telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

April 2022

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

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

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

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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

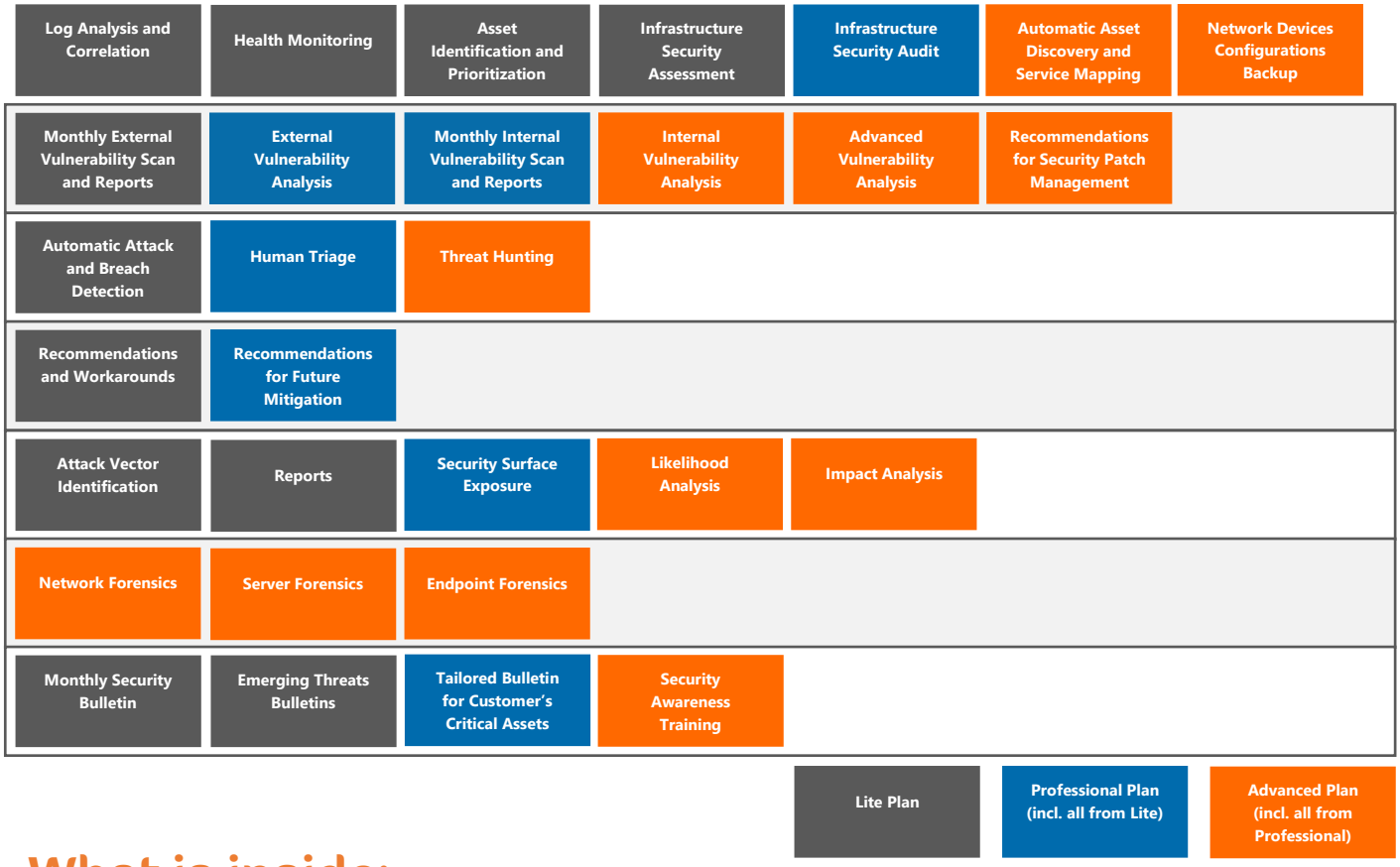
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



What is inside:

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

Table of Contents

1. Reality Winner's Twitter account was hacked to target journalists

Twitter account of former intelligence specialist, Reality Winner was hacked over the weekend by threat actors looking to target journalists at prominent media organizations.

Hackers took over Winner's verified Twitter account and changed the profile name to "Feedback Team" to impersonate Twitter staff before sending out suspicious DMs to verified users.

Bogus 'Copyright Infringement' notices

On Sunday, multiple journalists and verified Twitter users reported receiving suspicious DMs from a "verified" Twitter account called "Feedback Team."

On taking a closer look at "Feedback Team's" account's handle **@reazlepuff** however, Jacob Silverman, staff reporter for **The New Republic** pointed out the hacked account appeared to belong to Reality Winner:

> *Pretty sure that this is Reality Winner's account and that it's been hacked. Second image is a DM I just received. pic.twitter.com/KxXZmGfL6B*
>
> *— Jacob Silverman (@SilvermanJacob) February 27, 2022*

Reality Leigh Winner is an American former intelligence specialist who, in 2018, was sentenced to five years and three months in prison for unauthorized release of classified information to the media.

In 2017, Winner shared a National Security Agency (NSA) report about the Russian interference in the 2016 U.S. elections with the news outlet **The Intercept.** The report suggested that Russian hackers had illegally accessed U.S. voter registration rolls via email phishing attacks, although it didn't conclude if this had led to any tampering of electoral records.

Within minutes of Silverman's tweet, **Daily Dot** staff writer Mikael Thalen also reported receiving the DM, as did writer Tara Dublin.

These DMs impersonated Twitter staff and contained bogus "copyright infringement" notices enticing the recipients to click on a Google Sites link.

> *Hi Dear User,*
>
> *Copyright infringement was detected in one of the shares on your account. If you think copyright infringement is wrong, you need to provide feedback. Otherwise, your account will be removed within 48 hours. You can give feedback at the link below. Thank you for your understanding.*

https://sites.google.com/view/...

Thanks,
Twitter Support

The Google Sites webpage, seen by BleepingComputer, contained an embedded HTML iframe.

The contents of the iframe impersonated Twitter's look and feel and asked the user to provide "feedback on the form" to prevent their account from getting "permanently suspended" over copyright infringement:

Phishing webpage embedded on a Google Sites page (BleepingComputer)

The source URL of the malicious iframe, **https://begetadmadir[.]tk/juri/** is no longer accessible, as confirmed by BleepingComputer.

Credentials harvesting attack targets media companies

This appears to be a credentials harvesting attack and this isn't the first time such an attack has occurred either.

Mid-February some Indian journalists, including Sreedevi Jayarajan of The News Minute had their verified Twitter account taken over to target other verified profiles in a similar fashion.

The use of the account profile name "Feedback Team," and the identical wording of the DMs sent at the time from Jayarajan's hacked account imply the same threat actor(s) may be behind these attacks.

In January, British actor, comedian, and BBC presenter, Adil Ray "almost fell for this" phishing scam purportedly sent by another hacked verified account.

BleepingComputer has previously reported threat actors sending fake DMCA and DDoS complaints to prominent Twitter accounts to spread malware. This scam, however, distinctly targets media personalities via phishing, to harvest credentials from journalists, with the possible goal of breaching news outlets.

BleepingComputer reached out to Reality Winner to better understand what had happened:

"It started with these log ins from Turkey and I couldn't secure my account quickly enough," Winner tells BleepingComputer.

"I only had a verified account for like 6 days and thought I was gonna lose it. Also I'm really embarrassed that it sent the DM out to journalists, like I felt like I'd lost all credibility."

Additionally, Winner also released a statement confirming the hack and expressed regret for anyone affected.

Should you come across a suspicious DM or a Twitter account that appears to be hacked, consider reaching out to real Twitter Support.

Source: https://www.bleepingcomputer.com/news/security/reality-winners-twitter-account-was-hacked-to-target-journalists/

2. Daxin Espionage Backdoor Ups the Ante on Chinese Malware

Via node-hopping, the espionage tool can reach computers that aren't even connected to the internet.

The Daxin malware is taking aim at hardened government networks around the world, according to researchers, with the goal of cyberespionage.

The Symantec Threat Hunter team noticed the advanced persistent threat (APT) weapon in action in November, noting that it's "the most advanced piece of malware Symantec researchers have seen from China-linked actors…exhibiting technical complexity previously unseen by such actors."

They added that Daxin's specific scope of operations includes reading and writing arbitrary files; starting and interacting with arbitrary processes; and advanced lateral movement and stealth capabilities.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) also flagged the activity, which Symantec characterized as "long-running." The earliest known sample of the malware dates from 2013, when it already had a large part of the codebase fully developed.

"Daxin malware is a highly sophisticated rootkit backdoor with complex, stealthy command-and-control (C2) functionality that enabled remote actors to communicate with secured devices not connected directly to the internet," warned CISA, in a Monday alert. "Daxin appears to be optimized for use against hardened targets, allowing the actors to deeply burrow into targeted networks and exfiltrate data without raising suspicions."

Built for Stealth

From a technical standpoint, Daxin takes the form of a Windows kernel driver, according to Symantec's Monday analysis, and has a focus on stealth.

"Daxin's capabilities suggest the attackers invested significant effort into developing communication techniques that can blend in unseen with normal network traffic on the target's network," the firm found. "Specifically, the malware avoids starting its own network services. Instead, it can abuse any legitimate services already running on the infected computers."

It communicates with legitimate services via network tunneling, they added – and further, it can set up daisy-chain communications, researchers added to move internally via hops between several linked computers.

"Daxin is also capable of relaying its communications across a network of infected computers within the attacked organization," they said. "The attackers can select an arbitrary path across infected computers and send a single command that instructs these computers to establish requested connectivity. This use case has been optimized by Daxin's designers."

Daxin also can hijack legitimate TCP/IP connections. According to Symantec, it monitors all incoming TCP traffic for certain patterns, and when a preferred pattern is detected, it disconnects the legitimate recipient and takes over the connection.

"It then performs a custom key exchange with the remote peer, where two sides follow complementary steps. The malware can be both the initiator and the target of a key exchange," according to the analysis. "A successful key exchange opens an encrypted communication channel for receiving commands and sending responses. Daxin's use of hijacked TCP connections affords a high degree of stealth to its communications and helps to establish connectivity on networks with strict firewall rules. It may also lower the risk of discovery by SOC analysts monitoring for network anomalies."

When all of this is put together, the result is that a single command message that includes all the details required to establish communication, specifically the node IP address, its TCP port number and the credentials to use during custom key exchange. When Daxin receives this message, it picks the next node from the list.

The research team linked Daxin to Chinese actors because it's usually deployed alongside tools known to be associated with Chinese espionage actors.

"Most of the targets appear to be organizations and governments of strategic interest to China," they added. "Daxin is without doubt the most advanced piece of malware Symantec researchers have seen used by a China-linked actor."

Source: https://threatpost.com/daxin-espionage-backdoor-chinese-malware/178706/

3. Conti Ransomware Decryptor, TrickBot Source Code Leaked

The decryptor spilled by ContiLeaks won't work with recent victims. Conti couldn't care less: It's still operating just fine. Still, the dump is a bouquet's worth of intel.

The pro-Ukraine member of the Conti ransomware gang who promised to eviscerate the extortionists after they pledged support for the Russian government has spilled yet more Conti guts: The latest dump includes source code for Conti ransomware, TrickBot malware, a decryptor and the gang's administrative panels, among other core secrets.

On Monday, vx-underground – an internet collection of malware source code, samples and papers that's generally considered to be a benign entity – shared on Twitter a message from a Conti member saying that "This is a friendly heads-up that the Conti gang has just lost all their sh•t."

The first of what ContiLeaks promised would be a series of "very interesting" leaks included 60,000 of the Conti gang's internal chat messages.

The Conti Intel Treasure Trove

Then, on Tuesday, ContiLeaks leaked even more of Conti's common tactics, techniques and procedures (TTPs), which were shared by vx-underground.

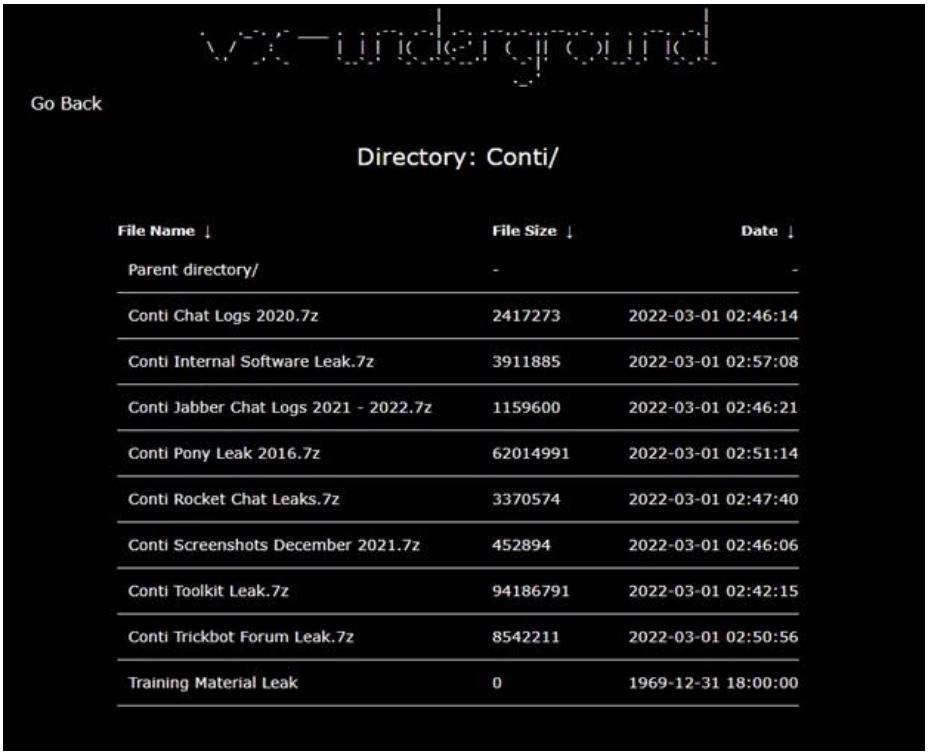
In a Wednesday analysis, CyberArk researchers enumerated the leaked content and why it's important. This intel is vital as Russian tanks roll through Ukraine and cyberattacks fly in support of either aiding the besieged country or tripping up the aggressor, CyberArk researchers asserted.

Its analysis pointed to a cybersecurity bulletin issued jointly over the weekend by the Cybersecurity and Infrastructure Agency (CISA) and the FBI: an advisory that warned that Russia's attack on Ukraine – which has included cyberattacks on Ukrainian government and critical infrastructure organizations – may spill over Ukraine's borders, particularly in the wake of sanctions imposed by the United States and its allies.

"As cybersecurity researchers, we believe insight gained from these leaks is incredibly important to the cybersecurity community at large. Ongoing awareness and visibility into the leaked tools while supporting the need for continued vigilance is critical during this time, and reinforced by [the CISA/FBI alert]."

What's in the Second Dump

The files shared by ContiLeaks have a slew of fresh meat, with some dated as recently as yesterday, March 1.



ContiLeaks' data dump content as of March 1. Source: vx-underground.

Here's a selection of the repositories and what researchers can do with them:

- **Chats**

  As far as the leaked chats go, they span internal communications of the Conti gang between June and November 2020. CyberArk noted that one user in particular "frequently spams all the other users."

  This can also be a useful tool for us to investigate since we can see maybe even all the usernames in one place, allowing us to enumerate all the people in the Conti group.

  The chats will enable researchers to see a good chunk of Conti gang usernames in one place, researchers said, "allowing us to enumerate all the people in the Conti group."

- **Admin Panel Code**

A quick look at the cache's repositories led the researchers to surmise that most of the code Conti uses appears to be open-source software. They pointed to two examples: the two PHP frameworks yii2 and Kohana, which are "used as part of (what seems to be) the admin panel," they said.

"The code is mostly written in PHP and is managed by Composer, with the exception of one repository of a tool written in Go," they said. The repositories also contain some config files that list local database usernames and passwords, as well as a few public IP addresses.

- **Credentials Ripped Off by Pony Malware**

The Conti Pony Leak 2016 repository contains a collection of email accounts and passwords – including from mail services such as gmail.com, mail.ru and yahoo.com – that were apparently stolen from various sources by the Pony credential-stealing malware: a credential stealer that, at least as of 2018, was crooks' favorite stealer.

It also contains credentials from FTP/ RDP and SSH services, plus credentials from different websites.

- **TTPs**

The Conti Rocket Chat Leaks contains a chat history of Conti members swapping tips about targets and carrying out attacks via crooks' favorite: Cobalt Strike, the legitimate, commercially available tool used by network penetration testers and by crooks to sniff out vulnerabilities.

The Conti gang chatters talked about these techniques:

- Active Directory Enumeration
- SQL Databases Enumeration via sqlcmd.
- How to gain access to Shadow Protect SPX (StorageCraft) backups.
- How to create NTDS dumps vs vssadmin
- How to open New RDP Port 1350

And these tools:

- Cobalt Strike
- Metasploit
- PowerView
- ShareFinder
- AnyDesk
- Mimikatz

- **Conti Locker v2 & the Decryptor That Probably De-Won't**

The dump also contains the source code for Conti Locker v2, which was first leaked as a password-protected zip file but then again without any password.

Besides the source code for v2 of the ransomware encryption source code, the leak also contained source code for the decryptor – a decryptor that reportedly won't work, as pointed out on Twitter.

> *Just a heads up: The decryptor code contained within this package is not the latest version and will not work for the most recent Conti victims.*
>
> *— Fabian Wosar (@fwosar) March 1, 2022*

"I had heard it's not the latest version and does not work," Marcus confirmed.

The released decryptor might be a version that Conti sends to victims who've paid the ransom, he suggested.

Decryptors act kind of like unzipping a password-protected file, he suggested, except that they're more complex, given that they vary by the ransomware family.

"Some are built into a standalone binary, others can be remote-enabled. Usually they have keys built into them," Marcus described.

- **Conti Training Materials**

The leaked documents also contain training materials, including videos of online courses in Russian, as well as how-tos about this list of TTPs:

- Cracking
- Metasploit
- Network Pentesting
- Cobalt Strike
- PowerShell for Pentesters
- Windows Red Teaming
- WMI Attacks (and Defenses)
- SQL Server
- Active Directory
- Reverse Engineering

Conti training in Russia. Course: CyberArk.

TrickBot Leaks

One of the leaked files is a dump of chats from the forums used by the operators of the TricKBot trojan/malware, spanning forum messages from 2019 until 2021.

Most of the chats are about how to move laterally across networks and how to use certain tools, but CyberArk also found out quite a bit about the TrickBot and Conti gang's TTPs.

"For instance in one of the correspondences a member shares his web shell of choice, 'he lightest and most durable webshell I use,'" researchers said.

Also included are evidence from early July 2021 that the group used exploits such as Zerologon: Not surprising, given that starting in September 2020, at least four public proof-of-concept (PoC) exploits for the flaw were released on Github, along with technical details of the vulnerability.

Other TrickBot leaks include server-side components written in Erlang, a trickbot-command-dispatcher-backend and trickbot-data-collector-backend, dubbed lero and dero.

Thank heavens for the readable code, said one Twitter commenter: "That's finally something worth reviewing (Conti Trickbot Leaks.7z file) – clean, reusable implementation in Erlang, better than several open source Erlang server examples."

> *That's finally something worth reviewing (Conti Trickbot Leaks.7z file) – clean, reusable implementation in Erlang, better than several open source Erlang server examples.*
>
> *— PAYLOAD – magazyn o ofensywnym bezpieczeństwie IT (@PayloadPl)*
> *March 1, 2022*

TrickBot Code Could Lead to … Better TrickBot

Will the leak slow down TrickBot operators? Well, it didn't actually have to, since the operators already seem to have taken a few hits of Zanax.

Last week, researchers at Intel 471 published a report about how the group behind the TrickBot malware is back after an unusually long lull between campaigns. If not a full stop, they've been operating pretty languidly: from Dec. 28, 2021 until Feb. 17, Intel 471 researchers hadn't seen any new TrickBot campaigns.

Researchers said at the time that the pause could be due to the TrickBot gang making an operational shift to focus on partner malware, such as Emotet.

The ContiLeaks source code leak could, however, change the scene, and not for the better. David Marcus, senior director of threat intelligence at threat-intel security company LookingGlass, told Threatpost on Wednesday that the leaks will have "a huge impact" long term as security researchers continue to research the fresh data. "The amount we will learn about their tactics, code development, monetization efforts, potential members and such cannot be overstated," he said via email.

But as far as the source code leak is concerned, that will be a double-edged sword, he cautioned. "It will benefit researchers from a defensive point-of-view, as a better understanding of how TrickBot works will allow for better defensive measures," he said. "The flip side of that is that it will also allow for more TrickBot development by more malware writers."

Conti Couldn't Care Less

As far as the leak of Conti code goes, it would be nice to think that the gang's operators were howling in pain at the disclosures, but that's not exactly what's happening.

Yelisey Boguslavskiy, head of research at the threat intel firm Advanced Intelligence (AdvInt), told Threatpost on Wednesday that none of the firm's primary source intel demonstrates that this will affect Conti.

"The leak was related to only one group out of six, and even though this group was likely the most important one, the rest of the teams were not impacted at all," he explained. "Conti relaunched all of its infrastructural capacities and keep operating."

Source: https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/

4. Hacking Alexa through Alexa's Speech

An Alexa can respond to voice commands it issues. This can be exploited:

> The attack works by using the device's speaker to issue voice commands. As long as the speech contains the device wake word (usually "Alexa" or "Echo") followed by a permissible command, the Echo will carry it out, researchers from Royal Holloway University in London and Italy's University of Catania found. Even when devices require verbal confirmation before executing sensitive commands, it's trivial to bypass the measure by adding the word "yes" about six seconds after issuing the command. Attackers can also exploit what the researchers call the "FVV," or full voice vulnerability, which allows Echos to make self-issued commands without temporarily reducing the device volume.

It does require proximate access, though, at least to set the attack up:

> It requires only a few seconds of proximity to a vulnerable device while it's turned on so an attacker can utter a voice command instructing it to pair with an attacker's Bluetooth-enabled device. As long as the device remains within radio range of the Echo, the attacker will be able to issue commands.

Research paper.

Source: https://www.schneier.com/blog/archives/2022/03/hacking-alexa-through-alexas-speech.html

5. Google: Russia, China, Belarus state hackers target Ukraine, Europe

Google says Russian, Belarusian, and Chinese threat actors targeted Ukrainian and European government and military organizations, as well as individuals, in sweeping phishing campaigns and DDoS attacks.

The company's Threat Analysis Group (TAG), a dedicated team of security experts that works to defend Google users from state-sponsored attacks, has alerted hundreds of Ukrainians they've been targeted.

"In the last 12 months, TAG has issued hundreds of government-backed attack warnings to Ukrainian users alerting them that they have been the target of government-backed hacking, largely emanating from Russia," said Shane Huntley, Google's TAG lead.

"Over the past two weeks, TAG has observed activity from a range of threat actors that we regularly monitor and are well-known to law enforcement, including FancyBear and Ghostwriter. This activity ranges from espionage to phishing campaigns."

Phishing for European and Ukrainian credentials

For instance, Huntley said that the FancyBear hacking group (aka APT28), part of Russia's Main Directorate of the General Staff of the Armed Forces (also known as GRU), launched several large-scale credential phishing campaigns using compromised email accounts and redirecting targets to attacker-controlled Blogspot domains.

Belarusian threat actor Ghostwriter (aka UNC1151) was also observed by Google TAG while targeting Polish and Ukrainian military and government organizations during the last seven days.

The Computer Emergency Response Team of Ukraine (CERT-UA) and Facebook previously warned of other phishing campaigns against Ukrainian officials and military personnel, also attributed Ghostwriter hackers (previously linked with high confidence by Mandiant to the Belarusian government).

Cybersecurity firm Proofpoint also spotted spear-phishing attacks targeting European government personnel aiding Ukrainian refugees, a campaign aligned with and likely related to July 2021 phishing attacks also attributed to the Ghostwriter hacking group.

Russia and Belarus are not the only ones attacking Ukrainian and European orgs. Huntley says that China-based hacking group Mustang Panda (aka Temp.Hex and TA416) also switched from regular Southeast Asian targets to European entities, now using phishing lures related to the Ukrainian invasion.

On Monday, Proofpoint revealed that it also detected Mustang Panda phishing activity "targeting European diplomatic entities, including an individual involved in refugee and migrant services."

DDoS attacks launched from Ukraine and Russia

As BleepingComputer previously reported, this deluge of ongoing attacks has also included DDoS attacks targeting Ukrainian government agencies and state banks, as well as multiple series of destructive malware attacks [1, 2].

Google TAG also detected "DDoS attempts against numerous Ukraine sites, including the Ministry of Foreign Affairs, Ministry of Internal Affairs, as well as services like Liveuamap that are designed to help people find information".

To help websites belonging to Ukrainian government websites, embassies worldwide, and other governments stay online throughout these attacks, Google also expanded eligibility for Project Shield, the company's free protection service against distributed denial-of-service (DDoS) attacks.

According to Google, more than Ukrainian 150 websites, including many news organizations, have registered and are using the service to block incoming DDoS attacks.

Last week, the Russian government also shared a list of over 17,000 IP addresses allegedly used to launch DDoS attacks targeting Russian organizations and their networks.

Ukraine's Vice Prime Minister Mykhailo Fedorov previously announced the creation of an "IT army" that would support the country's "fight on the cyber front."

The creation of the Ukrainian IT Army was prompted by a "massive wave of hybrid warfare," and it was only revealed after the Defense Ministry of Ukraine began recruiting Ukraine's underground hacker community to launch cyberattacks against Russia.

Source: https://www.bleepingcomputer.com/news/security/google-russia-china-belarus-state-hackers-target-ukraine-europe/

6. 93% of Organizations Have Network Vulnerabilities: Here's How to Beat the Odds

Cybersecurity is an ongoing battle, and the latest figures from penetration testers prove that the fight is far from over. According to Positive Technologies, 93% of all networks are open to breaches due to common vulnerabilities. However, there are proactive steps business owners can take to stay on the right side of that ratio.

Take a look at some of the common vulnerabilities as outlined by the report. We'll also address some important actions that businesses and agencies can take to reduce their attack surface and harden their networks.

Protecting Your Network

It's easy to think that your network is mostly protected from common network threats. After all, you have a security operations center team already, right? They're watching the network for anomalies and responding quickly to alerts. You also have some excellent software in place that helps you uncover malware attempts and malicious websites.

These are basic steps that any well-prepared enterprise should take if they're serious about cyber defense. However, these measures may not be enough.

From July 2020 to June 2021, multiple pen testers across several different industries assessed organizations' readiness. The compiled data painted a grim picture. 93% of those networks are poorly configured, even at the most basic levels. In 71% of these cases, attackers would be able to impact a business to an "unacceptable" degree.

The findings in this report showed that common vulnerabilities still exist in most networks today. Think poor password management, outdated and unpatched devices and software, poor security configurations and inconsistent user access protocols.

These statistics are a sobering reminder that no one is immune to digital attacks. It's more important than ever for businesses to take proactive steps to secure their networks.

Avoiding a Defeatist Attitude

At the same time, though, people and tech solve problems like this all the time. It can be easy to feel overwhelmed and defeated. Protecting a network from all possible attack vectors is a daunting task. We can take simple, progressive steps to avoid being at risk, though.

In many cases, training and awareness for employees are the most overlooked yet impactful steps you can take. By teaching your team how to spot a phishing email or malicious website, you're arming them with the knowledge they need to help protect your network from these threats.

In addition, it's crucial to have a security policy in place that outlines norms for employee behavior and lays out best practices for protecting company data. This document should outline procedures for password management best practices and guidelines for device and software usage. Make sure you have this as you increase remote working and personal device use.

Applying Zero Trust Protocols and Hardening App Security

In addition to awareness training for employees, another best practice is using zero trust network protocols. Your team should deploy these protocols across all internal and external environments. That way, each user must prove who they are before accessing any network apps or data.

In an ideal world, a zero trust network also includes multi-factor authentication. This provides more layers of protection against unwanted access attempts. This can include biometric identification, facial recognition through supported webcams and traditional password management.

Another critical step you can take is to harden application security. Ensure you have proper visibility into known and unknown threats lurking in your networks. Threat intelligence gathering and proactive penetration testing can help your company gain this. From there, it helps find and address vulnerabilities in app security before a breach occurs.

Renewed Focus on Incident Response Plans

Having a thorough incident response plan (IRP) is also essential. It can help you to rapidly respond to any type of attack or data breach.

Your IRP should include step-by-step procedures for spotting and containing an attack. Also include protocols for informing impacted people and groups. You should have certain personnel assigned to each step of the response plan. In addition, perform regular testing and updates to ensure that the plan is up-to-date and effective.

A well-drafted IRP is a critical part of any cybersecurity strategy and should be considered a high priority. With the proper steps in place, your team can work to stay ahead of the curve and beat the odds.

Up to the Task

It can be a daunting task for security teams to patch network vulnerabilities before they become a problem, but it is possible to do. The report cited above is less of a grim truth and more of a call to action. There is still work to be done in reducing the attack surface. However, through proactive planning, the right level of awareness and the proper tools and technologies, you can increase the chances of remaining secure.

Source: https://securityintelligence.com/articles/93-of-organizations-have-network-vulnerabilities-heres-how-to-beat-the-odds/

7. Massive phishing campaign uses 500+ domains leading to fake login pages

Large-scale phishing activity using hundreds of domains to steal credentials for Naver, a Google-like online platform in South Korea, shows infrastructure overlaps linked to the TrickBot botnet.

The resources used for this attack show the sheer size of the cybercriminal effort to collect login data to be used in various attacks.

Similar to Google, Naver provides a diverse set of services that range from web search to email, news, and the NAVER Knowledge iN online Q&A platform.

Massive infrastructure

Besides access to normal user accounts, Naver credentials can also open the door to enterprise environments, as a result of password reuse.

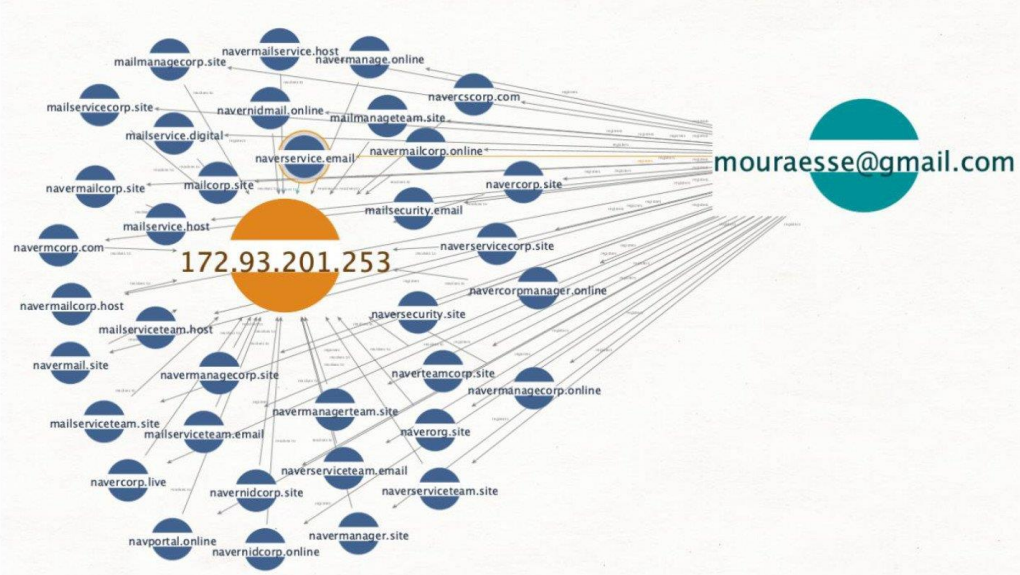
Security researchers at cyber intelligence company Prevailion earlier this year identified a massive phishing operation focused on collecting credentials of Naver users.

They started the investigation from one domain name - mailmangecorp[.]us - shared by Joe Słowik, which opened the door to a "vast network of targeted phishing infrastructure designed to harvest valid login credentials for Naver."

"While investigating the hosting infrastructure being used to serve the Naver-themed phishing pages, PACT analysts identified overlaps with the WIZARD SPIDER [a.k.a. TrickBot] infrastructure," Prevailion says in a report today.

The TrickBot operation is believed to have changed management recently, with its old partner, the Conti ransomware syndicate, moving to its helm.

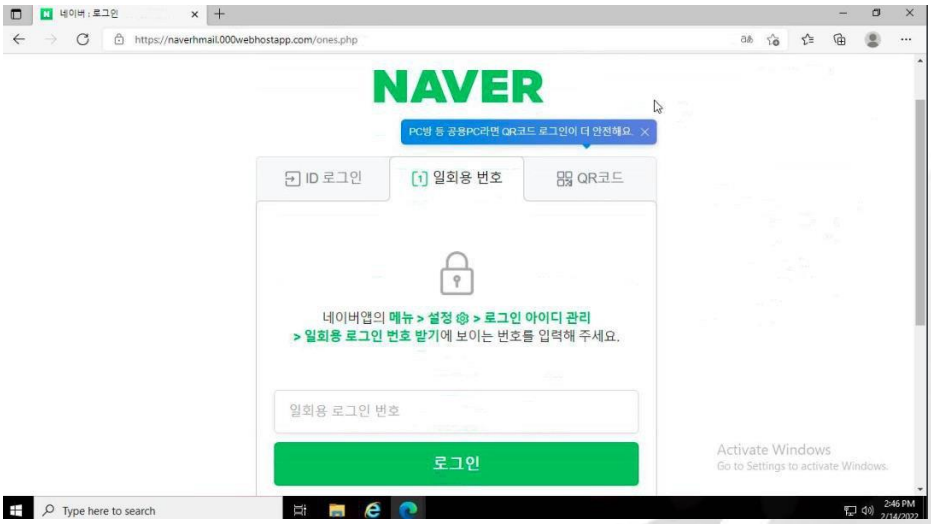
The researchers linked 542 unique domains to the operation, 532 of them being used for Naver-themed phishing. They noticed that the operator would use an email address to register a set of domain names that resolved to a single IP address.



source: Prevailion

The threat actor relied on multiple addresses to create registrant personas for the Naver campaign. Some of the domains are registered as recently as February, while the oldest ones date from August 2021.

Prevailion researchers discovered that the domains resolving to the IP address in the image above were part of a redirect scheme (HTTP/302) that took potential victims to fake login pages for the Naver platform hosted on Hostinger.



source: Prevailion

From the initial email address, Prevailion was able to find another cluster of 58 phishing domains resolving to 23.81.246[.]131, an IP address that proved critical in establishing the initial connection between Naver credential phishing and the infrastructure associated with TrickBot.

According to the researchers, a couple of Cobalt Strike beacon samples on Virus Total were associated with 23.81.246[.]131 as part of a campaign that exploited CVE-2021-40444 to deliver Conti ransomware, a common payload for TrickBot.

In the report today, Prevailion provides additional indicators connecting the Naver phishing domains to TrickBot infrastructure revealed in public research from RiskIQ and Microsoft.

The researchers say that their findings are suggesting that the Naver phishing activity is continuing as the infrastructure is still in use and numerous domains have been registered this month for this purpose.

Prevailion notes that "this infrastructure appears to support separate, discrete campaigns" and while the overlaps with TrickBot infrastructure exist, they are limited to hosting and DNS resolutions.

The company also underlines that "the Naver-themed phishing activity that was initially discovered does not appear to be the work of a ransomware group directly."

However, these file-encrypting attacks are often preceded by phishing or credential-stealing campaigns run by affiliates or partners seeking access to networks of valuable targets.

One theory that Prevalion believes explains their findings is that cybercriminals are relying on an "infrastructure-as-a-service" type of offering for their operations.

Source: https://www.bleepingcomputer.com/news/security/massive-phishing-campaign-uses-500-plus-domains-leading-to-fake-login-pages/

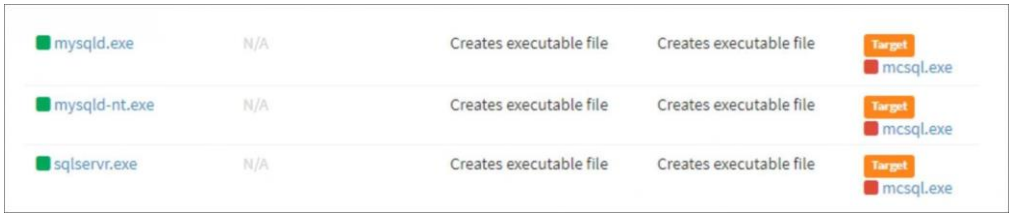
8. Unsecured Microsoft SQL, MySQL servers hit by Gh0stCringe malware

Hackers target poorly secured Microsoft SQL and MySQL database servers to deploy the Gh0stCringe remote access trojans on vulnerable devices.

Gh0stCringe, aka CirenegRAT, is a variant of Gh0st RAT malware that was most recently deployed in 2020 Chinese cyber-espionage operations but dates as far back as 2018.

In a new report today by cybersecurity firm AhnLab, researchers outline how the threat actors behind GhostCringe are targeting poorly secured database servers with weak account credentials and no oversight.

As you can see below, the threat actors are breaching the database servers and using the mysqld.exe, mysqld-nt.exe, and sqlserver.exe processes to write the malicious 'mcsql.exe' executable to disk.



MySQL and Microsoft SQL processes writing malware files to disk
Source: AhnLab

These attacks are similar to the Microsoft SQL server attacks we reported last February, which dropped Cobalt Strike beacons using the Microsoft SQL xp_cmdshell command.

In addition to Gh0stCringe, AhnLab's report mentions the presence of multiple malware samples on the examined servers, indicating competing threat actors are breaching the same servers to drop payloads for their own campaigns.

Gh0stCringe on the server

Gh0stCringe RAT is a powerful malware that establishes a connection with the C2 server to receive custom commands or exfiltrate stolen information to the adversaries.

The malware can be configured during deployment with specific settings concerning its functions, as detailed below:

- **Self-copy** [On/Off]: If turned on, it copies itself to a certain path depending on the mode.
- **Mode of execution** [Mode]: Can have values of 0, 1, and 2.
- **File size change** [Size]: In Mode #2, the malware copies itself to the path '%ProgramFiles%\Cccogae.exe', and if there is a set value, it adds junk data of the designated size to the back of the file.
- **Analysis disruption technique** [On/Off]: Obtains the PID of its parent process and the explorer.exe process. If it results in a value of 0, terminates itself.
- **Keylogger** [On/Off]: If turned on, the keylogging thread operates.
- **Rundll32 process termination** [On/Off] If turned on, executes 'taskkill /f /im rundll32.exe' command to terminate the rundll32 process that is running.
- **Self-copy file property** [Attr]: Sets property to read-only, hidden, and system (FILE_ATTRIBUTE_READONLY|FILE_ATTRIBUTE_HIDDEN|FILE_ATTRIBUTE_SYSTEM).

```
.data:10011FB2                 db    0
.data:10011FB3                 db    0
.data:10011FB4 conf_selfCopy   dd 1                    ; DATA XREF: fn_installService+428↑r
.data:10011FB4                                         ; DllMain(x,x,x)+416↑r
.data:10011FB8 conf_execMode   db 2                    ; DATA XREF: FUCKYOU:loc_1000724B↑r
.data:10011FB8                                         ; FUCKYOU:loc_100072D3↑r ...
.data:10011FB9                 align 2
.data:10011FBA conf_fileAppend dw 0                    ; DATA XREF: gh0st_SaveToFile↑r
.data:10011FBC conf_AntiAnalysis dd 1                  ; DATA XREF: FUCKYOU+3F↑r
.data:10011FBC                                         ; DllMain(x,x,x)+32↑r
.data:10011FC0 conf_offlineKeylogger dd 0              ; DATA XREF: thread_main+9C↑r
.data:10011FC4                 align 8
.data:10011FC8 conf_killRundll32 dd 0                  ; DATA XREF: FUCKYOU:loc_1000723E↑r
.data:10011FC8                                         ; DllMain(x,x,x):loc_10007BEA↑r
.data:10011FCC conf_fileAttr   dd 7                    ; DATA XREF: fn_installService+1A9↑r
.data:10011FCC                                         ; FUCKYOU+91↑o ...
.data:10011FD0                 db    0
```

The RAT's settings data (ASEC)

Of the above, the keylogger is maybe the most aggressive component as this is what steals user inputs from the compromised system.

The keylogging component uses the Windows Polling method (GetAsyncKeyState API) for querying the state of every key through an endless loop.

This otherwise reliable logging method introduces the risk of suspiciously high CPU usage, but in poorly managed servers, this is unlikely to cause problems to the threat actors.

The malware will also monitor the keypresses for the last three minutes and send them with basic system and network information to the malware's command and control servers.

These logged keystrokes will allow the threat actors to steal login credentials and other sensitive information that logged-in users entered on the device.

Modes and commands

CirenegRAT supports four operational modes, namely 0, 1, 2, and a special Windows 10 mode, selected by the threat actor during deployment.

The modes configure how persistence is established via the modification of the Windows registry and the activation of the self-copy module. For example, Mode #0 is running without persistence, while Mode #2 establishes persistence and considers self-copy settings.

As for the remote commands supported by the RAT, these are summed up in the following:

- Download additional payloads from the C2 and execute them.
- Connect to a URL via IE
- Destroy MBR (master boot record)
- Keylogging (independent command)
- Steal clipboard database
- Collect Tencent-related information
- Update
- Uninstall

- Register Run Key
- Terminate host system
- Reboot NIC
- Scan for running processes
- Display message pop-up

How to secure database servers

First, update your server software to apply the latest available security updates, which helps exclude a range of attacks that leverage known vulnerabilities.

It is also essential to use a strong admin password that is hard to guess or brute-force.

The most crucial step is to place the database server behind a firewall allowing only authorized devices to access the server.

Finally, monitor all actions to identify suspicious reconnaissance activity and use a data access controller for data transaction policy inspection.

Source: https://www.bleepingcomputer.com/news/security/unsecured-microsoft-sql-mysql-servers-hit-by-gh0stcringe-malware/

9. Free decryptor released for TrickBot gang's Diavol ransomware

Cybersecurity firm Emsisoft has released a free decryption tool to help Diavol ransomware victims recover their files without paying a ransom.

Diavol ransomware victims can download the free tool from Emsisoft's servers to decrypt their data using detailed instructions available in this usage guide [PDF].

"The decryptor requires access to a file pair consisting of one encrypted file and the original, unencrypted version of the encrypted file to reconstruct the encryption keys needed to decrypt the rest of your data," Emsisoft explains.

"By default, the decryptor will pre-populate the locations to decrypt with the currently connected drives and network drives."

This Diavol ransomware decryption tool will keep the files encrypted in the attack as a failsafe if the decrypted files are not identical to the original documents.

Additionally, it comes with an "Allow partial decryption of large files," needed to partially recover some files larger than the pair of files provided for reconstructing the encryption keys. This is required because the decryptor might fail to recover such files due to technical limitations.

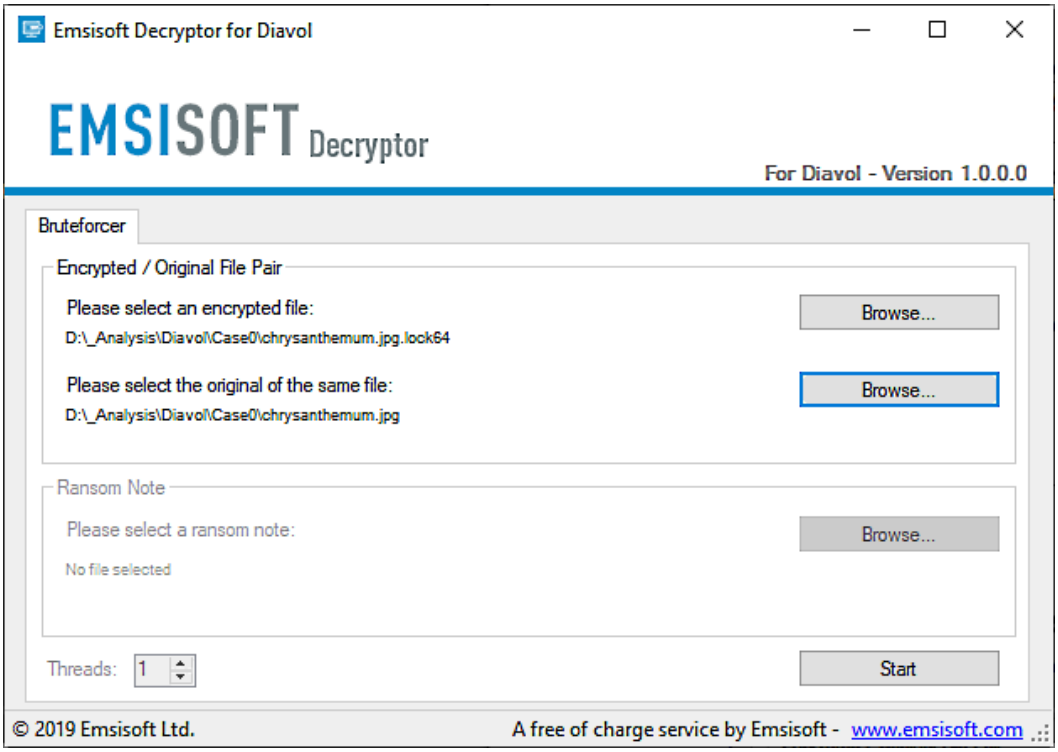


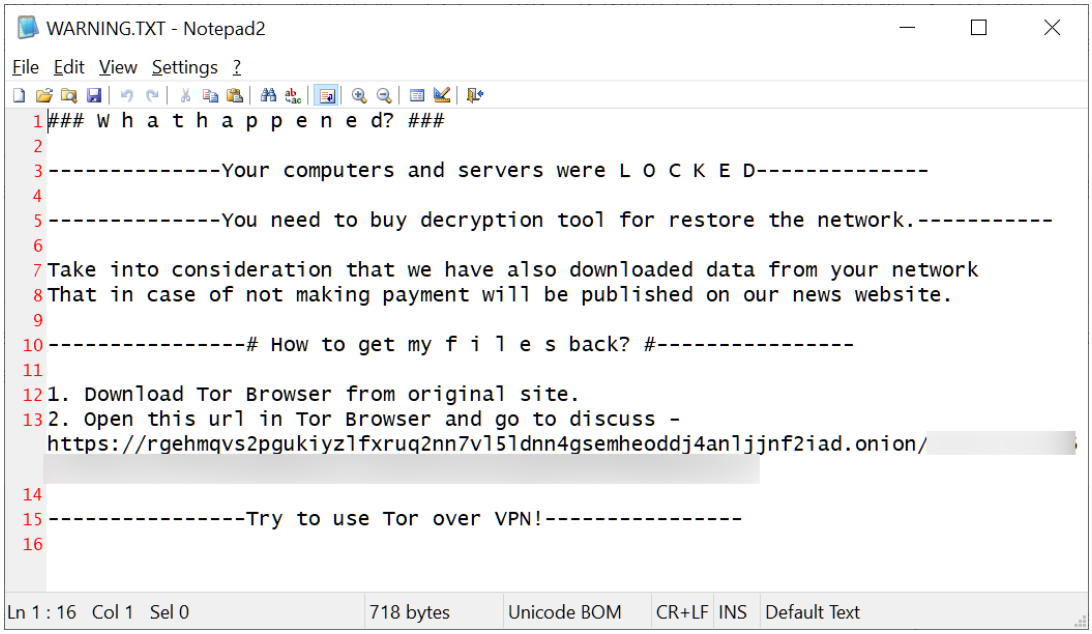
Image: Emsisoft

Unlike other ransomware families that use symmetric algorithms to speed up the encryption process significantly, Diavol's encryption procedure employs user-mode Asynchronous Procedure Calls (APCs) with an asymmetric encryption algorithm.

Diavol also comes with no obfuscation as it doesn't use packing or anti-disassembly tricks, but it still hinders analysis efforts by storing its main routines within bitmap images.

Before the encryption process is done, Diavol will change encrypted Windows devices' backgrounds to a black wallpaper with an "All your files are encrypted! For more information see README-FOR-DECRYPT.txt" message.

Notably, while the Diavol ransomware originally created ransom notes named README_FOR_DECRYPT.txt, as the FBI pointed out, BleepingComputer has seen a switch in November to ransom notes named Warning.txt.



Diavol ransom note (BleepingComputer)

FortiGuard Labs security researchers first tied this ransomware strain to the TrickBot gang (aka Wizard Spider) after spotting it deployed on different systems together with Conti ransomware payloads in an attack blocked by the company's EDR solution in early June 2021.

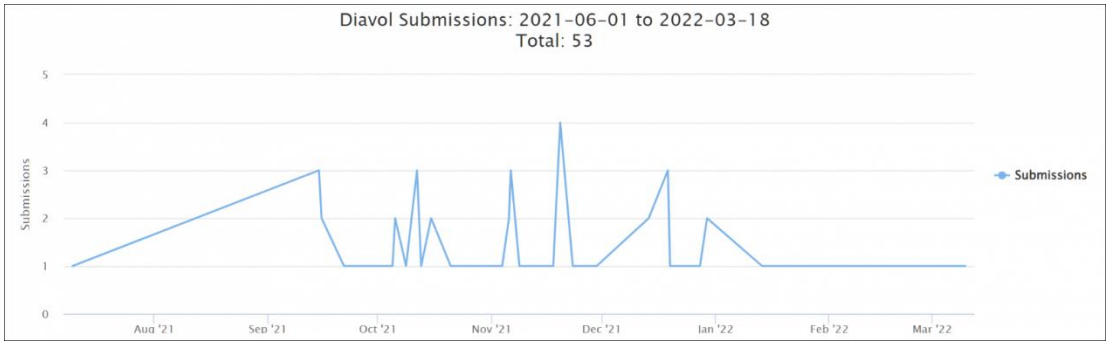
Following their report and likely after the arrest of Alla Witte, who was involved in ransomware development for the malware gang, the FBI also formally linked it to the TrickBot cybercrime gang.

This Russian-based financially motivated cybercrime group operates the Trickbot botnet used to drop second-stage malware on compromised systems and networks.

The FBI first learned of the ransomware strain in October 2021, and, since then, it has seen ransom demands between $10,000 and $500,000, with lower payments accepted following ransom negotiations.

These ransoms are in stark contrast to the massive ransoms demanded by other ransomware gangs linked to TrickBot, including Conti and Ryuk. They have historically requested multi-million dollar payments for decryptors and not leaking stolen data online.

Although active since at least June 2021, Diavol ransomware has never been very active and has only a few dozen submissions on the ID-Ransomware service.



Diavol ransomware activity (BleepingComputer/ID-Ransomware)

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/

10. Lapsus$ Data Kidnappers Claim Snatches From Microsoft, Okta

Lapsus$ shared screenshots of internal Okta systems and 40Gb of purportedly stolen Microsoft data on Bing, Bing Maps and Cortana.

Both Microsoft and Okta are investigating claims by the new, precocious data extortion group Lapsus$ that the gang has breached their systems.

Lapsus$ claimed to have gotten itself "superuser/admin" access to internal systems at authentication firm Okta. It also posted 40GB worth of files to its Telegram channel, including screenshots and source code, of what the group said is Microsoft's internal projects and systems.

The news was first reported by Vice and Reuters.

Okta confirmed on Tuesday that it had been hit and that some customers may have been affected. The scope of the breach isn't yet clear, but it could be huge: According to Okta, it has hundreds of millions of users that use its platform to provide access to networks, including employees at thousands of large companies such as Fedex, Moody's, T-Mobile, Hewlett Packard Enterprise and GrubHub, to name a few.

A Microsoft spokesperson told Threatpost that its investigation found that an account had been compromised, "granting limited access." Its cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity, the spokesperson said.

"We do not rely on the secrecy of code as a security measure and viewing source code isn't tied to elevation of risk," Microsoft said. The Microsoft Threat Intelligence team on Tuesday

published a blog detailing observed activity of the Lapsus$, which Microsoft tracks as DEV-0537.

'Very Worrisome' Screenshots

The purported Okta screenshots included one that appears to show Okta's Slack channels and another with a Cloudflare interface. In an accompanying message, the group said its focus was "ONLY on Okta customers."

Bill Demirkapi, an independent security researcher, tweeted that the screenshots "are very worrisome. … LAPSUS$ appears to have gotten access to the @Cloudflare tenant with the ability to reset employee passwords."

Cloudflare announced on Tuesday that it's not up for risking its employees' Okta credentials. The company, which uses Okta for employee authentication, is resetting its employees credentials, Co-founder and CEO Matthew Prince said on Twitter, "out of an abundance of caution."

> *We are resetting the @Okta credentials of any employees who've changed their passwords in the last 4 months, out of abundance of caution. We've confirmed no compromise. Okta is one layer of security. Given they may have an issue we're evaluating alternatives for that layer.*
>
> *— Matthew Prince (@eastdakota) March 22, 2022*

Breach Dates to January

Demirkapi noted another scary thing about the screenshots: Namely, they indicate a date of Jan. 21, 2022. If the date is correct, it suggests that Okta "failed to publicly acknowledge any breach for at least two months," he said.

> *The screenshots are very worrisome. In the pictures below, LAPSUS$ appears to have gotten access to the @Cloudflare tenant with the ability to reset employee passwords: pic.twitter.com/OZBMenuwgJ*
>
> *— Bill Demirkapi (@BillDemirkapi) March 22, 2022*

Yes, the dates could mean that Lapsus$ has had access to Okta for months, but then again, they could instead indicate that Lapsus$ enjoyed a brief romp before it got kicked out. The latter is the case, Okta CEO Todd McKinnon.

On Tuesday, the CEO tweeted that in January 2022, Okta detected an attempted compromise of "a third-party customer support engineer working for one of our subprocessors" but that "the matter was investigated and contained by the subprocessor."

Okta believes the screenshots Lapsus$ shared online are connected to the January incident. "Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January," McKinnon said.

> *We believe the screenshots shared online are connected to this January event. Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January. (2 of 2)*
>
> *— Todd McKinnon (@toddmckinnon) March 22, 2022*

Did Rogue Employees Pitch In?

If the dates are accurate, it means that Lapsus$ may well have been successful when it put up a "help wanted" notice on its Telegram channel on March 10. The group posted that it recruiting company insiders – including those at Microsoft; other big software/gaming companies such as Apple, IBM or EA; telecoms such as Telefonica, ATT; and more – to help it carry out its dirty work.

From its March 10 Telegram post:

> *"We recruit employees/insider at the following!!!! ... TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk" – references to technologies that the cybercriminals could use to penetrate targets' networks with insiders' help.*

Data on Bing, Bing Maps, Cortana Allegedly Stolen

On Monday, Lapsus$ began to circulate a 10GB compressed archive that purportedly contains internal data on Microsoft's Bing search engine and Bing Maps, along with the source code to the company's voice assistant software Cortana.

The leaked data is dated March 20, 2022.

"Bing maps is 90% complete dump. Bing and Cortana around 45%," Lapsus$ wrote on its Telegram channel.

Microsoft acknowledged the claims and said that it's investigating.

Lapsus$ Sneers at Okta's Claims

On Tuesday, Okta Chief Security Officer David Bradbury made a number of claims In an updated statement that, within hours, Lapsus$ dismissed. Demirkapi tweeted the group's slap-back:

> *The LAPSUS$ ransomware group has issued the following response to Okta's statement. pic.twitter.com/D6KYQjnKPU*

— Bill Demirkapi (@BillDemirkapi) March 22, 2022

Among other things, Lapsus$ scorned Bradbury's description of the group having breached an engineer's laptop in the January attempt (it was a thin client, the gang said). The gang also laughed at Bradbury's claim that the January attempt to access an engineer's account was unsuccessful ("I'm STILL unsure of how its an unsuccessful attempt? Logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients isn't successful?").

Lapsus$ also said that "the potential impact to Okta customers is NOT limited. I'm pretty sure that resetting passwords and MFA would result in complete compromise of many clients systems."

032822 11:01 UPDATE: In a March 23 update, Bradbury clarified that most support engineering tasks are performed using an internally built app called SuperUser, or SU for short. With the role of SU, support engineers can perform perform basic management functions of Okta customer tenants.. he said.

"This does not provide 'god-like access' to all its users," Bradbury explained. "This is an application built with least privilege in mind to ensure that support engineers are granted only the specific access they require to perform their roles. They are unable to create or delete users. They cannot download customer databases. They cannot access our source code repositories."

The Many Notches on Lapsus$' Belt

The Lapsus$ group has pulled off a mounting pile of high-profile attacks. In December, it attacked the Brazil Ministry of Health, taking down several online entities, successfully wiping out information on citizens' COVID-19 vaccination data as well as disrupting the system that issues digital vaccination certificates.

More recently, Lapsus$ crippled the Portuguese media giant Impresa; attacked Nvidia, making off with code-signing certificates then used to sign malware and thus enabling malicious programs to slide past security safeguards on Windows machines; released a purportedly massive dump of proprietary source code stolen from Samsung; and attacked Assassin's Creed video game developer Ubisoft.

On Monday, the group also claimed to have breached the electronics giant LGE, according to Security Week.

Lapsus$ Is a 'Wild Card'

Drew Schmitt, Lapsus$ ransomware expert and principal threat intelligence analyst at cybersecurity firm GuidePoint Security, has interacted directly with the group through his years of ransomware negotiations and threat intelligence work.

He told Threatpost on Tuesday that the group is a "wild card" in that "they do not perform encryption of files or data for extortion purposes, rather they target and exfiltrate sensitive data and use that for the primary extortion effort."

That sets Lapsus$ from the traditional ransomware approach used by groups such as Conti, Lockbit and others he said. Another deviation from traditional ransomware groups is their use of Telegram for communication and extortion purposes versus the use of a leak site hosted using a TOR service, he noted. As well, their initial access to targeted organizations is unorthodox, he said, referring to the March 11 recruiting message for rogue insiders.

Lapsus$ apparently operates on its own, without ties to other cybercriminal/ransomware syndicates or nation-state sponsorship, Schmitt said. That could change, though, as analysis continues, he said: "As this group has gained a lot of notoriety in the past few weeks, it is possible that we will learn new intelligence that indicates connections to other known groups and syndicates."

Schmitt said that Lapsus$ is changing the ransomware game with its non-traditional approaches to initial access, its move away from file encryption, and its deviation from the traditional leak site infrastructure. These are changes that could be adopted by more traditional ransomware groups, he predicted.

Not Just the New Kid on the Block

The Lapsus$ group's move on Okta makes it clear that these guys are more than simply the new kid on the block, according to security experts.

Dave Stapleton, a former government security analyst and current CISO of third-party risk management company CyberGRX, thinks that Lapsus$ is looking to increase its notoriety – all the better to recruit insiders willing to sell remote access to major technology corporations. Yet another far-reaching supply-chain attack could also be in its sites, he told Threatpost on Tuesday.

"While details are scarce at the moment, it is clear that this threat actor is working hard to make a name for themselves," Stapleton said via email. "Continuing to increase their notoriety and standing will support their recruitment of insiders who are willing to sell remote access to major technology corporations and ISPs. With this latest move against Okta, the Lapsus$ group is essentially advertising to potential recruits how they operate."

Given that Okta is "a crucial identity provider for organizations around the world," Stapleton fears another in the string of supply-chain attacks that have struck the likes of Toyota, et al. "I'm sure [Okta's] customers will be watching closely. The threat of another far-reaching supply chain attack certainly has my attention," he said.

Kevin Novak, managing director of Breakwater Solutions, suspects that the scope of Okta's backend breach is likely limited. Otherwise, given Okta's massive customer base, we'd likely know it by now. "While some have made conjectures about whether this hack contributed to

another breach here or there, it would seem that a full compromise of Okta's backend would have become far more obvious by now, but we'll see more over the next few months," he said.

"If … the compromise involved a successful assault on client information, such as client credentialing, key materials, or source code pertaining to environments that may lead to client compromises, then Okta may suffer much greater scrutiny from the field for its lack of adequate, timely notification of the event," Novak noted.

What to Do Now

The Okta breach is still developing. Still, there are steps organizations can take now to secure their employees and networks. Jon Hencinski, director of global operations at Expel, told Threatpost that precautionary actions to take immediately include rotating privileged Okta passwords and Okta-generated tokens and reviewing Okta admin authentications and activity for the past four months.

He provided these other tips:

- Review configuration changes to ensure they align with expected activities and sources.
- Review admin authentications and ensure they originate from expected sources based on the source user.
- Identify any Okta accounts where MFA was disabled during the same time period and determine the user and root cause of that disablement, then re-enable MFA for those accounts.
- Throughout this process, communicate transparently what you're doing and have done with your internal and external stakeholders.
- This is also an opportunity to stress-test your incident response plan (IRP). And if you don't have an IRP — create one, then test it and test it again.

"Fortune favors the prepared," Hencinski said.

Source: https://threatpost.com/lapsus-data-kidnappers-claim-snatches-from-microsoft-okta/179041/

11. Hacked WordPress sites force visitors to DDoS Ukrainian targets

Hackers are compromising WordPress sites to insert a malicious script that uses visitors' browsers to perform distributed denial-of-service attacks on Ukrainian websites.

Today, MalwareHunterTeam discovered a WordPress site compromised to use this script, targeting ten websites with Distributed Denial of Service (DDoS) attacks.

These websites include Ukrainian government agencies, think tanks, recruitment sites for the International Legion of Defense of Ukraine, financial sites, and other pro-Ukrainian sites.

The complete list of targeted websites is below:

```
https://stop-russian-desinformation.near.page
https://gfsis.org/
http://93.79.82.132/
http://195.66.140.252/
https://kordon.io/
https://war.ukraine.ua/
https://www.fightforua.org/
https://bank.gov.ua/
https://liqpay.ua
https://edmo.eu
```

When loaded, the JavaScript will force the visitor's browser to perform HTTP GET requests to each of the listed sites, with no more 1,000 concurrent connections at a time.

> *The website of @IformaRedsocial, https://iforma[.]es/, looks got hacked as it is currently includes a script to attempt DDoS Ukrainian / Ukraine related domains/IPs...*
> *cc @0xDanielLopez pic.twitter.com/9cpAgvBiGg*
>
> *— MalwareHunterTeam (@malwrhunterteam) March 28, 2022*

The DDoS attacks will occur in the background without the user knowing it's happening, other than a slow down of their browser.

This allows the scripts to perform the DDoS attacks while the visitor is unaware that their browser has been coopted for an attack.

Each request to the targeted websites will utilize a random query string so that the request is not served through a caching service, such as Cloudflare or Akamai, and is directly received by the server being attacked.`1

For example, the DDoS script will generate requests like the following in a web server's access logs:

```
"GET /?17.650025158868488 HTTP/1.1"
"GET /?932.8529889504794 HTTP/1.1"
"GET /?71.59119445542395 HTTP/1.1"
```

BleepingComputer has only been able to find a few sites infected with this DDoS script. However, developer Andrii Savchenko states that hundreds of WordPress sites are compromised to conduct these attacks.

"There's about hundred of them actually. All through the WP vulns. Unfortunately, many providers/owners doesn't react," tweeted Savchenko.

Avast also saw the same script on compromised websites as far back as March 7th.

When researching the script to find other infected sites, BleepingComputer discovered that the same script, which was shared on GitHub, is being used by the pro-Ukrainian site, https://stop-

russian-desinformation.near.page. However, this website is used to conduct attacks on Russian targets.

When visiting the site, users' browsers are used to conduct DDoS attacks on 67 Russian websites.

While this site clarifies that it will use visitors' browsers to conduct DDoS attacks against Russian websites, the compromised WordPress sites use the scripts without the website owners' or their visitors' knowledge.

Source: https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/

12. Cyberattackers Target UPS Backup Power Devices in Mission-Critical Environments

The active attacks could result in critical-infrastructure damage, business disruption, lateral movement and more.

Cyberattackers are targeting uninterruptible power supply (UPS) devices, which provide battery backup power during power surges and outages. UPS devices are usually used in mission-critical environments, safeguarding critical infrastructure installations and important computer systems and IT equipment, so the stakes are high.

That's according to the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy, which warned that malicious types are going after internet-connected versions of UPS via default usernames and passwords, mostly – though vulnerabilities, like the TLStorm bugs disclosed earlier this month – are also in the attacker toolbox.

"In recent years, UPS vendors have added an Internet of Things [IoT] capability, and UPSs are routinely attached to networks for power monitoring, routine maintenance and/or convenience," according to a Tuesday alert from CISA (PDF). "Loads for UPSs can range from small (e.g., a few servers) to large (e.g., a building) to massive (e.g., a data center)."

If attackers are able to remotely take over the devices, they can be used for a host of nefarious ends. For instance, bad actors can use them as a jumping-off point to breach a company's internal network and steal data. Or, in a grimmer scenario, they could be used to cut power for mission-critical appliances, equipment or services, which could cause physical injury in an industrial environment, or disrupt business services, leading to significant financial losses.

Further, cyberattackers could also execute remote code to alter the operation of the UPSs themselves, or physically damage them (or the devices connected to them).

"It's easy to forget that every device connected to the internet is at increased risk of attack," Tim Erlin, vice president of strategy at Tripwire, noted via email. "Just because a vendor provides the capability to put a device on the internet, doesn't mean that it's set up to be secure. It's up to each organization to ensure that the systems they deploy are configured securely."

An Easy Fix

Thus, those responsible for UPS upkeep (which CISA noted could include IT staff, building operations people, industrial maintenance workers or third-party contractors from monitoring services) have an easy fix for this one: Enumerating all connected UPSs and similar systems and simply take them offline.

If maintaining an active IoT connection is a requirement, admins should change the default credentials to a strong user-name-and-password combo – and preferably, implement multifactor authentication (MFA) too, CISA added. And other mitigations, according to CISA, include ensuring UPSs are behind a virtual private network (VPN), and adopting login timeout/lockout features so that the devices aren't continually online and open to the world.

"The use of a default username and password to maliciously access a system isn't a new technique," said Erlin. "If you're responding to this advisory by updating the credentials for your UPS systems, take the follow-up step to ensure that other systems aren't using default credentials as well."

Source: https://threatpost.com/cyberattackers-ups-backup-power-critical-environments/179169/

13. Globant confirms hack after Lapsus$ leaks 70GB of stolen data

IT and software consultancy firm Globant has confirmed that they were breached by the Lapsus$ data extortion group, where data consisting of administrator credentials and source code was leaked by the threat actors.

As part of the leak, the hacking group released a 70GB archive of data stolen from Globant, describing it as "some customers source code."

Source code and private keys

Globant is an IT and software development firm with over 16,000 employees worldwide and $1.2 billion in revenue for 2021.

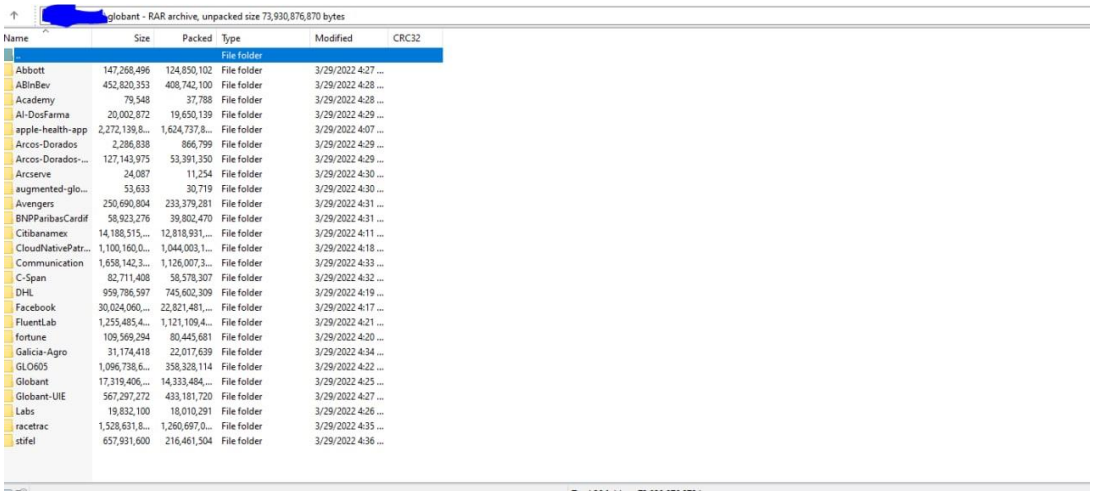
Founded in Buenos Aires, Argentina, Globant is currently headquartered in Luxembourg and boasts a well-known list of customers, including Metropolitan Police, SmileDirectClub, Autodesk, Electronic Arts, Santander, Interbank, Royal Carribbean, and many more.

Following the leak from Lapsus$, Globant issued a press release confirming that some of the company source code has been exposed to an unauthorized party.

“We have recently detected that a limited section of our company's code repository has been subject to unauthorized access” - Globant

Among the data published by Lapsus$, there is a screenshot the group claims to be of an archived directory from Globant, containing folder names that appear to be company customers.

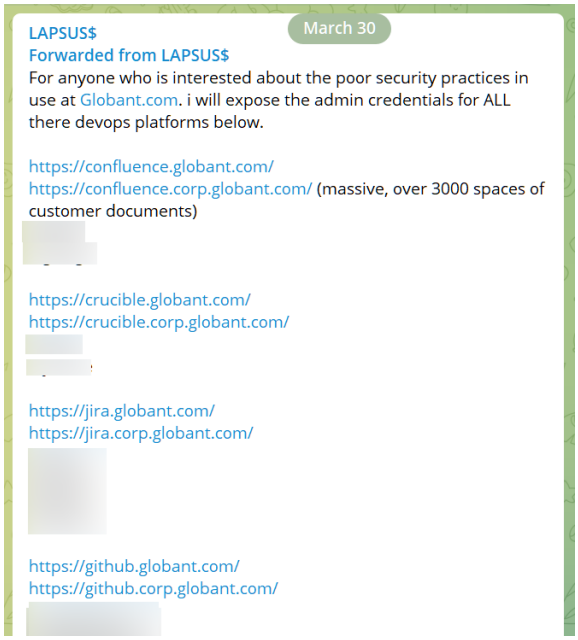
Some of the source code folders listed in the screenshot include, Abbott, apple-health-app, C-span, Fortune, Facebook, DHL, and Arcserve.


[redacted]globant - RAR archive, unpacked size 73,930,876,870 bytes

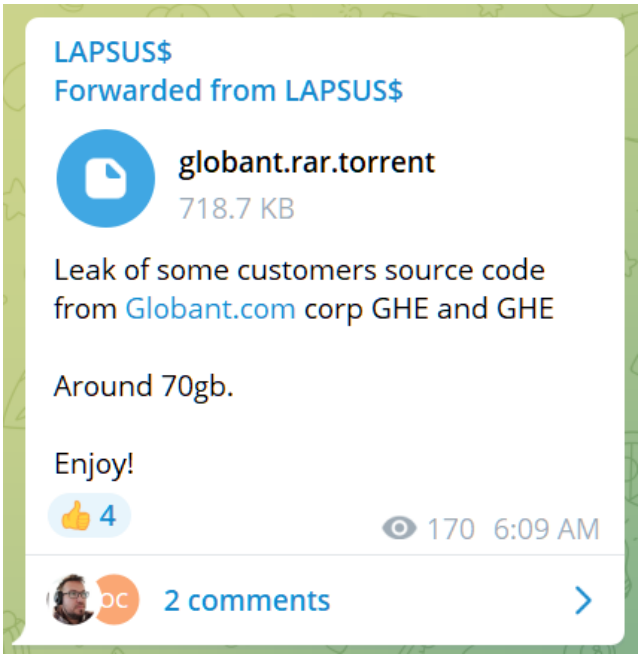
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Abbott	147,268,496	124,850,102	File folder	3/29/2022 4:27 ...	
ABInBev	452,820,353	408,742,100	File folder	3/29/2022 4:28 ...	
Academy	79,548	37,788	File folder	3/29/2022 4:28 ...	
Al-DosFarma	20,002,872	19,650,139	File folder	3/29/2022 4:29 ...	
apple-health-app	2,272,139,8...	1,624,737,8...	File folder	3/29/2022 4:07 ...	
Arcos-Dorados	2,286,838	866,799	File folder	3/29/2022 4:29 ...	
Arcos-Dorados-...	127,143,975	53,391,350	File folder	3/29/2022 4:29 ...	
Arcserve	24,087	11,254	File folder	3/29/2022 4:30 ...	
augmented-glo...	53,633	30,719	File folder	3/29/2022 4:30 ...	
Avengers	250,690,804	233,379,281	File folder	3/29/2022 4:31 ...	
BNPParibasCardif	58,923,276	39,802,470	File folder	3/29/2022 4:31 ...	
Citibanamex	14,188,515,...	12,818,931,...	File folder	3/29/2022 4:11 ...	
CloudNativePatr...	1,100,160,0...	1,044,003,1...	File folder	3/29/2022 4:18 ...	
Communication	1,658,142,3...	1,126,007,3...	File folder	3/29/2022 4:33 ...	
C-Span	82,711,408	58,578,307	File folder	3/29/2022 4:32 ...	
DHL	959,786,597	745,602,309	File folder	3/29/2022 4:19 ...	
Facebook	30,024,060,...	22,821,481,...	File folder	3/29/2022 4:17 ...	
FluentLab	1,255,485,4...	1,121,109,4...	File folder	3/29/2022 4:21 ...	
fortune	109,569,294	80,445,681	File folder	3/29/2022 4:20 ...	
Galicia-Agro	31,174,418	22,017,639	File folder	3/29/2022 4:34 ...	
GLO605	1,096,738,6...	358,328,114	File folder	3/29/2022 4:22 ...	
Globant	17,319,406,...	14,333,484,...	File folder	3/29/2022 4:25 ...	
Globant-UIE	567,297,272	433,181,720	File folder	3/29/2022 4:27 ...	
Labs	19,832,100	18,010,291	File folder	3/29/2022 4:26 ...	
racetrac	1,528,631,8...	1,260,697,0...	File folder	3/29/2022 4:35 ...	
stifel	657,931,600	216,461,504	File folder	3/29/2022 4:36 ...	

The metadata for the entries shows that the folders have been modified on March 29, which could indicate when the data was stolen.

In a follow-up post, Lapsus$ published a set of credentials for what they say give administrator access to various platforms used by Globant for developing, reviewing, and collaborating on customer code (Jira, Confluence, GitHub, Crucible).



A third post from the gang today shared a torrent file for about 70GB of data stolen from Globant. The company says that the intruder on its systems accessed "certain source code and project-related documentation for a very limited number of clients."



The damage appears to be significant.

According to threat intelligence company SOS Intelligence, the leaked data contains customer information as well as a code repositories with a large number of private keys (full chain, web server SSL certificates, Globant server, API keys).

One of the repositories is for the Bluecap app for consultancy in the financial sector, that Globant acquired in late 2020.

The cache that Lapsus$ leaked also includes a little over 150 SQL database files for various customer applications, SOS Intelligence says.

"In terms of legitimacy, going just by volume alone it's hard to fabricate that amount of data - however samples of the data have been cross referenced with live systems and other methods that show the leak is legitimate and very significant as far as Globant and Globant's impacted customers are concerned" - SOS Intelligence

Globant said today that its investigation into the incident did not reveal any evidence that the hackers compromised other parts of its infrastructure system.

Lapsus$ on LE radar

The Lapsus$ data extortion group has been constantly making the news due to their attacks on big technological companies, like Microsoft, Nvidia, Samsung, Okta, Ubisoft, many of them resulting in big data leaks.

Despite the big names on their victim list, Lapsus$ is believed to be formed mainly by teenagers exercising their hacking skills driven mainly by making a name on the hacking scene, not by financial motivation.

The group has been on the radar of law enforcement for a while and some individuals, all teens believed to be connected to Lapsus$, have been arrested in the U.K.

The FBI is also investigating the activities of the group and has asked the public for any information leading to identifying Lapsus$ members involved in the compromise of computer networks from U.S.-based companies.

SEEKING INFORMATION

LAPSUS$

Cyber Intrusions of United States-Based Technology Companies
March 21, 2022

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of computer networks belonging to United States-based technology companies.

On March 21, 2022, individuals from a group identifying themselves as Lapsus$ posted on a social media platform and alleged to have stolen source code from a number of United States-based technology companies. These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Francisco

However, it is unclear how many active members are in the group and what roles they play.

It is believed that Lapsus$ has affiliates all over the world, as their Telegram chats seem to suggest that some of them speak English, Russian, Turkish, German, and Portuguese.

Source: https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/

14. QNAP Customers Adrift, Waiting on Fix for OpenSSL Bug

Bottom of Form

QNAP is warning clients that a recently disclosed vulnerability affects most of its NAS devices, with no mitigation available while the vendor readies a patch.

Customers of Taiwan-based QNAP Systems are in a bit of limbo, waiting until the company releases a patch for an OpenSSL bug that the company has warned affects most of its network-attached storage (NAS) devices. The vulnerability can trigger an infinite loop that creates a denial-of-service (DoS) scenario.

Though the bug – tracked as CVE-2022-0778 and rated 7.5 (high severity) on the CVSS severity-rating scale – has been patched by OpenSSL, QNAP hasn't gotten around to applying a fix yet for its NAS devices affected by the vulnerability. The company is telling customers that "there is no mitigation available" and they "must check back and install security updates as soon as they become available."

"QNAP is thoroughly investigating the case," the company said. "We will release security updates and provide further information as soon as possible."

The vulnerability is in OpenSSL's BN_mod_sqrt() function, which computes a modular square root. The bug can be triggered by crafting a certificate that has invalid explicit curve parameters, causing the function to loop forever, according to its listing in the NIST National Vulnerability Database. This creates DoS conditions on the device, according to OpenSSL. OpenSSL is a popular cryptography library primarily used by networking software that offers open-source application of the TLS protocol.

"Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack," according to the listing. "The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters."

Vulnerable scenarios on devices using OpenSSL include:

- TLS clients consuming server certificates,
- TLS servers consuming client certificates,
- Hosting providers taking certificates or private keys from customers,
- Certificate authorities parsing certification requests from subscribers, or
- Anything else that parses ASN.1 elliptic curve parameters.

QNAP devices affected by the bug are:

- QTS 5.0.x and later
- QTS 4.5.4 and later
- QTS 4.3.6 and later
- QTS 4.3.4 and later
- QTS 4.3.3 and later
- QTS 4.2.6 and later
- QuTS hero h5.0.x and later
- QuTS hero h4.5.4 and later
- QuTScloud c5.0.x

Though QNAP said it's not aware of any exploits for the bug, a security advisory issued by Italy's national cybersecurity agency, CSIRT, suggests that it already is being exploited in the wild.

QNAP Under Fire

QNAP devices have indeed had their share of cybersecurity woes in the past several months, a number of which are ongoing.

As the company readies a fix for the OpenSSL flaw, it's also working on another patch for the so-called Dirty Pipe Linux kernel flaw discovered earlier this month, which also currently has no mitigation on QNAP NAS devices. The flaw, a local privilege-escalation vulnerability, affects the Linux kernel on QNAP NAS running QTS 5.0.x and QuTS hero h5.0.x.

Attackers also have been pummeling QNAP devices with both ransomware and brute-force attacks since the beginning of the year, the latter of which prompted the vendor to urge customers to get their internet-exposed NAS devices off the internet.

In late January, QNAP forced out an unexpected and not entirely welcome update to its customers' NAS devices after warning them that the DeadBolt ransomware was mounting an offensive against them. And just last week, reports surfaced that DeadBolt was at it again in a new wave of attacks against QNAP.

The current OpenSSL scenario also is not the first time the vendor's devices were rattled by a flaw in the cryptography library. Last August, two vulnerabilities tracked as CVE-2021-3711 and CVE-2021-3712 that respectively could cause remote-code execution (RCE) and DoS also prompted a security advisory and eventually emergency patches by QNAP.

Source: https://threatpost.com/qnap-customers-adrift-fix-openssl-bug/179197/

15. Spring patches leaked Spring4Shell zero-day RCE vulnerability

Spring released emergency updates to fix the 'Spring4Shell' zero-day remote code execution vulnerability, which leaked prematurely online before a patch was released.

Yesterday, an exploit for a zero-day remote code execution vulnerability in the Spring Framework dubbed 'Spring4Shell' was briefly published on GitHub and then removed.

However, as nothing stays hidden on the Internet, the code was quickly shared in other repositories and tested by security researchers, who confirmed it was a legitimate exploit for a new vulnerability.

Today, Spring has released a security advisory explaining that the vulnerability is now tracked as CVE-2022-22965 and impacts Spring MVC and Spring WebFlux applications on JDK 9.

The exploitation of the vulnerability also requires Apache Tomcat, an application packaged as a WAR, and the spring-webmvc or spring-webflux dependencies.

"The vulnerability impacts Spring MVC and Spring WebFlux applications running on JDK 9+. The specific exploit requires the application to run on Tomcat as a WAR deployment," reads the Spring advisory.

"If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it."

Spring says that the vulnerability was responsibly disclosed to them on Tuesday by odeplutos, meizjm3i of AntGroup FG, and they had been developing and testing a fix that was expected to be released today.

However, after a security researcher published the full details online on Wednesday, they pushed the release of the patch forward ahead of the planned release.

The Spring versions that fix the new vulnerability are listed below, with all except Spring Boot available on Maven Central:

- Spring Framework 5.3.18 and Spring Framework 5.2.20
- Spring Boot 2.5.12
- Spring Boot 2.6.6 (not available yet)

Spring Boot 2.6.6 should be released within the next few hours.

While the vulnerability has specific requirements to be exploited, Will Dormann, a vulnerability analyst at CERT/CC, found that even sample code from spring.io was vulnerable.

As developers commonly use sample code as a template for their own apps, there could be many vulnerable apps accessible online.

Spring admins should prioritize deploying these security updates as soon as possible, as Spring4Shell scanners have already been created, and there are reports of the vulnerability already being actively exploited in the wild.

Source: https://www.bleepingcomputer.com/news/security/spring-patches-leaked-spring4shell-zero-day-rce-vulnerability/

16. Viasat confirms satellite modems were wiped with AcidRain malware

A newly discovered data wiper malware that wipes routers and modems has been deployed in the cyberattack that targeted the KA-SAT satellite broadband service to wipe SATCOM modems on February 24, affecting thousands in Ukraine and tens of thousands more across Europe.

The malware, dubbed AcidRain by researchers at SentinelOne, is designed to brute-force device file names and wipe every file it can find, making it easy to redeploy in future attacks.

SentinelOne says this might hint at the attackers' lack of familiarity with the targeted devices' filesystem and firmware or their intent to develop a reusable tool.

AcidRain was first spotted on March 15 after its upload onto the VirusTotal malware analysis platform from an IP address in Italy as a 32-bit MIPS ELF binary using the "ukrop" filename.

Once deployed, it goes through the compromised router or modem's entire filesystem. It also wipes flash memory, SD/MMC cards, and any virtual block devices it can find, using all possible device identifiers.

"The binary performs an in-depth wipe of the filesystem and various known storage device files. If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files in the filesystem," SentinelOne threat researchers Juan Andres Guerrero-Saade and Max van Amerongen explained.

To destroy data on compromised devices, the wiper overwrites file contents with up to 0x40000 bytes of data or uses MEMGETINFO, MEMUNLOCK, MEMERASE, and MEMWRITEOOB input/output control (IOCTL) system calls.

After AcidRain's data wiping processes are completed, the malware reboots the device, rendering it unusable.

Used to wipe satellite communication modems in Ukraine

Based on the name of the AcidRain binary uploaded to VirusTotal, which could be an abbreviation of "Ukraine Operation," SentinelOne said the malware might have been

developed explicitly for an operation against Ukraine and likely used to wipe modems in the KA-SAT cyberattack.

"The threat actor used the KA-SAT management mechanism in a supply-chain attack to push a wiper designed for modems and routers," SentinelOne hypothesized.

"A wiper for this kind of device would overwrite key data in the modem's flash memory, rendering it inoperable and in need of reflashing or replacing."

This directly contradicts a Viasat incident report on the KA-SAT incident saying it found "no evidence of any compromise or tampering with Viasat modem software or firmware images and no evidence of any supply-chain interference."

However, Viasat confirmed SentinelOne's hypothesis, saying the data destroying malware was deployed on modems using "legitimate management" commands.

"The analysis in the SentinelLabs report regarding the ukrop binary is consistent with the facts in our report - specifically, SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described," a Viasat spokesperson told BleepingComputer.

"We expect we can provide additional forensic details when this investigation is complete."

The use of AcidRain to wipe modems was also confirmed by security researcher Ruben Santamarta who dumped the flash memory of a SATCOM modem corrupted in the attack against KA-SAT.

As SentinelOne says, the destructive pattern observed by Santamarta matches the output of AcidRain's overwriting wiper method.

If you're wondering what that might look like...https://t.co/vbCNsgcwtz

— J. A. Guerrero-Saade (@juanandres_gs) March 31, 2022

The fact that Viasat shipped almost 30,000 modems since the February 2022 attack to bring customers back online and continues to even more to expedite service restoration also hints that SentinelOne's supply-chain attack theory holds water.

As a side note, the IOCTLs used by this malware also match the ones used by the VPNFilter malware 'dstr' wiper plugin, a malicious tool attributed to Russian GRU hackers (Fancy Bear or Sandworm).

Seventh data wiper deployed against Ukraine this year

AcidRain is the seventh data wiper malware deployed in attacks against Ukraine, with six others having been used to target the country since the start of the year.

The Computer Emergency Response Team of Ukraine recently reported that a data wiper it tracks as DoubleZero has been deployed in attacks targeting Ukrainian enterprises.

One day before the Russian invasion of Ukraine started, ESET spotted a data-wiping malware now known as HermeticWiper, that was used against organizations in Ukraine together with ransomware decoys.

The day Russia invaded Ukraine, they also discovered a data wiper dubbed IsaacWiper and a new worm named HermeticWizard used to drop HermeticWiper payloads.

ESET also spotted a fourth data-destroying malware strain they dubbed CaddyWiper, a wiper that deletes user data and partition information from attached drivers and also wipes data across Windows domains it's deployed on.

A fifth wiper malware, tracked as WhisperKill, was spotted by Ukraine's State Service for Communications and Information Protection (CIP), who said it reused 80% of the Encrpt3d Ransomware's code (also known as WhiteBlackCrypt Ransomware).

In mid-January, Microsoft found a sixth wiper now tracked as WhisperGate, used in data-wiping attacks against Ukraine, disguised as ransomware.

Update: A Viasat spokesperson sent the following statement after the story was published:

> The facts provided in the Viasat Incident Report yesterday are accurate. The analysis in the SentinelLabs report regarding the ukrop binary is consistent with the facts in our report - specifically, SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described.
>
> As noted in our report: "the attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously."
>
> Additionally, we don't view this as a supply chain attack or vulnerability. As we noted, "Viasat has no evidence that standard modem software or firmware distribution or update processes involved in normal network operations were used or compromised in the attack." Further, "there is no evidence that any end-user data was accessed or compromised."
>
> Due to the ongoing investigation and to ensure the security of our systems from ongoing attack, we cannot publicly share all forensic details of the event. Through this process, we have been, and continue to cooperate with various law enforcement and government agencies around the world, who've had access to details of the event.
>
> We expect we can provide additional forensic details when this investigation is complete.

Source: https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/

17. Apple emergency update fixes zero-days used to hack iPhones, Macs

Apple has released security updates on Thursday to address two zero-day vulnerabilities exploited by attackers to hack iPhones, iPads, and Macs.

Zero-day security bugs are flaws the software vendor is unaware of and hasn't patched. In some cases, they also have publicly available proof-of-concept exploits or may be actively exploited in the wild.

In security advisories published today, Apple said that they're aware of reports the issues "may have been actively exploited."

The two flaws are an out-of-bounds write issue (CVE-2022-22674) in the Intel Graphics Driver that allows apps to read kernel memory and an out-of-bounds read issue (CVE-2022-22675) in the AppleAVD media decoder that will enable apps to execute arbitrary code with kernel privileges.

The bugs were reported by anonymous researchers and fixed by Apple in iOS 15.4.1, iPadOS 15.4.1, and macOS Monterey 12.3.1 with improved input validation and bounds checking, respectively.

The list of impacted devices includes:

- Macs running macOS Monterey
- iPhone 6s and later
- iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation).

Apple disclosed active exploitation in the wild, however, it did not release any additional info regarding these attacks.

Withholding this information is likely designed to allow the security updates to reach as many iPhones, iPads, and Macs as possible before threat actors pick up on the details and start abusing the now-patched zero-days.

Even though these zero-days were likely only used in targeted attacks, it's still strongly advised to install today's security updates as soon as possible to block potential attack attempts.

Five zero-days patched by Apple this year

In January, Apple patched two more actively exploited zero-days that can enable attackers to achieve arbitrary code execution with kernel privileges (CVE-2022-22587) and track web browsing activity and the users' identities in real-time (CVE-2022-22594).

In February, Apple released security updates to fix a new zero-day bug exploited to hack iPhones, iPads, and Macs, leading to OS crashes and remote code execution on compromised devices after processing maliciously crafted web content.

These first three zero-days also impacted iPhones (iPhone 6s and up), Macs running macOS Monterey, and multiple iPad models.

The company also had to deal with an almost unending stream of zero-days exploited in the wild to target iOS, iPadOS, and macOS devices throughout 2021.

That list includes multiple flaws used to deploy NSO's Pegasus spyware on iPhones belonging to journalists, activists, and politicians.

Source: https://www.bleepingcomputer.com/news/security/apple-emergency-update-fixes-zero-days-used-to-hack-iphones-macs/

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.