against the United States.

- **ERA Technopolis** - A research center and technology park funded and operated by the Russian Ministry of Defense. ERA Technopolis houses and supports units of Russia's Main Intelligence Directorate (GRU) responsible for offensive cyber and information operations and leverages the personnel and expertise of the Russian technology sector to develop military and dual-use technologies.
- **Pasit** - A Russia-based information technology (IT) company that conducted research and development in support of Russia's Foreign Intelligence Service's (SVR) malicious cyber operations.
- **SVA** - A Russian state-owned research institute specializing in advanced systems for information security located in Russia. SVA conducted research and development in support of the SVR's malicious cyber operations.
- **Neobit** - A Saint Petersburg, Russia-based IT security firm whose clients include the Russian Ministry of Defense, SVR, and Russia's Federal Security Service (FSB). Neobit conducted research and development in support of the cyber operations conducted by the FSB, GRU, and SVR. Neobit was also designated today under cyber-related E.O. 13694, as amended by E.O. 13757, WMD-related E.O. 13382, and the Countering America's Adversaries Through Sanctions Act (CAATSA) for providing material support to the GRU.
- **AST** - A Russian IT security firm whose clients include the Russian Ministry of Defense, SVR, and FSB. AST provided technical support to cyber operations conducted by the FSB, GRU, and SVR. AST was also designated today under E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.
- **Positive Technologies** - A Russian IT security firm that supports Russian Government clients, including the FSB. Positive Technologies provides computer network security solutions to Russian businesses, foreign governments, and international companies and hosts large-scale conventions that are used as recruiting events for the FSB and GRU. Positive Technologies was also designated today under E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.

US companies and financial institutions are no longer able to do business with the above-sanctioned companies without first applying for and receiving a license from the Office of Foreign Assets Control (OFAC).

Source: <https://www.bleepingcomputer.com/news/security/us-government-confirms-russian-svr-behind-the-solarwinds-hack/>

9. Hundreds of networks reportedly hacked in Codecov supply-chain attack

More details have emerged on the recent Codecov system breach which is now being likened to the SolarWinds hack.

In new reporting by Reuters, investigators have stated that hundreds of customer networks have been breached in the incident, expanding the scope of this system breach beyond just Codecov's systems.

As reported by BleepingComputer last week, Codecov had suffered a supply-chain attack that went undetected for over 2-months.

In this attack, threat actors had gained Codecov's credentials from their flawed Docker image that the actors then used to alter Codecov's Bash Uploader script, used by the company's clients.

By replacing Codecov's IP address with their own in the Bash Uploader script, the attackers paved a way to silently collect Codecov customers' credentials—tokens, API keys, and anything stored as environment variables in the customers' continuous integration (CI) environments.

Codecov is an online software testing platform that can be integrated with your GitHub projects, to generate code coverage reports and statistics, which is why it is favored by over 29,000 enterprises building software.

Hundreds of customer networks breached in Codecov incident

Codecov's initial investigation revealed that from January 31, 2021, periodic unauthorized alterations of Bash Uploader script occurred which enabled the threat actors to potentially exfiltrate information of Codecov users stored in their CI environments.

But, it was not until April 1st that the company became aware of this malicious activity when a customer noticed a discrepancy between the hash (shashum) of the Bash Uploader script hosted on Codecov's domain and the (correct) hash listed on the company's GitHub.

Soon enough, the incident got the attention of U.S. federal investigators since the breach has been compared to the recent SolarWinds attacks that the U.S. government has attributed to the Russian Foreign Intelligence Service (SVR).

Codecov has over 29,000 customers, including prominent names like GoDaddy, Atlassian, The Washington Post, Procter & Gamble (P & G), making this a noteworthy supply-chain incident.

According to federal investigators, Codecov attackers deployed automation to use the collected customer credentials to tap into hundreds of client networks, thereby expanding the scope of this system breach beyond just Codecov's systems.

"The hackers put extra effort into using Codecov to get inside other makers of software development programs, as well as companies that themselves provide many customers with technology services, including IBM," a federal investigator anonymously told Reuters.

By abusing the customer credentials collected via the Bash Uploader script, hackers could potentially gain credentials for thousands of other restricted systems, according to the investigator.

U.S. government and Codecov clients investigating the impact

The list of companies and GitHub projects using Codecov is extensive, as seen by BleepingComputer.

A simple search for the link to Codecov's compromised Bash Uploader script revealed thousands of projects that were or are using the script.

Note, this does not necessarily mean each of these projects was compromised, but rather that the complete impact of this incident is unclear and yet to be known in the upcoming days.

U.S. federal government investigators have therefore stepped in and are thoroughly investigating the incident.

Codecov clients including IBM have said that their code has not been modified, but declined to comment on whether their systems had been breached.

However, an Atlassian spokesperson got back to BleepingComputer stating, so far there was no indication of system compromise:

"We are aware of the claims and we are investigating them."

"At this moment, we have not found any evidence that we have been impacted nor have identified signs of a compromise," Atlassian told BleepingComputer.

Hewlett Packard Enterprise (HPE), which is another one of Codecov's 29,000 customers, said they were continuing their investigation into the incident:

"HPE has a dedicated team of professionals investigating this matter, and customers should rest assured we will keep them informed of any impacts and necessary remedies as soon as we know more," an HPE spokesman Adam Bauer told Reuters.

The Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) have not commented on the investigation at this time.

Codecov customers who, at any point in time used Codecov's uploaders (the Codecov-actions uploader for Github, the Codecov CircleCI Orb, or the Codecov Bitrise Step), are

advised to reset credentials and keys that may have been exposed as a result of this attack, and to audit their systems for any signs of malicious activity.

Source: <https://www.bleepingcomputer.com/news/security/hundreds-of-networks-reportedly-hacked-in-codecov-supply-chain-attack/>

10. The Value of Independent Testing to Assess Your Cybersecurity Posture

According to Gartner, 78% of organizations use 16 or more security tools and more than \$150B is spent on information security every year. Further the Gartner hype cycles for cloud, network, application, and endpoint security cover more than 60 products.

Despite all of these security solutions and spending, it remains difficult to definitively answer a key question: "How secure is our organization?" Let alone, "Are we protected from [the latest] cyber attack?" Here are some ways to start answering those questions.

Security Scoring

Whether internally developed or established by industry available tools, key performance indicators (KPIs) can be used to assess your cybersecurity posture across all security configurations and controls. KPIs are one way to answer the question of how secure an organization may be either as an absolute, based on its historical levels, or as compared to organizations of similar size, geographies, or business. Using KPIs can provide a relative assessment that can be considered reasonable. But simply being better than the average does not necessarily mean that your security is adequate for your level of risk.

Penetration Testing

To understand your real risk of an incident, you can engage a red team of ethical hackers to attempt to breach your security configurations, controls, and teams. These groups are experts in the latest tools, techniques, and tactics. They act like cyber criminals and attempt to breach your defenses, which is an excellent way to stress test every aspect of your security, including employee awareness. This approach helps you determine which defenses are strong and which are weak. A key limitation is that it is dependent on the expertise of the red team and it only occurs at a single point and defined scope of attack.

Breach Attack Simulation

Breach attack simulation (BAS) is similar to penetration testing. Like penetration testing, it attempts to assess the totality and effectiveness of your defenses, but it uses automation tools to seek entry, rather than human experts. BAS can be run regularly and broadly,

rather than at a single point in time or scope. However, the attacks are more programmatic, so they may be less sophisticated or customized than penetration testing.

Independent Effectiveness Testing

In addition to the organization-specific assessment of overall security, expert test labs run independent assessments of specific security tools. These assessments often benefit from a much larger sample set of attacks, since they are relevant to a broad set of organizations. And in many cases, they can provide comparative scoring for security tools of the same type. The common downside is that they operate in a lab, rather than the real-world. The conditions may vary from those of your organization, particularly over time. The assessments also typically focus on just one type of control, such as network security, email security, or endpoint security. They rarely test combinations of controls.

MITRE Engenuity ATT&CK Evaluations

MITRE Engenuity's ATT&CK Evaluations are another useful tool. The evaluations test a range of security tools that are typically in the same security category and expose them to a single or small number of sophisticated cybercriminal campaigns. These campaigns are comprised of a series of tactics and techniques that are designed to accomplish a defined cyber mission. The key benefits of this approach are:

Enterprise security teams to see the inner workings of security controls. They can understand not only what the solution detects but also why and how it performed. Seeing the process can give teams more confidence in the type of protection they have. The evaluation goes beyond a single attack, sample set, point in time, or control. Evaluation results also can be combined across controls for a more comprehensive view of coverage or exposure.

Security vendors get an independent assessment of their product's capabilities through the lens of the cybercriminal and a real-world campaign. They also have a collaborative community that can help them continuously improving the capabilities of their security products.

The primary drawback is that tactics and techniques evolve over time and the evaluation results are constrained to the scope of the campaigns that are run. They also focus only on detection of the attack technique, with no ability to assess what else (including legitimate operation) that might be flagged by the control.

Conclusion

Answering tough questions like "How secure are we?" or "Are we protected from [fill in the blank]?" requires considering a range of resources. If your objective is to do more than the average organization, security scoring is a great tool. If your objective is to push your security posture to higher levels, penetration testing and/or breach attack simulation are

great aids. For granular assessments of individual security controls at points of exceptional risk, independent effectiveness testing can help. And for planning and implementing a rigorous and resilient defense based on capabilities across controls in aggregate, the MITRE ATT&CK Evaluation is a valuable tool. Finally, if you have questions that relate to a specific cyberattack or campaign, you should talk to each security vendor to get the answers you need.

Source: <https://www.fortinet.com/blog/business-and-technology/the-value-of-independent-testing-to-assess-your-cybersecurity-posture>

11. Emotet malware nukes itself today from all infected computers worldwide

Emotet, one of the most dangerous email spam botnets in recent history, is being uninstalled today from all infected devices with the help of a malware module delivered in January by law enforcement.

The botnet's takedown is the result of an international law enforcement action that allowed investigators to take control of the Emotet's servers and disrupt the malware's operation.

Emotet was used by the TA542 threat group (aka Mummy Spider) to deploy second-stage malware payloads, including QBot and Trickbot, onto its victims' compromised computers.

TA542's attacks usually led to full network compromise and the deployment of ransomware payloads on all infected systems, including ProLock or Egregor by Qbot, and Ryuk and Conti by TrickBot.

How the Emotet uninstaller works

After the takedown operation, law enforcement pushed a new configuration to active Emotet infections so that the malware would begin to use command and control servers controlled by the Bundeskriminalamt, Germany's federal police agency.

Law enforcement then distributed a new Emotet module in the form of a 32-bit EmotetLoader.dll to all infected systems that will automatically uninstall the malware on April 25th, 2021.

Malwarebytes security researchers Jérôme Segura and Hasherezade took a closer look at the uninstaller module delivered by law enforcement-controlled to Emotet servers.

After changing the system clock on a test machine to trigger the module, they found that it only deletes associated Windows services, autorun Registry keys, and then exits the process, leaving everything else on the compromised devices untouched.

"For this type of approach to be successful over time, it will be important to have as many eyes as possible on these updates and, if possible, the law enforcement agencies involved should release these updates to the open internet so analysts can make sure nothing unwanted is being slipped in," Marcin Kleczynski, CEO of Malwarebytes, told BleepingComputer.

"That all said, we view this specific instance as a unique situation and encourage our industry partners to view this as an isolated event that required a special solution and not as an opportunity to set policy moving forward."

German federal police agency behind Emotet uninstaller module

In January, when law enforcement took down Emotet, BleepingComputer was told by Europol that the German Bundeskriminalamt (BKA) federal police agency was responsible for creating and pushing the uninstall module.

"Within the framework of the criminal procedural measures carried out at international level, the Bundeskriminalamt has arranged for the malware Emotet to be quarantined in the computer systems affected," Bundeskriminalamt told Bleepingcomputer.

In a January 28th press release, the US Department of Justice (DOJ) also confirmed that the Bundeskriminalamt pushed the uninstaller module to Emotet-infected computers.

"Foreign law enforcement, working in collaboration with the FBI, replaced Emotet malware on servers located in their jurisdiction with a file created by law enforcement," the DOJ said.

"The law enforcement file does not remediate other malware that was already installed on the infected computer through Emotet; instead, it is designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet."

Emotet removal delayed for collecting more evidence

BleepingComputer was told in January by the Bundeskriminalamt that the delay in uninstalling was for seizing evidence and clean the machines of the malware.

An identification of the systems affected is necessary in order to seize evidence and to enable the users concerned to carry out a complete system clean-up to prevent further offences. For this purpose, the communication parameters of the software have been adjusted in a way that the victim systems no longer communicate with the infrastructure

of the offenders but with an infrastructure created for the seizure of evidence. --
Bundeskriminalamt

"Please understand that we cannot provide any further information as the investigations are still ongoing," the Bundeskriminalamt told BleepingComputer when asked for more info.

When BleepingComputer reached out again for comment about today's operation, we did not receive a response.

The FBI also declined to comment when asked this week if the Emotet removal operation from devices located in the USA is still planned to occur on Sunday, April 25th.

Earlier this month, FBI coordinated a court-approved operation to remove web shells from US-based Microsoft Exchange servers compromised using ProxyLogon exploits without first notifying the servers' owners.

The FBI said that it only removed web shells and did not apply security updates or removed other malware that threat actors may have deployed on the servers.

Source: <https://www.bleepingcomputer.com/news/security/emotet-malware-nukes-itself-today-from-all-infected-computers-worldwide/>

12. FBI shares 4 million email addresses used by Emotet with Have I Been Pwned

Millions of email addresses collected by Emotet botnet for malware distribution campaigns have been shared by the Federal Bureau of Investigation (FBI) as part of the agency's effort to clean infected computers.

Individuals and domain owners can now learn if Emotet impacted their accounts by searching the database with email addresses stolen by the malware.

Over 4 million emails collected

Earlier this year, law enforcement [took control of Emotet botnet's infrastructure](#) that involved several hundreds of servers all over the world.

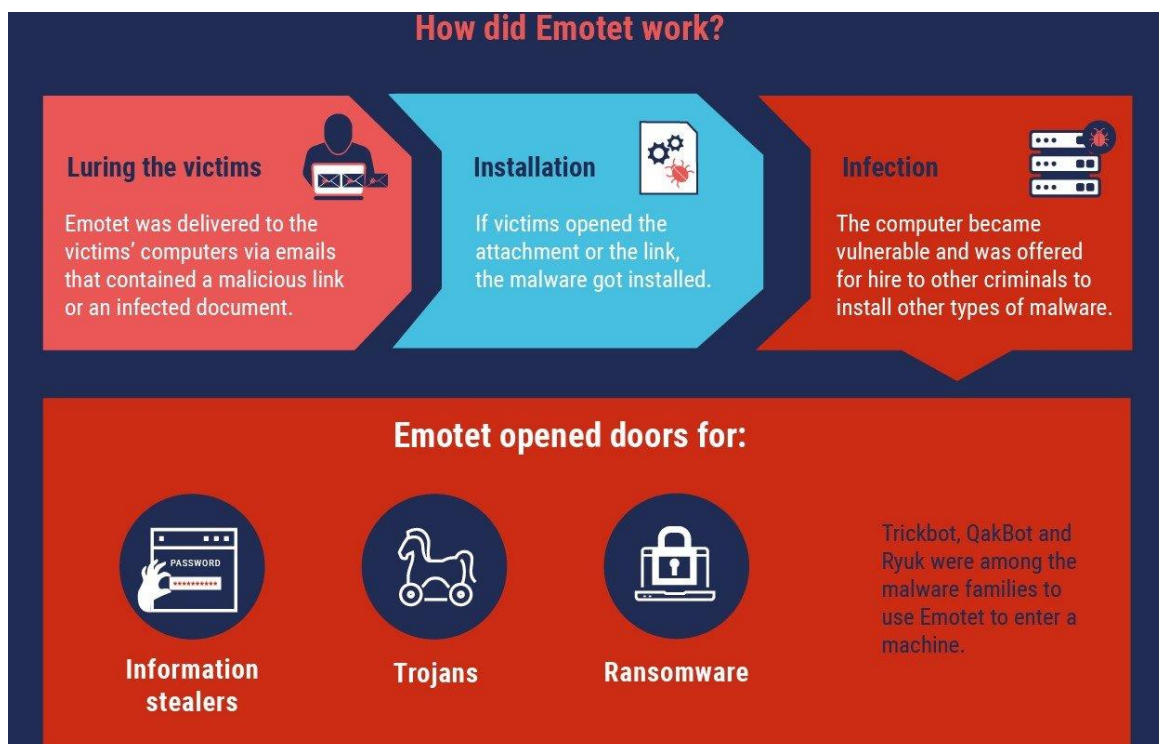
Using the communication line to infected computers, law enforcement on April 25 was able to send out an update that [uninstalled Emotet malware](#) on all affected systems.

Apart from computer systems, Emotet also compromised a large number of email addresses and used them for its operations. The FBI now wants to give the owners of these email addresses a quick way to check if they've been affected by Emotet.

For this purpose, the agency and the Dutch National High Technical Crimes Unit (NHTCU) shared 4,324,770 email addresses that had been stolen by Emotet with the Have I Been Pwned ([HIBP](#)) data breach notification service.

Troy Hunt, the creator of the HIBP service [says](#) that 39% of these email addresses had already been indexed as part of other data breach incidents.

The email addresses belong to users from multiple countries. They came from logins stored on Emotet’s infrastructure for sending out malicious emails or had been harvested from the users’ web browsers.



Emotet operation

Given its [sensitive nature](#), the Emotet data is not publicly searchable. Subscribers to the service that were impacted by the Emotet breach have already been alerted, says HIBP creator, Troy Hunt.

Referring to the verification process, Hunt says that “individuals will either need to verify control of the address via [the notification service](#) or perform a [domain search](#) to see if they're impacted.”

The Dutch National Police, which was part of the Emotet takedown operation, has a similar [lookup service](#), where users can check if Emotet compromised their emails.

Individuals can type in an email address, and if the account is part of the seized data from the Emotet botnet, the Dutch police will send it a message with instructions on what to do next. On February 3rd, the Dutch police added 3.6 million email addresses to its checking service.

Another service, called [Have I Been Emotet](#) from cybersecurity company TG Soft launched on October 1, 2020. It checks if Emotet used an email address as a sender or a recipient. However, it was last updated on January 25th, two days before the botnet was taken down.

Huge takedown effort

Emotet is among this decade's most prominent botnets causing hundreds of millions of dollars in damage across the world and infecting around 1.6 million computers in about nine months.

It played a key role in the distribution chain for several ransomware strains as it often delivered QakBot and Trickbot malware on the compromised network, which further dropped ProLock or Egregor, and Ryuk and Conti, respectively.

On January 27th, all three Epochs - subgroups of the botnet with a separate infrastructure - of [Emotet fell](#) under the control of law enforcement agencies. The operation was possible with the effort from authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine.

Source: <https://www.bleepingcomputer.com/news/security/fbi-shares-4-million-email-addresses-used-by-emotet-with-have-i-been-pwned/>

13. New stealthy Linux malware used to backdoor systems for years

A recently discovered Linux malware with backdoor capabilities has flown under the radar for years, allowing attackers to harvest and exfiltrate sensitive information from compromised devices.

The backdoor, dubbed RotaJakiro by researchers at Qihoo 360's Network Security Research Lab (360 Netlab), remains undetected by VirusTotal's anti-malware engines, although a sample was first uploaded in 2018.

RotaJakiro is designed to operate as stealthy as possible, encrypting its communication channels using ZLIB compression and AES, XOR, ROTATE encryption.

It also does its best to block malware analysts from dissecting it as resource information found within the sample spotted by 360 Netlab's BotMon system is encrypted using the AES algorithm.

"At the functional level, RotaJakiro first determines whether the user is root or non-root at run time, with different execution policies for different accounts, then decrypts the relevant sensitive resources using AES& ROTATE for subsequent persistence, process

guarding and single instance use, and finally establishes communication with C2 and waits for the execution of commands issued by C2," 360 Netlab said.

Linux backdoor used to exfil stolen data

Attackers can use RotaJakiro to exfiltrate system info and sensitive data, manage plugins and files, and execute various plugins on compromised 64-bit Linux devices.

However, 360 Netlab is yet to discover the malware creators' true intent for their malicious tool due to lack of visibility when it comes to the plugins it deploys on infected systems.

"RotaJakiro supports a total of 12 functions, three of which are related to the execution of specific Plugins," the researchers added. "Unfortunately, we have no visibility to the plugins, and therefore do not know its true purpose."

Since 2018 when the first RotaJakiro sample landed on VirusTotal, 360 Netlab found four different samples uploaded between May 2018 and January 2021, all of them with an impressive total of zero detections.

Command-and-control servers historically used by the malware have domains registered six years ago, in December 2015, all of them

FileName	MD5	Detection	First Seen in VT
systemd-daemon	1d45cd2c1283f927940c099b8fab593b	0/61	2018-05-16 04:22:59
systemd-daemon	11ad1e9b74b144d564825d65d7fb37d6	0/58	2018-12-25 08:02:05
systemd-daemon	5c0f375e92f551e8f2321b141c15c48f	0/56	2020-05-08 05:50:06
gvfsd-helper	64f6cfe44ba08b0babdd3904233c4857	0/61	2021-01-18 13:13:19

360 Netlab researchers also discovered links to the Torii IoT botnet first spotted by malware expert Vesselin Bontchev and analyzed by Avast's Threat Intelligence Team in September 2018.

The two malware strains use the same commands after being deployed on compromised systems, similar construction methods and constants used by both developers.

RotaJakiro and Torii also share multiple functional similarities, including "the use of encryption algorithms to hide sensitive resources, the implementation of a rather old-school style of persistence, structured network traffic."

Source: <https://www.bleepingcomputer.com/news/security/new-stealthy-linux-malware-used-to-backdoor-systems-for-years/>

14. Microsoft Office SharePoint Targeted With High-Risk Phish, Ransomware Attacks

SharePoint servers are being picked at with high-risk, legitimate-looking, branded phish messages and preyed on by a ransomware gang using an old bug.

A phishing campaign, discovered by researchers at [Cofense](#), is draping itself in a Microsoft Office SharePoint theme and successfully bypassing security email gateways (SEGs). In a post on Tuesday, the firm said that this is an example of why it's not always prudent to share documents via Microsoft's hugely popular, widely used SharePoint collaboration platform.

The phish is targeting Office 365 users with a legitimate-looking SharePoint document that claims to urgently need an email signature. The campaign cropped up in a spot that's supposed to be protected by Microsoft's own SEG. This isn't the first time that we've seen the SEG sanctuary get polluted: In December, [spearphishers spoofed Microsoft.com](#) itself to target 200 million Office 365 users, successfully slipping past SEG controls due to Microsoft's reported failure to enforce domain-based message authentication, reporting & conformance (DMARC): an email authentication protocol built specifically to stop exact domain spoofing (SPF/DKIM).

'Response Urgently...?'

As this image of the text in the phishing email shows, the spelling and grammar used in the boobytrapped message aren't the most egregious, atrociously spelled, syntactically bizarre giveaways you can find in these kinds of phishing campaigns. But then again, it's probably safe to assume that any SharePoint message that asks you to "response urgently" isn't coming from a native speaker.

The mere fact that the message presses urgency on its recipients should be a tip-off, of course: "Rush-rush" is a typical phishing ploy. Cofense notes that other red flags include the fact that the user's name isn't apparent in the opening message: an indication that it's a mass-distribution campaign intended to reach many targets.

As well, when recipients hover over the hyperlink, they'll see hide nor hair of any reference to Microsoft. Those who click on the link will instead be shuffled over to the landing page shown below, which display's Microsoft's SharePoint logo and the "Pending file" notification in front of a blurry background and a request for the intended victim to log in to view the document. That "could suffice for threat actors to extract and harvest users' personal data," Cofense says. If and when credentials are handed over, the campaign redirects the user to a spoofed, unrelated document, "which might be enough to trick the user into thinking this is a legitimate transaction," Cofense says.

In its [X-Force Threat Activity Report](#), IBM labelled the phish a high-risk threat and gave these recommendations:

- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated incidents of compromise (IoCs) in your environment.
- Consider blocking and/or setting up detection for all URL and IP based IoCs.
- Keep applications and operating systems running at the current released patch level.
- Exercise caution with attachments and links in emails.

Though it's high risk, this phishing campaign is basically just another story of a malicious actor putting up bogus material that looks legitimate in order to lure users into clicking, in the hopes of obtaining credentials. Don't shrug it off, though: it's yet another attack against SharePoint servers, which have now joined the roster of network devices – including much-bedeviled [Microsoft Exchange email servers](#), [SonicWall gateways](#) and [Pulse Secure gateways](#) – that are being used by ransomware gangs to jimmy open enterprise networks.

Which brings us to ransomware: the second slap in the double-SharePoint whammy:

Ransomware Gang Pings the Pain Via Wickr

It's a fairly new variant, first spotted in January by [Pondurance](#). Analysts are calling it two names: Hello, since some samples use .hello as an extension; or WickrMe, since the gang that's pushing it are using the Wickr encrypted instant messaging service to try to shake down victims for ransom.

The attackers are using a dusty Microsoft SharePoint 2019 vulnerability ([CVE-2019-0604](#)) to pry their way into victims' networks. From there, they're using Cobalt Strike to pivot to the domain controller and launch ransomware attacks.

CVE-2019-0604 is a high-severity CVE that can lead to remote code-execution. Microsoft [patched](#) the flaw in March 2019, but nonetheless, there seems to be no end to the attacks that have used it to penetrate unpatched servers since then. One example: Microsoft warned in October 2020 that Iranian nation-state actors were using CVE-2019-0604 to exploit remotely unpatched servers and to then implant a web shell to gain persistent access and code execution. Following the web shell installation, an attacker deploys [Cobalt Strike](#) – a commercially available penetration-testing tool that they later use to install a backdoor that lets them run automated PowerShell script, which eventually download and install the final payload: the Hello/Wickr ransomware.

Jeff Costlow, CISO of ExtraHop, told Threatpost on Wednesday that the ransomware attacks against the 2019 vulnerability affecting SharePoint servers are the more insidious

threat in the double whammy, in that they install remote control software and thus allow direct access to the infrastructure where attackers can freely frolic.

“The common thread is the SharePoint server,” Costlow said in an email. “Anyone using SharePoint needs to ensure that they are patching any instances of SharePoint to avoid the malware/ransomware installations. Long term, no amount of patching will solve the phishing problem. It’s too easy for attackers to build sites that mimic legitimate sites. We need to rethink how sharing is done. Security teams need to take a proactive stance to help their users conduct business safely. There are various tactics to help alert users to possible attacks, such as setting up each SharePoint server to use a familiar background or image for users to ensure that they only input credentials on legitimate sites.”

Two Separate SharePoint Jabs

Cofense told Threatpost in an email on Wednesday morning that there’s no apparent connection between the SharePoint phishing campaign that its analysts uncovered and the Wickr/Hello ransomware gang’s ongoing exploitation of SharePoint server vulnerabilities.

But one expert noted that there’s a monotonous regularity in the pattern that these attacks follow: First we get the news about a vulnerability, then it gets jumped on by attackers looking for the sitting ducks of unpatched servers.

In an email to Threatpost on Wednesday, Avihai Ben-Yossef, CTO and co-founder of Cymulate, said that we’ve seen this happen over and over. “In the last year, we see a repetitious pattern in such attacks. A zero-day is taken advantage of by a nation-state actor,” he said. “The affected company – in this case, Microsoft – announces the vulnerability and subsequently patches it. Then other nation-state actors learning about the vulnerability subsequently launch attacks on those who have not patched. Finally, the criminal ransomware attackers come in, socialize the exploit on Dark Net sites and use it ... to launch their own attacks. The double-SharePoint whammy is the fact that nation state actors used it first as a zero day (and then as a known vulnerability). Then ransomware actors came in and used it as well.

“The idea is to know what kind of problems you have and where,” he said. “If you don’t know, you can’t protect yourself. Organizations must develop a better response capability to track these announcements and threat intelligence and patch quicker.”

Source: <https://threatpost.com/sharepoint-phish-ransomware-attacks/165671/>

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.