telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

September 2021

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 Business Services 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 Business Services?

- 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

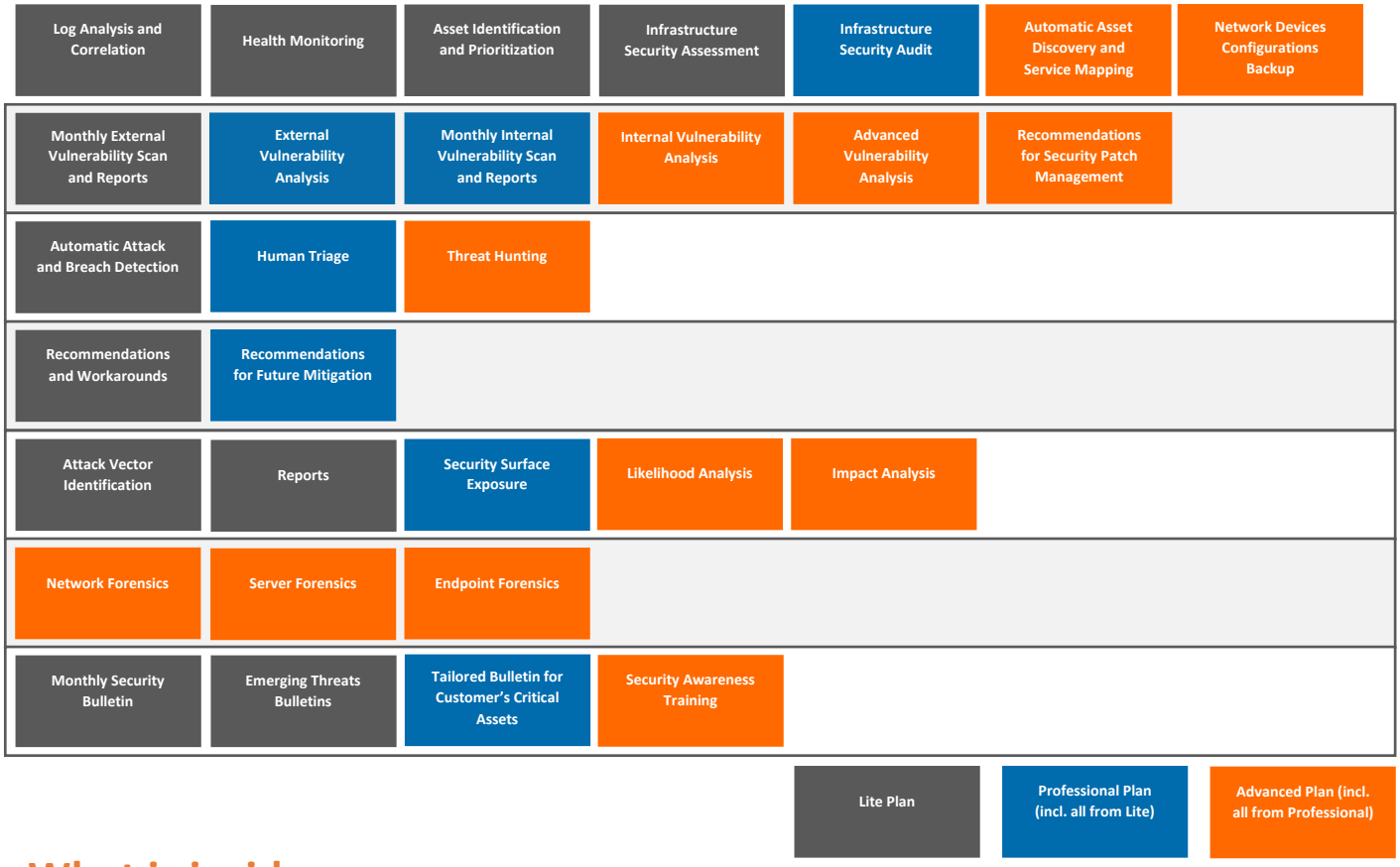
Start to mitigate cyber threats and minimize the risk!

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. Ransomware Volumes Hit Record Highs as 2021 Wears On 4
2. New Cobalt Strike bugs allow takedown of attackers' servers 6
3. Zoom Lied about End-to-End Encryption 8
4. CISA teams up with Microsoft, Google, Amazon to fight ransomware 8
5. Malware campaign uses clever 'captcha' to bypass browser warning 10
6. Liquid cryptocurrency exchange loses $94 million following hack 13
7. Wanted: Disgruntled Employees to Deploy Ransomware 15
8. Hackers can bypass Cisco security products in data theft attacks 19
9. T-Mobile data breach just got worse — now at 54 million customers 20
10. Microsoft Exchange servers being hacked by new LockFile ransomware 22
11. Can Your Wearable Health Monitors Be Compromised? 26
12. Botnet targets hundreds of thousands of devices using Realtek SDK 28
13. Microsoft Spills 38 Million Sensitive Data Records Via Careless Power App Configs 29
14. How to Spot Fake Login Pages 32
15. Ragnarok Ransomware Gang Bites the Dust, Releases Decryptor 35

1. Ransomware Volumes Hit Record Highs as 2021 Wears On

The second quarter of the year saw the highest volumes of ransomware attacks ever, with Ryuk leading the way.

Ransomware has seen a significant uptick so far in 2021, with global attack volume increasing by 151 percent for the first six months of the year as compared with the year-ago half. Meanwhile, the FBI has warned that there are now 100 different strains circulating around the world.

From a hard-number perspective, the ransomware scourge hit a staggering 304.7 million attempted attacks within SonicWall Capture Labs' telemetry. To put that in perspective, the firm logged 304.6 million ransomware attempts for the entirety of 2020.

The top three ransomware strains seen in the wild by the firm are Ryuk, Cerber and SamSam, according to a recent mid-year report from SonicWall.

Top Ransomware Variants

In terms of the three most common types of ransomware, SonicWall researchers recorded 93.9 million instances of Ryuk in the first half, catapulting it to the No. 1 position – a number that's triple the number of Ryuk attempts seen in the first six months of 2020.

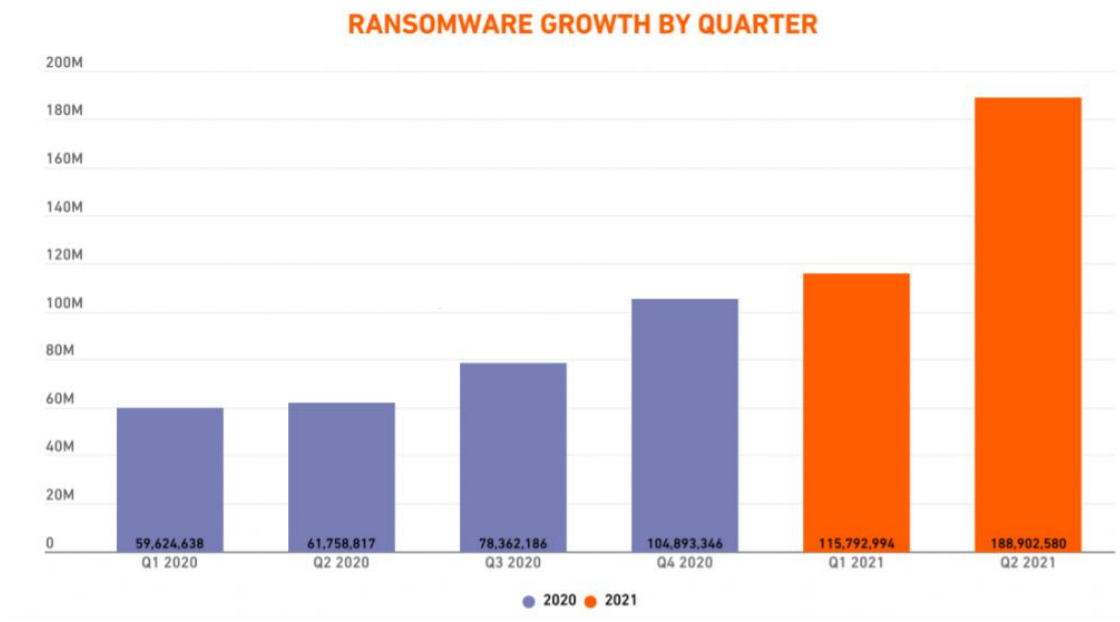
Meanwhile, researchers also saw Cerber used in 52.5 million recorded hits in the first half of 2021. Researchers said that Cerber is definitely on the rise; the number of attacks nearly quadrupled in April, and by May it had risen to nearly five times the levels seen in January.

And finally, there were 49.7 million recorded instances of SamSam in SonicWall's numbers for the first half — more than double the volume seen during the entire year of 2020. June alone saw 15.7 million hits, researchers said, which is more than two-thirds of the 23.5 million SamSam hits seen for all of last year.

Record-Setting Cyberattack Volumes

The level of attacks appears to be increasing, according to SonicWall. Ransomware volume jumped from 115.8 million attacks in Q1 to 188.9 million attacks in Q2.

"Even if we don't record a single ransomware attempt in the entire second half (which is irrationally optimistic), 2021 will already go down as the worst year for ransomware SonicWall has ever recorded," according to the report.



Source: SonicWall.

To boot, every month during the second quarter also set a new record.

"After rising to a new high in April, ransomware rose again in May, then saw another increase in June," researchers said. "During that month, SonicWall recorded 78.4 million ransomware attempts — more than the entire second quarter of 2020, and nearly half the total number of attacks for the year in 2019."

Ransomware: A Global Problem

The report found that ransomware isn't just growing — it's a worldwide problem.

Europe felt the brunt of the spikes in volume, with a 234 percent spike in ransomware attacks in the first half, according to SonicWall. North America wasn't too far behind, with ransomware volume jumping 180 percent in the region.

The news is better for Asia, where ransomware hits were up just 59 percent year-to-date. However, after hitting a high point in March, attack volume began dropping, researchers said. By June, there were only about a fifth as many attacks as there had been three months prior.

While Europe as a region saw the most pain, the U.S. recorded far and away the most ransomware attacks, the analysis found, with attack volume in the U.S. rising 185 percent from the first half last year.

"In fact, of the top 10 countries for ransomware volume, the U.S. had nearly as much ransomware as the other nine put together…times four," according to the report.

Ransomware volume in the second-ranking country, the U.K., rose 144 percent.

Government Most-Targeted Sector

By an overwhelming margin, the most commonly targeted industry in 2021 has been government. By June, government customers were seeing about 10 times more ransomware attempts than the average, according to researchers. However, the devil is in the details when it comes to interpreting this stat.

"Government customers are still seeing a higher-than-average number of ransomware attempts, but in three out of six months during the first half of 2021, education customers saw even more," noted the report.

Source: https://threatpost.com/ransomware-volumes-record-highs-2021/168327/

2. New Cobalt Strike bugs allow takedown of attackers' servers

Security researchers have discovered Cobalt Strike denial of service (DoS) vulnerabilities that allow blocking beacon command-and-control (C2) communication channels and new deployments.

Cobalt Strike is a legitimate penetration testing tool designed to be used as an attack framework by red teams (groups of security professionals who act as attackers on their own organization's infrastructure to discover security gaps and vulnerabilities.)

However, Cobalt Strike is also used by threat actors (commonly seen used during ransomware attacks) for post-exploitation tasks after deploying so-called beacons, which provide them with persistent remote access to compromised devices.

Using these beacons, the attackers can later access the breached servers to harvest data or deploy second-stage malware payloads.

Targets on attackers' infrastructure

SentinelLabs (the threat research team at SentinelOne) found the DoS vulnerabilities collectively tracked as CVE-2021-36798 (and dubbed Hotcobalt) in the latest versions of Cobalt Strike's server.

As they discovered, one can register fake beacons with the server of a particular Cobalt Strike installation. By sending fake tasks (or abnormally large screenshots) to the server, one can crash the server by exhausting available memory.

The crash can render already installed beacons unable to communicate with the C2 server, block new beacons from being installed on infiltrated systems, and interfere with ongoing red team (or malicious) operations that used the deployed beacons.

"This lets a malicious actor cause memory exhaustion on the machine the Cobalt's server (the 'Teamserver') runs on, which makes the server unresponsive until it's restarted," SentinelLabs said.

"This means that live beacons cannot communicate to their C2 until the operators restart the server. Restarting, however, won't be enough to defend against this vulnerability as it is possible to repeatedly target the server until it is patched or the beacon's configuration is changed."

Since Cobalt Strike is also heavily used by threat actors for various nefarious purposes, law enforcement and security researchers can also employ the Hotcobalt vulnerabilities to take down malicious infrastructure.

On April 20, SentinelLabs has disclosed the vulnerabilities to CobaltStrike's parent company HelpSystems, who addressed them in Cobalt Strike 4.4, released earlier today.

HelpSystems also advises those who cannot immediately update to the last Cobalt Strike version to harden their C2 infrastructure by:

- Disabling staging on versions of Cobalt Strike prior to 4.4
- Limiting access to their teamserver infrastructure to only trusted sources

Disclosure Timeline:

04/20/2021 - Initial contact with HelpSystems for issue disclosure.
04/22/2021 - Issue details disclosed to HelpSystems.
04/23/2021 - HelpSystems confirmed the issue and asked for an extension until August 3rd.
04/28/2021 - SentinelOne accepted the extension.
07/18/2021 - Submitted CVE request to MITRE.
07/19/2021 - CVE-2021-36798 was assigned and reserved for the specified issue.
08/02/2021 - SentinelOne shared the publication date and post for review.
08/02/2021 - HelpSystems reviewed and confirmed the post for publication.
08/04/2021 - HelpSystems released Cobalt Strike 4.4, which contains a fix for CVE-2021-36798.

RCE and source code leak

This is not the first vulnerability to affect CobaltStrike, with HelpSystems having patched a directory traversal attack vulnerability in the team server in 2016, leading to remote code execution attacks.

In November 2020, BleepingComputer also reported that the source code for the Cobalt Strike post-exploitation toolkit had allegedly been leaked in a GitHub repository.

As Advanced Intel's Vitali Kremez told BleepingComputer at the time, the leak was most likely the re-compiled source code of the 2019 Cobalt Strike 4.0 version.

Kremez also said that the possible leak of Cobalt Strike source code "has significant consequences for all defenders as it removes barriers of entry to obtaining the tool and essentially makes its easy for the crime groups to procure and modify code as needed on the fly."

While BleepingComputer contacted Cobalt Strike and their parent company Help Systems to confirm the source code's authenticity when the leak was discovered, we haven't heard back.

Source: https://www.bleepingcomputer.com/news/security/new-cobalt-strike-bugs-allow-takedown-of-attackers-servers/

3. Zoom Lied about End-to-End Encryption

The facts aren't news, but Zoom will pay $85M — to the class-action attorneys, and to users — for lying to users about end-to-end encryption, and for giving user data to Facebook and Google without consent.

The proposed settlement would generally give Zoom users $15 or $25 each and was filed Saturday at US District Court for the Northern District of California. It came nine months after Zoom agreed to security improvements and a "prohibition on privacy and security misrepresentations" in a settlement with the Federal Trade Commission, but the FTC settlement didn't include compensation for users.

Source: https://www.schneier.com/blog/archives/2021/08/zoom-lied-about-end-to-end-encryption.html

4. CISA teams up with Microsoft, Google, Amazon to fight ransomware

CISA has announced the launch of Joint Cyber Defense Collaborative (JCDC), a partnership across public and private sectors focused on defending US critical infrastructure from ransomware and other cyber threats.

The new initiative's goal is to allow CISA to develop cyber defense plans in collaboration with federal agencies, SLTT (state, local, tribal and territorial) partners, and private sector orgs for national resilience against malicious cyber activity targeting critical infrastructure.

"The industry partners that have agreed to work side-by-side with CISA and our interagency teammates share the same commitment to defending our country's national critical functions from cyber intrusions, and the imagination to spark new solutions," CISA Director Jen Easterly said.

"With these extraordinarily capable partners, our initial focus will be on efforts to combat ransomware and developing a planning framework to coordinate incidents affecting cloud service providers."

The first industry partners to joint the JCDC include Microsoft, Google Cloud, Amazon Web Services, AT&T, Crowdstrike, FireEye Mandiant, Lumen, Palo Alto Networks, and Verizon, with plans to expand with more private sector and SLTT partners from across sectors.

Government partners already participating include the Department of Defense, the National Security Agency, the Department of Justice, the Federal Bureau of Investigation, the U.S. Cyber Command, and the Office of the Director of National Intelligence, with additional Sector Risk Management Agencies (SRMAs) to join the effort at a later time.

The launch of this parnership between the US public and private sector platform comes after an almost continuous barrage of cyberattacks targeting US government agencies and critical infrastructure, starting with the December 2020 SolarWinds supply-chain attack.

Since the start of 2021, both state-sponsored and financially motivated hacking groups have coordinated widespread attacks on Microsoft Exchange servers worldwide and hit the networks of Colonial Pipeline, JBS Foods, and Kaseya customers in ransomware incidents.

President Joe Biden issued a national security memorandum during late July in response to this stream of attacks, a memorandum designed to help bolster the security of US critical infrastructure by setting baseline performance goals for infrastructure owners and operators.

The US President also warned lasat month that severe security breaches could potentially escalate to a "real shooting war" with another major world power.

"In recent months, various major cyber incidents have had an impact on our critical infrastructure community and caused downstream consequences to Americans that rely on it for everyday functions," CISA said today, after announcing JCDC's formation.

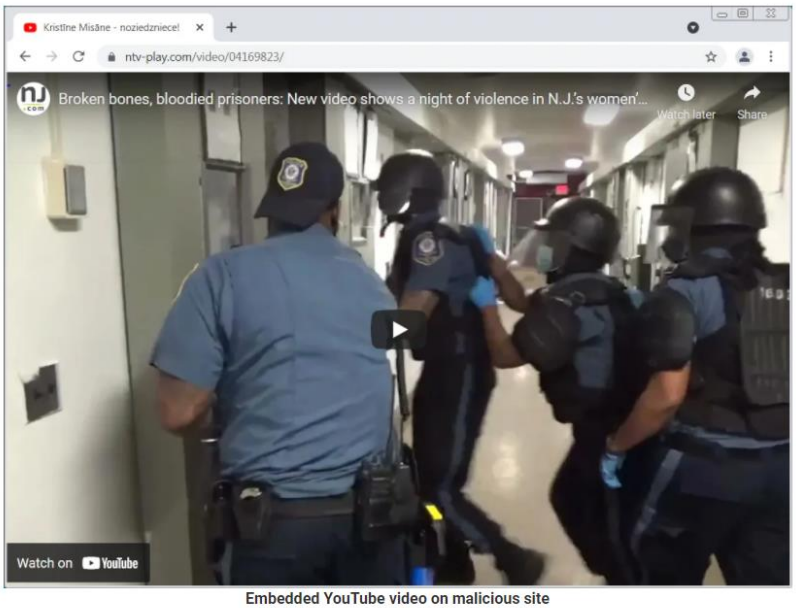
"As a community, the JCDC will deploy innovation, collaboration, and imagination to protect American businesses, government agencies, and our people against cyber intrusions."

Source: https://www.bleepingcomputer.com/news/security/cisa-teams-up-with-microsoft-google-amazon-to-fight-ransomware/

5. Malware campaign uses clever 'captcha' to bypass browser warning

A malware campaign uses a clever captcha prompt to trick users into bypassing browsers warnings to download the Gozi (aka Ursnif) banking trojan.

Yesterday, security researcher MalwareHunterTeam shared a suspicious URL with BleepingComputer that downloads a file when attempting to watch an embedded YouTube video about a New Jersey women's prison.

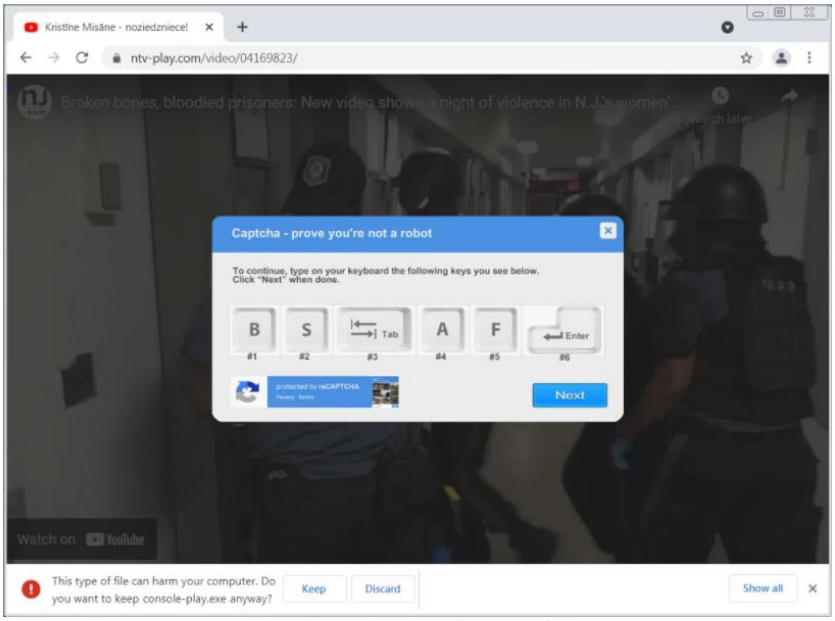


Embedded YouTube video on malicious site
Source: BleepingComputer

When you click on the play button, the browser will download a file named console-play.exe [VirusTotal], and the site will display a fake reCaptcha image on the screen.

As this file is an executable, Google Chrome automatically warns that the file may be malicious and prompts whether you wish to 'Keep' or 'Discard' the file.

To bypass this warning, the threat actors are displaying a fake reCaptcha image that prompts the user to press the B, S, Tab, A, F, and the Enter buttons on their keyboard, as shown below.



Fake reCaptcha bypasses browser warnings
Source: BleepingComputer

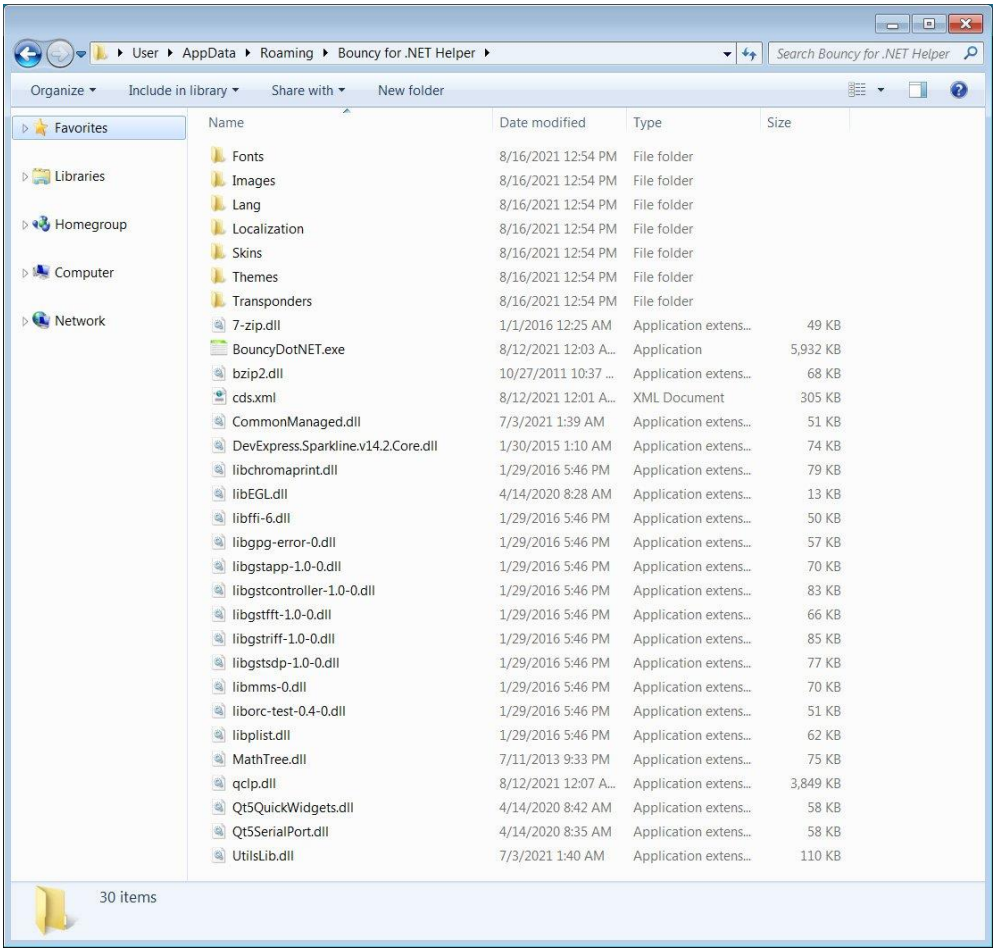
While pressing the B, S, A, and F keys do not do anything, pressing the Tab key will make the 'Keep' button become focused, and then pressing the 'Enter' key will act as a click on the button, causing the browser to download and save the file to the computer.

As you can see, this fake captcha prompt is a clever way to trick a user into downloading a malicious file that the browser is warning could be malicious.

After a certain amount of time, the video will automatically play, potentially making users think the successful 'captcha' allowed it.

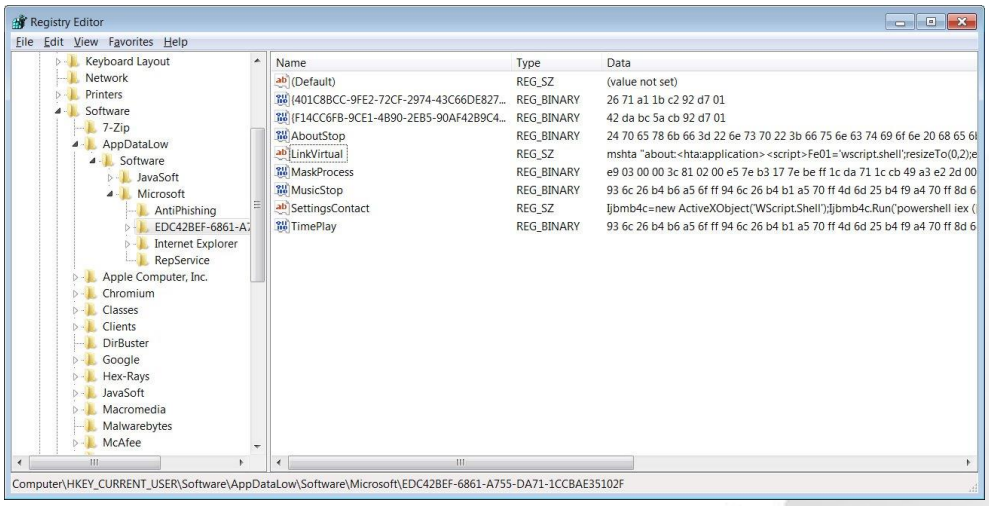
Site distributes Ursnif information-stealing trojan

If a user runs the executable, it will create a folder under %AppData%\Bouncy for .NET Helper and install numerous files. All of these files are a decoy, other than the BouncyDotNet.exe executable, which is launched.



Extracted Bouncy for .NET Helper folder
Source: BleepingComputer

While running, BouncyDotNet.exe will read various strings from the Windows Registry used to launch PowerShell commands.



Caption
Source: BleepingComputer

These PowerShell commands will compile a .NET application using the built-in CSC.exe compiler that launches a DLL for the Ursnif banking trojan.

Once running, Gozi will steal account credentials, download further malware to the computer, and execute commands issued remotely by the threat actors.

If you are infected with Ursnif, you should immediately change the passwords for your online accounts.

Source: https://www.bleepingcomputer.com/news/security/malware-campaign-uses-clever-captcha-to-bypass-browser-warning/

6. Liquid cryptocurrency exchange loses $94 million following hack

Japan-based cryptocurrency exchange Liquid has suspended deposits and withdrawals after attackers have compromised its warm wallets.

Liquid is one of the largest cryptocurrency-fiat exchange platforms worldwide (based on daily traded spot volume).

The exchange has more than 800,000 customers from over 100 countries and says that it reached a $1.1B+ daily trade volume this year.

After discovering that its warm wallets were hacked, the crypto exchange moved its assets into a cold wallet.

"We are currently investigating and will provide regular updates. In the meantime deposits and withdrawals will be suspended," Liquid said.

Current status of Liquid services:

- To ensure safety of funds, please do not deposit any crypto assets to your Liquid wallets until further notice.
- Liquid has halted all crypto withdrawals while we assess the impact.
- Fiat withdrawals and deposits remain available.
- Other services on Liquid, including trading and Liquid Earn, remain available.

Over $90 million worth of assets stolen

"A total of approximately 91.35mm USDe of crypto assets were moved out of Liquid wallets by an unauthorized party," Liquid said in a follow-up incident report.

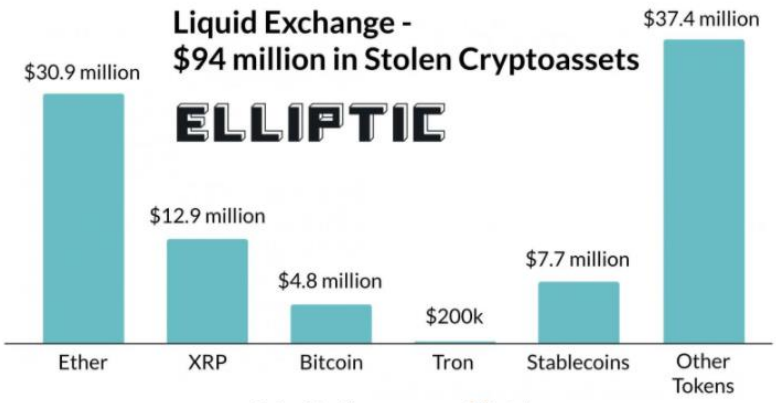
"69 different crypto assets were misappropriated and sent to other exchanges or defi swapping venues. Assets placed in Liquid Earn are not impacted."

Blockchain analytics firm Elliptic added that "the stolen funds include $45 million in Ethereum tokens, which are currently being exchanged for ETH on DEXs such as Uniswap and SushiSwap" which would allow the attackers to "avoid having these assets frozen."

Liquid is still assessing the attack vector used in the incident and is "taking measures to mitigate the impact to users."

Liquid previously reported a data breach in November 2020 after GoDaddy, the exchange's domain hosting provider, transferred control of its account and domain to a malicious actor.

A subsequent security notice issued in January revealed that the threat actor breached Liquid's infrastructure and gained access to customer personal information including emails, names, addresses, encrypted passwords, and API keys.



Stolen Liquid cryptoassets (Elliptic)

Today's incident follows the biggest cryptocurrency hack ever, the theft of over $611 million after an unknown threat actor hacked Poly Network's cross-chain interoperability protocol last week.

In a weird twist of events, Poly Network first threatened the attacker (known as Mr. White Hat) to return the stolen cryptocurrency to avoid landing on law enforcement's radar. It then awarded him a $500,000 bounty and invited him to be the company's Chief Security Advisor.

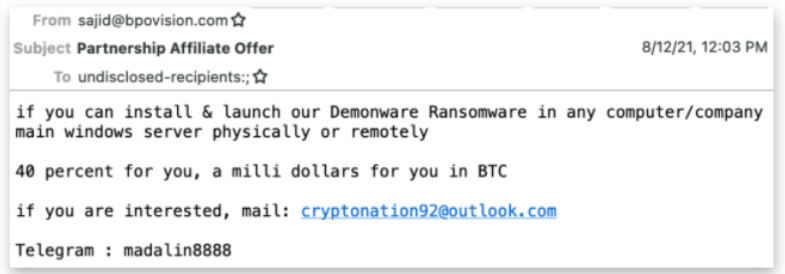
Since the attack took place, Mr. White Hat has gradually transferred the stolen assets to Poly Network's wallets.

In July, the FBI issued a Private Industry Notification warning cryptocurrency owners, exchanges, and third-party payment platforms of threat actors actively targeting virtual assets in attacks that can lead to significant financial losses.

Source: https://www.bleepingcomputer.com/news/security/liquid-cryptocurrency-exchange-loses-94-million-following-hack/

7. Wanted: Disgruntled Employees to Deploy Ransomware

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.


From sajid@bpovision.com
Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM
To undisclosed-recipients:;

if you can install & launch our Demonware Ransomware in any computer/company main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888

Initial email sent by the threat actor.

Crane Hassold, director of threat intelligence at Abnormal Security, described what happened after he adopted a fake persona and responded to the proposal in the screenshot above. It offered to pay him 40 percent of a million-dollar ransom demand if he agreed to launch their malware inside his employer's network.

This particular scammer was fairly chatty, and over the course of five days it emerged that Hassold's correspondent was forced to change up his initial approach in planning to deploy the DemonWare ransomware strain, which is freely available on GitHub.

"According to this actor, he had originally intended to send his targets—all senior-level executives—phishing emails to compromise their accounts, but after that was unsuccessful, he pivoted to this ransomware pretext," Hassold wrote.

Abnormal Security documented how it tied the email back to a young man in Nigeria who acknowledged he was trying to save up money to help fund a new social network he is building called Sociogram.

Image: Abnormal Security.

Reached via LinkedIn, Sociogram founder Oluwaseun Medayedupin asked to have his startup's name removed from the story, although he did not respond to questions about whether there were an inaccuracies in Hassold's report.

"Please don't harm Sociogram's reputation," Medayedupin pleaded. "I beg you as a promising young man."

This attacker's approach may seem fairly amateur, but it would be a mistake to dismiss the threat from West African cybercriminals dabbling in ransomware. While multi-million dollar ransomware payments are hogging the headlines, by far the biggest financial losses tied to cybercrime each year stem from so-called Business Email Compromise (BEC) or CEO Scams, in which crooks mainly based in Africa and Southeast Asia will spoof communications from executives at the target firm in a bid to initiate unauthorized international wire transfers.

According to the latest figures (PDF) released by the FBI Internet Crime Complaint Center (IC3), the reported losses from BEC scams continue to dwarf other cybercrime loss categories, increasing to $1.86 billion in 2020.

2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Image: FBI

"Knowing the actor is Nigerian really brings the entire story full circle and provides some notable context to the tactics used in the initial email we identified," Hassold wrote. "For decades, West African scammers, primarily located in Nigeria, have perfected the use of social engineering in cybercrime activity."

"While the most common cyber attack we see from Nigerian actors (and most damaging attack globally) is business email compromise (BEC), it makes sense that a Nigerian actor would fall back on using similar social engineering techniques, even when attempting to successfully deploy a more technically sophisticated attack like ransomware," Hassold concluded.

DON'T QUIT YOUR DAY JOB

Cybercriminals trolling for disgruntled employees is hardly a new development. Big companies have long been worried about the very real threat of disgruntled employees creating identities on darknet sites and then offering to trash their employer's network for a fee (for more on that, see my 2016 story, Rise of the Darknet Stokes Fear of the Insider).

Indeed, perhaps this enterprising Nigerian scammer is just keeping up with current trends. Several established ransomware affiliate gangs that have recently rebranded under new banners seem to have done away with the affiliate model in favor of just buying illicit access to corporate networks.

For example, the Lockbit 2.0 ransomware-as-a-service gang actually includes a solicitation for insiders in the desktop wallpaper left behind on systems encrypted with the malware.

"Would you like to earn millions of dollars? Our company acquires access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company," LockBit's unusual ad reads. "You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate

email, etc. Open our letter at your email. Launch the provided virus on any computer in your company. Companies pay us the foreclosure for the decryption of files and prevention of data leak."

Image: Sophos.

Likewise, the newly formed BlackMatter ransomware gang kicked off its presence on the cybercrime forums with the unassuming thread, "Buying/monetizing your access to corporate networks." The rest of the post reads:

We are looking for access to corporate networks in the following countries:
– the USA
– Canada
– Australia
– the UK

All lines of business except for:
– Healthcare
– Government entities.

Requirements:
– Revenue according to ZoomInfo: over 100 million.
– Number of hosts: 500 to 15,000.
– We do not accept networks that anybody else has already tried to work on.

Two options of cooperation:
– We buy networks: 3 to 100k.
– We monetize them (subject to negotiation on a case-by-case basis).

How we work:
You select an option of cooperation. -> You provide access to the network. -> We check it. -> We take it or not (depending on whether it meets the requirements).

Source: https://krebsonsecurity.com/2021/08/wanted-disgruntled-employees-to-deploy-ransomware/

8. Hackers can bypass Cisco security products in data theft attacks

Cisco said that unauthenticated attackers could bypass TLS inspection filtering tech in multiple products to exfiltrate data from previously compromised servers inside customers' networks.

In such attacks, the threat actors can exploit a vulnerability in the Server Name Identification (SNI) request filtering impacting 3000 Series Industrial Security Appliances (ISAs), Firepower Threat Defense (FTD), and Web Security Appliance (WSA) products.

"Using SNIcat or a similar tool, a remote attacker can exfiltrate data in an SSL client hello packet because the return server hello packet from a server on the blocked list is not filtered," Cisco explained.

"This communication can be used to execute a command-and-control attack on a compromised host or perform additional data exfiltration attacks."

So far, the Cisco Product Security Incident Response Team (PSIRT) is not aware of attackers or malware exploiting this security flaw in the wild.

Stealthy data exfiltration by abusing TLS

SNIcat (Server Name Indication Concatenator) is a stealthy exfiltration method discovered by mnemonic Labs security researchers that bypasses security perimeter solutions and TLS inspection devices (e.g., web proxies, next-gen firewalls (NGFW) via TLS Client Hello packets.

"By using our exfiltration method SNIcat, we found that we can bypass a security solution performing TLS inspection, even when the Command & Control (C2) domain we use is blocked by common reputation and threat prevention features built into the security solutions themselves," the reearchers said.

"In short, we found that solutions designed to protect users, introduced them to a new vulnerability."

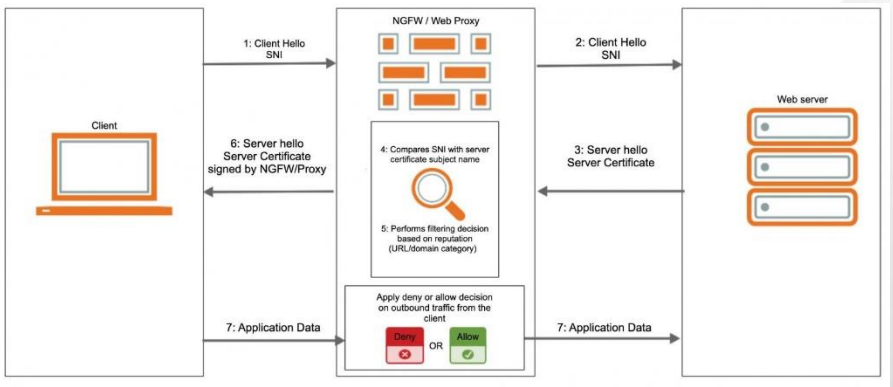


Image: mnemonic Labs

Besides Cisco, mnemonic Labs have successfully tested SNIcat against products from F5 Networks (F5 BIG-IP running TMOS 14.1.2, with SSL Orchestrator 5.5.8), Palo Alto Networks (Palo Alto NGFW running PAN-OS 9.1.1), and Fortinet (Fortigate NGFW running FortiOS 6.2.3).

The researchers also developed a proof of concept tool that helps extract data from previously hacked servers via an SNI covert channel, using an agent on the compromised host and a command-and-control server that gathers the exfiltrated data.

"Cisco is investigating its product line to determine which products may be affected by this vulnerability," Cisco added.

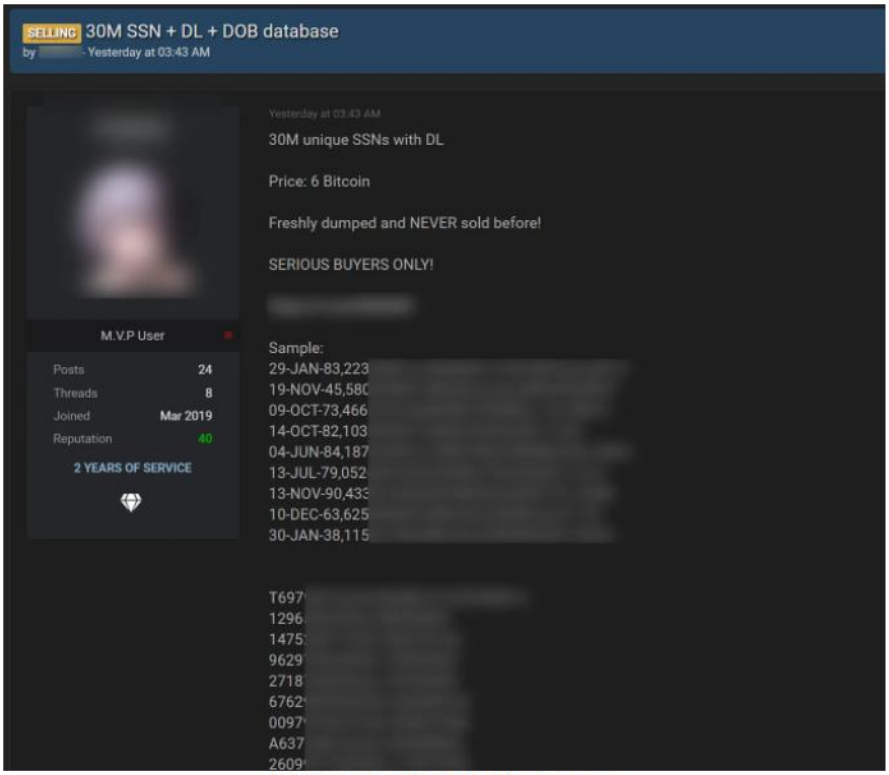
"As the investigation progresses, Cisco will update this advisory with information about affected products."

Source: https://www.bleepingcomputer.com/news/security/hackers-can-bypass-cisco-security-products-in-data-theft-attacks/

9. T-Mobile data breach just got worse — now at 54 million customers

The T-Mobile data breach keeps getting worse as an update to their investigation now reveals that cyberattack exposed over 54 million individuals' data.

Last weekend, a threat actor began selling the personal information of 100 million T-Mobile customers on a hacking forum for six bitcoin (~$280K).



Forum post selling T-Mobile database

The hacker said that the stolen database contains the data for approximately 100 million T-Mobile customers. The exposed data can include customers' IMSI, IMEI, phone numbers, customer names, security PINs, Social Security numbers, driver's license numbers, and date of birth.

The hackers said the database was stolen approximately two weeks ago and contains customer data from as far back as 2004.

"Their entire IMEI history database going back to 2004 was stolen," the hacker told BleepingComputer.

T-Mobile later confirmed that some of its servers were hacked and began investigating what customer data was exposed.

Affected T-Mobile customers keep increasing

On August 17th, T-Mobile first disclosed a summary of their investigation into their hacked servers and said that the personal information of 48.6 million individuals was exposed during the attack.

Today, T-Mobile has updated its advisory to include an additional 6 million customers or prospective customers affected by the attack.

Furthermore, T-Mobile has confirmed our original reporting on this attack that the attackers also stole IMSI and IMEI numbers.

As it stands today, the attack affected 54.6 million individuals, which is broken down below.

- 13.1 million current T-Mobile postpaid customer accounts that included first and last names, date of birth, SSN, and driver's license/ID information.
- 40 million former or prospective T-Mobile customers, including first and last names, date of birth, SSN, and driver's license/ID information.
- 667,000 accounts of former T- Mobile customers exposing customer names, phone numbers, addresses and dates of birth compromised.
- 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed.
- 52,000 names related to current Metro by T-Mobile accounts may have been included.

T-Mobile continues to see no sign of payment information or financial information exposed during the attack.

We will likely continue to see the number of exposed customers increase in the coming weeks.

It is advised that all T-Mobile customers assume that their data was exposed and be on the lookout for targeted phishing emails and SMS texts.

If any are received, do not click any links embedded in the messages as threat actors could use them to harvest credentials from unsuspecting T-Mobile customers.

Source: https://www.bleepingcomputer.com/news/security/t-mobile-data-breach-just-got-worse-now-at-54-million-customers/

10. Microsoft Exchange servers being hacked by new LockFile ransomware

A new ransomware gang known as LockFile encrypts Windows domains after hacking into Microsoft Exchange servers using the recently disclosed ProxyShell vulnerabilities.

ProxyShell is the name of an attack consisting of three chained Microsoft Exchange vulnerabilities that result in unauthenticated, remote code execution.

The three vulnerabilities were discovered by Devcore Principal Security Researcher Orange Tsai, who chained them together to take over a Microsoft Exchange server in April's Pwn2Own 2021 hacking contest.

- CVE-2021-34473 - Pre-auth Path Confusion leads to ACL Bypass (Patched in April by KB5001779)

- CVE-2021-34523 - Elevation of Privilege on Exchange PowerShell Backend (Patched in April by KB5001779)
- CVE-2021-31207 - Post-auth Arbitrary-File-Write leads to RCE (Patched in May by KB5003435)

While Microsoft fully patched these vulnerabilities in May 2021, more technical details were recently disclosed, allowing security researchers and threat actors to reproduce the exploit.

As reported last week by BleepingComputer, this has led to threat actors actively scanning for and hacking Microsoft Exchange servers using the ProxyShell vulnerabilities.

After exploiting an Exchange server, the threat actors dropped web shells that could be used to upload other programs and execute them.

At the time, NCC Group's vulnerability researcher Rich Warren told BleepingComputer that the web shells were being used to install a .NET backdoor that was downloading a harmless payload at the time.

Since then, security researcher Kevin Beaumont reports that a new ransomware operation known as LockFile uses the Microsoft Exchange ProxyShell and the Windows PetitPotam vulnerabilities to take over Windows domains and encrypt devices.

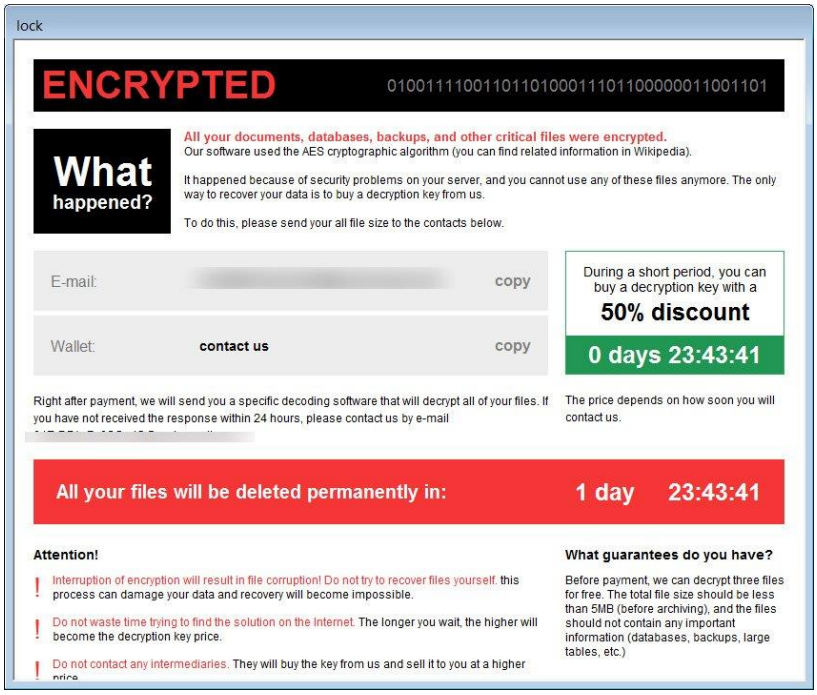
When breaching a network, the threat actors will first access the on-premise Microsoft Exchange server using the ProxyShell vulnerabilities. Once they gain a foothold, Symantec says the LockFile gang uses the PetitPotam vulnerability to take over a domain controller, and thus the Windows domain.

From there, it is trivial to deploy the ransomware through the entire network.

What we know about the LockFile ransomware

At this time, there is not much known about the new LockFile ransomware operation.

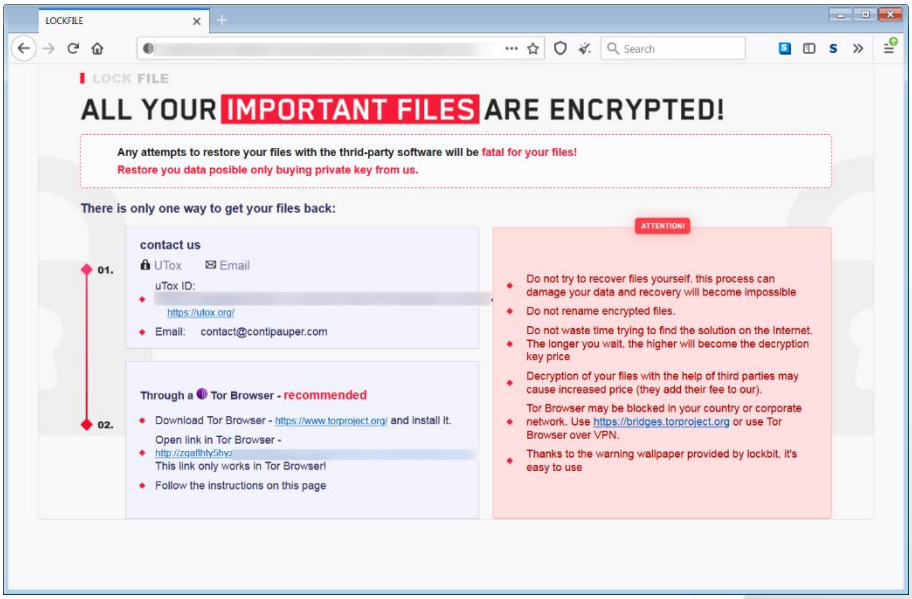
When first seen in July, the ransom note was named 'LOCKFILE-README.hta' but did not have any particular branding, as shown below.



Old LockFile ransom notes

Starting last week, BleepingComputer began receiving reports of a ransomware gang using branded ransom notes indicating that they were called 'LockFile,' as shown below

These ransom notes use a naming format of '[victim_name]-LOCKFILE-README.hta' and prompted the victim to contact them via Tox or email to negotiate the ransom. The current email address used by the operation is contact@contipauper.com, which appears to be a reference to the Conti ransomware operation.



While the color schemes of the ransom notes are similar, the communication methods and wording make it unclear if they are the same operation.

Of particular interest is that the color scheme and layout of the ransom notes is very similar to the LockBit ransomware, but there does not appear to be any relation.

When encrypting files, the ransomware will append the .lockfile extension to the encrypted file's names.

Yesterday afternoon, when BleepingComputer and ransomware expert Michael Gillespie analyzed the July version of LockFile, we found it to be a noisy ransomware, taking up many system resources and causing temporary freezes of the computer.

Patch now!

As the LockFile operation uses both the Microsoft Exchange ProxyShell vulnerabilities and the Windows PetitPotam NTLM Relay vulnerability, it is imperative that Windows administrators install the latest updates.

For the ProxyShell vulnerabilities, you can install the latest Microsoft Exchange cumulative updates to patch the vulnerabilities.

The Windows PetitPotam attack gets a bit complicated as Microsoft's security update is incomplete and does not patch all the vulnerability vectors.

To patch the PetitPotam attack, you can use an unofficial patch from 0patch to block this NTLM relay attack vector or apply NETSH RPC filters that block access to vulnerable functions in the MS-EFSRPC API.

Beaumont says you can perform the following Azure Sentinel queries to check if your Microsoft Exchange server has been scanned for the ProxyShell vulnerability.

```
W3CIISLog
| where csUriStem == "/autodiscover/autodiscover.json"
| where csUriQuery has "PowerShell" | where csMethod == "POST"
```

All organizations are strongly advised to apply the patches as soon as possible and create offline backups of their Exchange servers.

Source: https://www.bleepingcomputer.com/news/security/lockfile-ransomware-attacks-microsoft-exchange-with-proxyshell-exploits/

11. Can Your Wearable Health Monitors Be Compromised?

More senior adults are taking advantage of the array of wearable technology that helps them stay connected to healthcare providers and monitor their physical health and safety. But that newfound convivence comes with risk and, for many, the genuine fear of falling prey to an online hacker.

Protection + Peace of Mind

Wearable technology brings seniors both power and peace of mind. Many elderly consumers rely on wearable technology to monitor critical blood glucose levels, heart activity, and blood pressure. In addition, seniors and their families rely on fall detection, emergency alerts, and home security technology to monitor physical safety. Since the pandemic, wearable technology has played a central role in connecting virus-vulnerable seniors to healthcare professionals.

A recent study cites that 25 percent of U.S. homeowners with broadband internet expect to purchase a new connected consumer health or fitness device within the next year. Another study predicts the global market for wearable healthcare devices will reach $46.6 billion by 2025.

This kind of data is excellent to show consumer trends, but it also gives cybercriminals a road sign for new inroads into stealing consumer data.

So how do we dodge the digital dangers of our beloved wearable devices? With time, attention, and a few basics.

Basic Safety Protocols

- Know the risks. The first step is to acknowledge that every digital device brings risk despite a manufacturer's security claims. That's why digital security (at any age) begins with personal responsibility and education.
- Keep learning. Learn all you can about the device you've purchased and research the risks other consumers may have reported. If a security loophole in your device hasn't hit the headlines yet, give it time. Sadly, just about every device has a security loophole, as ongoing digital threat reports remind us.
- Master safety basics. With any new digital purchase, commit to following basic safety protocols. It's imperative to read device security warnings, configure basic privacy settings, set up strong passwords, and devote yourself to the monitoring of your account after setup.

Sound like a hassle? Perhaps. However, following these basic protocols is likely far more manageable than having to navigate through the potential chaos connected to a data breach.

6 ways to protect digital wearables

- Install updates immediately. When it comes to protecting your wearables, security updates are not optional. Be sure to install the updates (usually with a single click) to protect your device from reported bugs, enhance functionality, and of course, seal up any security loopholes.
- Add digital protection. It's more than a buzz. Extra security solutions such a Virtual Private Network (VPN) and added security software can be your saving grace from prying eyes and help protect the health data you send over the internet. A VPN uses an encrypted connection to send and receive data. For example, if you use a VPN, a hacker trying to eavesdrop on your network will be met with a cacophony of jumbled data on their screen. In addition, installing comprehensive security software can thwart viruses and malware scams from infecting your digital landscape.
- Level up your password IQ. Several practices can quickly shore up your password security: 1) Change your device's default username and password immediately, 2) choose a strong password, 3) use Two Factor Authentication (2FA), and 4) keep your passwords in one place such as a password manager.
- Switch devices off and on. Here's a fun one—go old school. The National Security Alliance (NSA) recently advised consumers of one powerful way to thwart cybercriminals, especially with smartphones. Turn your device on and off every now and then. Better yet, if a device is not in use, shut it down.
- Verify every source. Scams connected to your new device or health condition increasingly look legitimate. For that reason, verify sources, websites, and avoid giving out any personal information, and never send money to an unverified source. Scams come in the form of a phony email, people posing as an IT department or helpdesk, text message, pop-up, calendar invite, or even a direct message on social media. This is where antivirus software can save the day.
- Ask for help. Beyond your device manual, Google and YouTube, if you are a senior and still have issues securing a new device, reach out for help. Don't overlook the help desk associated with your new device, many of which also have a convenient online chat feature. Other possible resources include: Your local library, senior center, Agency on Aging, or community center may have help. In addition, AARP has published a list of helpful IT resources for seniors.

Having the right technology at your fingertips can feel like magic especially if you are a senior adult with health and safety concerns. In these times of widespread digital

insecurity, giving even a little extra time and attention to these basic digital security protocols can bring a new level of peace and power to your daily routine.

Source: https://www.mcafee.com/blogs/consumer/family-safety/can-your-wearable-health-monitors-be-compromised/

12. Botnet targets hundreds of thousands of devices using Realtek SDK

A Mirai-based botnet now targets a critical vulnerability in the software SDK used by hundreds of thousands of Realtek-based devices, encompassing 200 models from at least 65 vendors, including Asus, Belkin, D-Link, Netgear, Tenda, ZTE, and Zyxel.

The security flaw that IoT Inspector security researchers found is now tracked as CVE-2021-35395 and was assigned a 9.8/10 severity rating.

It impacts many Internet-exposed wireless devices ranging from residential gateways and travel routers to Wi-Fi repeaters, IP cameras, and smart lightning gateways or connected toys.

Attacks began only two days after public disclosure

Since the bug affects the management web interface, remote attackers can scan for and attempt to hack them to execute arbitrary code remotely on unpatched devices, allowing them to take over the impacted devices.

While Realtek shipped a patched version of the vulnerable SDK on August 13, three days before IoT Inspector security researchers published their advisory, this gave very little time to vulnerable device owners to apply the patch.

As network security firm SAM Seamless Network discovered, a Mirai botnet began searching for devices unpatched against CVE-2021-35395 on August 18, only two days after IoT Inspector shared details of the bug.

"As of August 18th, we have identified attempts to exploit CVE-2021-35395 in the wild," SAM said in a report published last week.

SAM says that the most common devices using buggy Realtek SDK targeted by this botnet are Netis E1+ extender, Edimax N150 and N300 Wi-Fi routers, and Repotec RP-WR5444 router, mainly used to enhance Wi-Fi reception.

Botnet updated to target new devices

The threat actor behind this Mirai-based botnet also updated their scanners more than two weeks ago to exploit a critical authentication bypass vulnerability (CVE-2021-20090) impacting millions of home routers using Arcadyan firmware.

As Juniper Threat Labs researchers revealed at the time, this threat actor has been targeting network and IoT devices since at least February.

"This chain of events shows that hackers are actively looking for command injection vulnerabilities and use them to propagate widely used malware quickly," said Omri Mallis, chief product architect at SAM Seamless Network.

"These kinds of vulnerabilities are easy to exploit and can be integrated quickly into existing hacking frameworks that attackers employ, well before devices are patched and security vendors can react."

The complete list of affected devices is too long to embed here, but it can be found at the end of the IoT Inspector report.

Source: https://www.bleepingcomputer.com/news/security/botnet-targets-hundreds-of-thousands-of-devices-using-realtek-sdk/

13. Microsoft Spills 38 Million Sensitive Data Records Via Careless Power App Configs

Data leaked includes COVID-19 vaccination records, Social Security numbers and email addresses tied to American Airlines, Ford, Indiana Department of Health and New York City public schools.

For months, Microsoft's Power Apps portals exposed personal data tied to 38 million records ranging from COVID-19 vaccination status, Social Security numbers and email addresses. Consumers most affected by what is being called a "platform issue" are those doing business with American Airlines, Ford, the Indiana Department of Health and New York City public schools.

Microsoft describes its Power Apps as a "suite of apps, services, and connectors, as well as a data platform, that provides a rapid development environment to build custom apps for your business needs." The tool is used by developers to build applications that share data locally or with the cloud.

On Monday, UpGuard Research revealed Microsoft's Power Apps management portal had inadvertently leaked the data of 47 businesses totaling the exposure of 38 million personal records. It asserted that Microsoft's Power Apps platform was flawed in the way it forced customers to configure their data as private or public. Microsoft does not consider the

leaky data issue a vulnerability, rather a configuration issue that can be improved on its part.

Besides data sets previously mentioned, researchers outlined what they found as:

American Airlines: A collection of 398,890 "contact" records, which included full names, job titles, phone numbers, and email addresses. A second "test" collection of data included 470,400 records, which included full names, job titles, phone numbers and email addresses.

Denton County, TX: A total of 632,171 records spilled included vaccination types, appointment dates and times, employee IDs, full names, email addresses, phone numbers, and birth dates. "The list 'contactVaccinationSet' had 400,091 records with fields for full names and vaccination types, and 'contactset' had 253,844 records with full names and email addresses," researchers wrote.

J.B. Hunt Transport Services: The transportation logistics firm made public 905,228 records that included customer full names, email addresses, physical addresses and phone numbers. Over a quarter million of the records also included US Social Security numbers.

Microsoft's own The Global Payroll Services Portal: Researchers found 332,000 records of Microsoft employees and contractors with their @microsoft.com email address, full name and phone numbers that appear to be for personal use.

How Microsoft's Power Apps Blew It

UpGuard said the data leak is tied to how the Power Apps platform juggles the use of the Open Data Protocol (OData) with its application programming interface (API). For example, some data handled within the Power Apps platform needs to be public, and other related data sets need to be private.

"In cases like registration pages for COVID-19 vaccinations, there are data types that should be public, like the locations of vaccination sites and available appointment times, and sensitive data that should be private, like the personally identifying information of the people being vaccinated," UpGuard wrote.

Researchers discovered sensitive private user data, which should have been private, was being segregated, but still publicly accessible. The issue, UpGuard explained, is that Microsoft's configuration options for data sharing and storing sensitive data in Power Apps "create the potential for data leaks."

Researchers zeroed in on the OData APIs used by Power Apps for retrieving and storing public and private/sensitive data. More specifically, they focused on how data (such as personal identifiable information, or PII) is stored and formatted into "Table Permissions" for sharing – or not. The crux of the issue boiled down to configuration settings that instruct a Power Apps user to "set the Enable Table Permissions Boolean value on the list record to true."

"If those configurations are not set and the OData feed is enabled, anonymous users can access list data freely," researchers wrote.

It's a Feature, Not a Bug, Says Microsoft

During the course of its researcher, UpGuard discovered the OData misconfiguration by Microsoft customers (and even Microsoft itself) to be widespread and systemic. "Empirical evidence suggests a warning in the technical documentation is not sufficient to avoid the serious consequences of misconfiguring OData list feeds for Power Apps portals," wrote researchers.

UpGuard notified Microsoft of the data leakage on June 24, 2021. Microsoft promptly began to investigate claims that its Power Apps were responsible for spilling millions of sensitive-data records. On June 29, the company asserted that the platform worked as planned.

"The case was closed, and the Microsoft analyst informed us that they had determined that this behavior is considered to be by design," UpGuard wrote.

Over the proceeding weeks, UpGuard continued to find massive data exposures tied to the way Power Apps handled OData via its API.

"Microsoft would later take action after we had notified some of the most severe exposures. We spent the next few weeks analyzing the data for indicators of sensitivity and reaching out to affected organizations," according to the UpGuard report.

Shoot the Messenger

For all of UpGuard's attempts to shed light onto Microsoft's Power Apps problems, it was persona non grata for not only Microsoft, but also others it notified of data leaks. Reaction to UpGuard's data discovery of sensitive COVID-19 vaccine records being publicly exposed by the state of Indiana was typical.

Researchers notified Indiana's deputy chief technology officer on July 2 of its publicly accessible stores of sensitive data. While data was removed by July 7, on August 17 the State of Indiana issued a press release publicly acknowledging the data exposure, it also accused UpGuard of "improperly" accessing the data, claiming it was done as a ploy to drum up business from the state.

"UpGuard has never approached Indiana or any other company notified of a breach for business, and there is no merit to [the press] statement. On the contrary, UpGuard has provided hours of unremunerated support in service of Indiana Department of Health and the people it serves," UpGuard wrote. UpGuard also verified to the state that all the publicly accessible data it had discovered has been destroyed.

Microsoft Takes Action to Help Customers

Since UpGuard's disclosure of the issue, Microsoft released a tool for checking Power Apps portals for leaky data. It also plans to change the product so that table permissions will be enforced by default, UpGuard said.

"To diagnose configuration issues, the Portal Checker can be used to detect lists that allow anonymous access. More importantly, newly created Power Apps portals will have table permissions enabled by default. Tables configurations can still be changed to allow for anonymous access, but defaulting to permissions enabled will greatly reduce the risk of future misconfiguration," UpGuard wrote.

UpGuard added that it agrees with Microsoft's stance that the issue is not a software vulnerability, rather a platform issue that "requires code changes to the product."

"It is a better resolution to change the product in response to observed user behaviors than to label systemic loss of data confidentiality [as] an end user misconfiguration, allowing the problem to persist and exposing end users to the cybersecurity risk of a data breach," UpGuard said. "Ultimately, Microsoft has done the best thing they can, which is to enable table permissions by default and provided tooling to help Power Apps users self-diagnose their portals."

Source: https://threatpost.com/microsoft-38-million-sensitive-records-power-app/168885/

14. How to Spot Fake Login Pages

Have you ever come across a website that just didn't look quite right? Perhaps the company logo looked slightly misshapen, or the font seemed off-brand. Odds are, you landed on a phony version of a legitimate corporation's website—a tried and true tactic relied on by many cybercriminals.

Fake Login Pages Explained

A fake login page is essentially a knock-off of a real login page used to trick people into entering their login credentials, which hackers can later use to break into online accounts. These websites mirror legitimate pages by using company logos, fonts, formatting, and overall templates. Depending on the attention to detail put in by the hackers behind the imposter website, it can be nearly impossible to distinguish from the real thing. Consequentially, fake login pages can be highly effective in their end goal: credential theft.

How do these pages get in front of a consumer in the first place? Typically, scammers will target unsuspecting recipients with phishing emails spoofing a trusted brand. These emails may state that the user needs to reset their password or entice them with a deal that sounds too good to be true. If the consumer clicks on the link in the email, they will

be directed to the fake login page and asked to enter their username and password. Once they submit their information, cybercriminals can use the consumer's data to conduct credential stuffing attacks and hack their online profiles. This could lead to credit card fraud, data extraction, wire transfers, identity theft, and more.

How Fake Login Pages Are Affecting Canadians

Scammers have recently targeted Canadians with attacks leveraging fake login pages to harvest personal data. For example, criminals preyed on employees who were expecting COVID-19 relief grants in the form of the CERB (Canada Emergency Response Benefit). These funds were sent via an electronic transfer from Interac, a legitimate Canadian interbank network. However, a phishing campaign spoofing Interac's e-transfer service circulated emails claiming that the Canada Revenue Agency (CRA) made a CERB deposit of $1,957.50 CAD.

These emails directed recipients to a fake CRA login page, which then redirected to a phony Interac e-transfer site where users were asked to select their personal bank. From there, the recipient was asked to enter their username, card number, password, security questions and answers for their online banking profile, and other personally identifiable information—providing all the information a criminal would need to hack into the user's bank account.

Why Fake Login Pages are Effective

If you Google "fake login pages," you will quickly find countless guides on how to create fake websites in seconds. Ethical concerns aside, this demonstrates just how common vector spoofed websites are for cyberattacks. While it has been easier to distinguish between real and fake login pages in the past, criminals are constantly updating their techniques to be more sophisticated, therefore making it more difficult for consumers to recognize their fraudulent schemes.

One reason why fake login pages are so effective is due to inattentional blindness, or failure to notice something that is completely visible because of a lack of attention. One of the most famous studies on inattentional blindness is the "invisible gorilla test." In this study, participants watched a video of people dressed in black and white shirts passing basketballs. Participants were asked to count the number of times the team in white passed the ball:

Because participants were intently focused on counting the number of times the players in white passed the ball, more than 50% failed to notice the person in the gorilla costume walking through the game. If this is the first time you've seen this video, it's likely that you didn't notice the gorilla, the curtain changing color from red to gold, or the player in black leaving the game. Similarly, if you come across a well-forged login page and aren't actively looking for signs of fraud, you could inherently miss a cybercriminal's "invisible gorilla." That's why it's crucial for even those with phishing training to practice caution when they come across a website asking them to take action or enter personal details.

How to Steer Clear of Fake Login Pages

The most important defense against steering clear of fake login pages is knowing how to recognize them. Follow these tips to help you decipher between a legitimate and a fake website:

- Don't fall for phishing

Most fake login pages are circulated vis phishing messages. If you receive a suspicious message that asks for personal details, there are a few ways to determine if it was sent by a phisher aiming to steal your identity. Phishers often send messages with a tone of urgency, and they try to inspire extreme emotions such as excitement or fear. If an unsolicited email urges you to "act fast!" slow down and evaluate the situation.

- Look for misspellings or grammatical errors

Oftentimes, hackers will use a URL for their spoofed website that is just one character off from the legitimate site, such as using "www.rbcr0yalbank.com" versus "www.rbcroyalbank.com." Before clicking on any website from an email asking you to act, hover over the link with your cursor. This will allow you to preview the URL and identify

any suspicious misspellings or grammatical errors before navigating to a potentially dangerous website.

- Ensure the website is secured with HTTPS

HTTPS, or Hypertext Transfer Protocol Secure, is a protocol that encrypts your interaction with a website. Typically, websites that begin with HTTPS and feature a padlock in the top left corner are considered safer. However, cybercriminals have more recently developed malware toolkits that leverage HTTPS to hide malware from detection by various security defenses. If the website is secured with HTTPS, ensure that this isn't the only way you're analyzing the page for online safety.

- Enable multi-factor authentication

Multi-factor authentication requires that users confirm a collection of things to verify their identity—usually something they have, and a factor unique to their physical being—such as a retina or fingerprint scan. This can prevent a cybercriminal from using credential-stuffing tactics (where they will use email and password combinations to hack into online profiles) to access your network or account if your login details were ever exposed during a data breach.

- Sign up for an identity theft alert service

An identity theft alert service warns you about suspicious activity surrounding your personal information, allowing you to jump to action before irreparable damage is done. McAfee Total Protection not only keeps your devices safe from viruses but gives you the added peace of mind that your identity is secure, as well.

Source: https://www.mcafee.com/blogs/consumer/consumer-cyber-awareness/how-to-spot-fake-login-pages%e2%80%af/

15. Ragnarok Ransomware Gang Bites the Dust, Releases Decryptor

The cybercriminal group, active since late 2019, has closed its doors and released the key to unlocking victims' files on its dark web portal.

Another cybercriminal gang notorious for ransomware attacks has shut down, publishing its decryptor online to allow victims unlock and recover files.

The Ragnarok gang, also known as Asnarok, closed up shop this week, publishing the news to their public website, according to a post published Thursday by analyst firm Recorded Future's The Record, among other sources.

As a parting "gift," the group released their decryptor, hardcoded with a master decryption key, for free as well on the portal. Previously, the site was primarily the place where Ragnarok would publish data from victims who refused to pay ransom.

"Ragnarok now becomes the third ransomware group that shuts down and releases a way for victims to recover files for free this summer, after the likes of Avaddon in June and SynAck earlier this month," according to The Record.

Several security researchers have confirmed that the Ragnarok decryptor works, according to the post. It's currently being analyzed and researchers will eventually release a clean version that is safe to use on Europol's NoMoreRansom portal.

Data Thieves

Ragnarok, active since late 2019, was seen in April in an attack on luxury Italian men's clothing line Boggi Milano. The gang xfiltrated 40 gigabytes of data from the fashion house, including human resources and salary details.

Ragnarok's typical modus operandi was to use exploits to breach a target company's network and perimeter devices. From there it would work from the internal network to encrypt an organization's servers and workstations.

Ragnarok also was of one of a number of ransomware groups that would not just encrypt but also steal files so it could threaten to leak them on its portal to pressure victims to pay demanded ransoms, and then make good on the threat if the threat actors didn't receive their money by an appointed deadline.

Targeting Citrix ADC gateways was a specialty of the group, which also was behind the campaign that exploited a zero-day in the Sophos XG firewalls, according to the post.

"While the zero-day exploit worked and allowed the gang to backdoor XG firewalls across the world, Sophos spotted the attack in time to prevent the group from deploying its file-encrypting payload," according to the Record.

Ransomware Gangs Dropping Like Flies

The gang is the latest ransomware group to shutter operations, due in part to mounting pressures and crackdowns from international authorities that already have led some key players to cease their activity. In addition to Avaddon and SyNack, two heavy hitters in the game — REvil and DarkSide – also closed up shop recently.

Other ransomware groups are feeling the pressure in other ways. An apparently vengeful affiliate of the Conti Gang recently leaked the playbook of the ransomware group after alleging that the notorious cybercriminal organization underpaid him for doing its dirty work.

However, even as some ransomware groups are hanging it up, new threat groups that may or may not have spawned from the previous ranks of these organizations are sliding in to fill the gaps they left.

Haron and BlackMatter are among those that have emerged recently with intent to use ransomware to target large organizations that can pay million-dollar ransoms to fill their pockets.

Indeed, some think Ragnarok's exit from the field also isn't permanent, and that the group will resurface in a new incarnation at some point.

"Even though I am sure is only temporary, it is nice to see another win," tweeted Allan Liska, from Recorded Future's Computer Security Incident Response Team, of the group's shutdown.

Source: https://threatpost.com/ragnarok-releases-decryptor/168976/

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.