



Advanced Security Operations Center  
Telelink Business Services  
[www.tbs.tech](http://www.tbs.tech)

# Monthly Security Bulletin

May 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. **Reality Winner's Twitter account was hacked to target journalists** Error! Bookmark not defined.
2. **Daxin Espionage Backdoor Ups the Ante on Chinese Malware** Error! Bookmark not defined.
3. **Conti Ransomware Decryptor, TrickBot Source Code Leaked ..** Error! Bookmark not defined.
4. **Hacking Alexa through Alexa's Speech.....** Error! Bookmark not defined.
5. **Google: Russia, China, Belarus state hackers target Ukraine, Europe.....** Error! Bookmark not defined.
6. **93% of Organizations Have Network Vulnerabilities: Here's How to Beat the Odds** Error! Bookmark not defined.
7. **Massive phishing campaign uses 500+ domains leading to fake login pages** Error! Bookmark not defined.
8. **Unsecured Microsoft SQL, MySQL servers hit by Gh0stCringe malware .....** Error! Bookmark not defined.
9. **Free decryptor released for TrickBot gang's Diavol ransomware ...** Error! Bookmark not defined.
10. **Lapsus\$ Data Kidnappers Claim Snatches From Microsoft, Okta....** Error! Bookmark not defined.
11. **Hacked WordPress sites force visitors to DDoS Ukrainian targets .** Error! Bookmark not defined.
12. **Cyberattackers Target UPS Backup Power Devices in Mission-Critical Environments .....** Error! Bookmark not defined.
13. **Globant confirms hack after Lapsus\$ leaks 70GB of stolen data ....** Error! Bookmark not defined.
14. **QNAP Customers Adrift, Waiting on Fix for OpenSSL Bug.....** Error! Bookmark not defined.

**15. Spring patches leaked Spring4Shell zero-day RCE vulnerability.....**Error! Bookmark not defined.

**16. Viasat confirms satellite modems were wiped with AcidRain malware .....**Error! Bookmark not defined.

**17. Apple emergency update fixes zero-days used to hack iPhones, Macs .....**Error! Bookmark not defined.

# 1. Critical GitLab vulnerability lets attackers take over accounts

GitLab has addressed a critical severity vulnerability that could allow remote attackers to take over user accounts using hardcoded passwords.

The bug (discovered internally and tracked as CVE-2022-1162) affects both GitLab Community Edition (CE) and Enterprise Edition (EE).

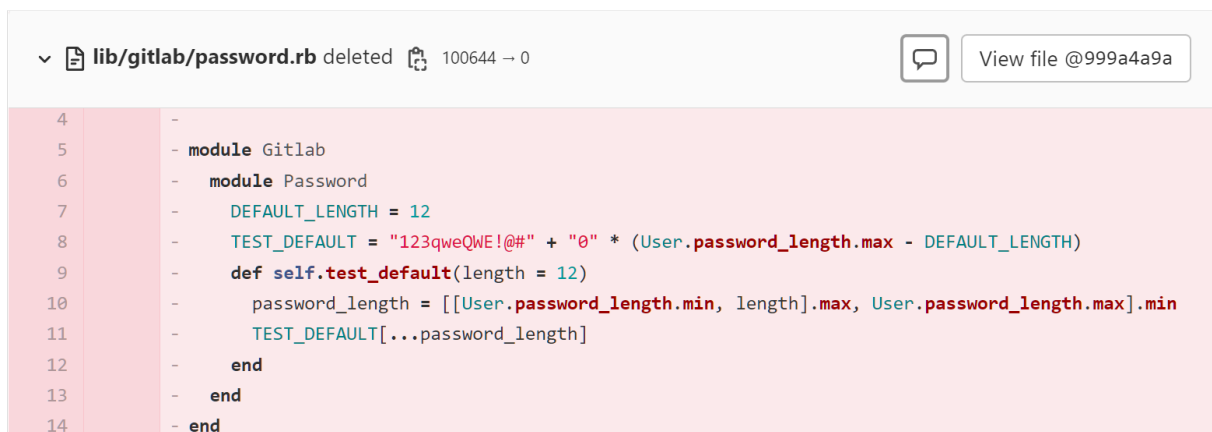
This flaw results from static passwords accidentally set during OmniAuth-based registration in GitLab CE/EE.

"A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts," the GitLab team explained in a security advisory published on Thursday.

GitLab urged users to immediately upgrade all GitLab installations to the latest versions (14.9.2, 14.8.5, or 14.7.7) to block potential attacks.

"We strongly recommend that all installations running a version affected by the issues described below are upgraded to the latest version as soon as possible," they said.

A code commit submitted two days shows that GitLab deleted the 'lib/gitlab/password.rb' file, which was used to assign a weak hardcoded password to the 'TEST\_DEFAULT' constant.



```
4 -  
5 - module Gitlab  
6 -   module Password  
7 -     DEFAULT_LENGTH = 12  
8 -     TEST_DEFAULT = "123qweQWE!@#" + "0" * (User.password_length.max - DEFAULT_LENGTH)  
9 -     def self.test_default(length = 12)  
10 -       password_length = [(User.password_length.min, length).max, User.password_length.max].min  
11 -       TEST_DEFAULT[...password_length]  
12 -     end  
13 -   end  
14 - end
```

*GitLab hardcoded password assignment code (BleepingComputer)*

## Passwords reset for some GitLab users

GitLab also added that it reset the passwords of a limited number of GitLab.com users as part of the CVE-2022-1162 mitigation effort.

It also found no evidence that any accounts have been compromised by attackers using this hardcoded password security flaw.

"We executed a reset of GitLab.com passwords for a selected set of users as of 15:38 UTC," the GitLab team said.

"Our investigation shows no indication that users or accounts have been compromised but we're taking precautionary measures for our users' security."

When asked to share the number of Gitlab.com users who had their passwords reset, a GitLab spokesperson shared the info already available in the advisory telling BleepingComputer that they only did it for "a selected set of users."

## Script to identify affected user accounts

While GitLab says no user accounts have been breached so far, the company has created a script that self-managed instance admins can use to identify user accounts potentially impacted by CVE-2022-1162.

After identifying potentially affected user accounts, admins are advised to reset the users' passwords.

Over 100,000 organizations use its DevOps platform, according to GitLab, and the company estimates it has more than 30 million estimated registered users from 66 countries worldwide.

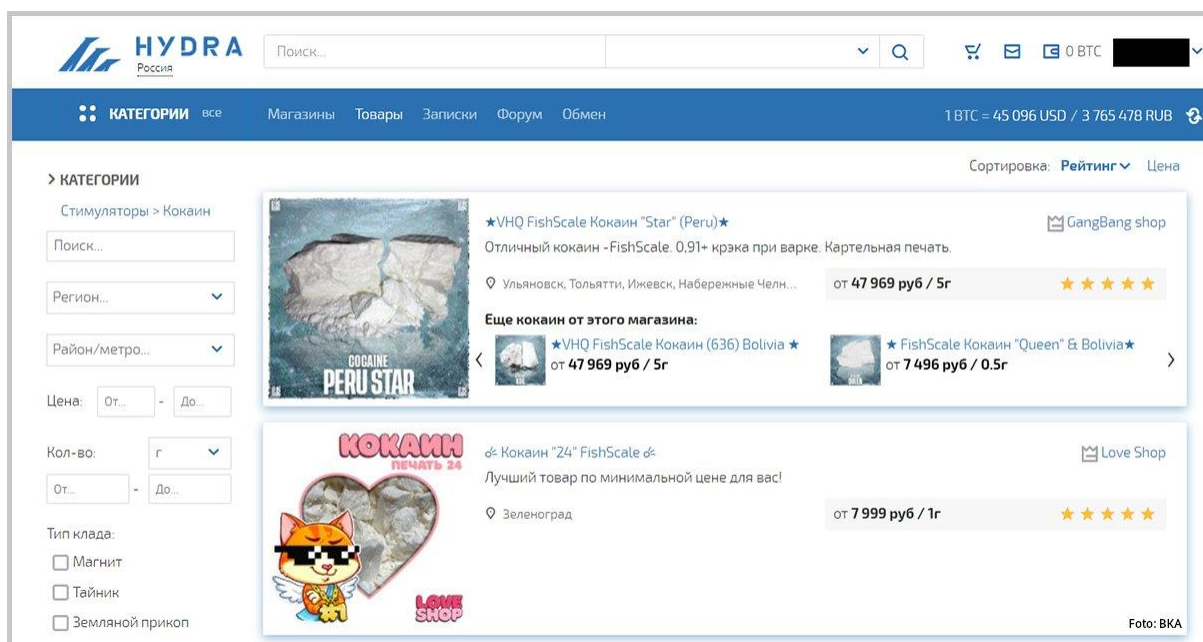
Source: <https://www.bleepingcomputer.com/news/security/critical-gitlab-vulnerability-lets-attackers-take-over-accounts/>

## 2. Germany takes down Hydra, world's largest darknet market

The servers of Hydra Market, the most prominent Russian darknet platform for selling drugs and money laundering, have been seized by the German police.

The police were also able to seize 543 bitcoins from the profits of Hydra, which are currently worth a little over \$25 million.

The confiscated money indicate the size of the Hydra market, which counted around 19,000 registered seller accounts that served at least 17 million customers around the world.



*A snapshot of Hydra Market before its take down*

In an announcement today, the Central Office for Combating Cybercrime (ZIT) and Germany's Federal Criminal Police Office (BKA) estimate that Hydra Market had a turnover of \$1.35 billion in 2020, making it the largest darknet market in the world.

Today, the blockchain analytics expert Elliptic, has confirmed the digital asset seizure from the authorities, tracking the action as 88 transactions amounting to 543.3 bitcoin.

Apart from narcotics and money laundering services, which were the main focus, Hydra also offered stolen databases, forged documents, and hacking for hire services.

## Investigation into an obscured space

At the moment, Hydra's homepage shows that the BKA acting on behalf of the Attorney General's Office in Frankfurt am Main seized the market's infrastructure following a coordinated international law enforcement effort.





Hydra's homepage after seizure (BKA)

This action was possible after a lengthy investigation directed against the previously unknown operators and administrators of the platform.

As the BKA announcement points out, Hydra Market featured a Bitcoin Bank Mixer, which obfuscated all cryptocurrency transactions made on the platform, making it hard for law enforcement agencies to track money obtained from illegal activities.

At this time, it is unknown if the German authorities have made any arrests or if they hold identification information or even clues about Hydra's core team.

Bleeping Computer has attempted to source more information in that regard, and we will update this post as soon as we hear back from BKA.

In the meantime, the seized equipment most likely contains incriminating evidence on Hydra sellers and clients, so a significant number of users could be charged in an upcoming second phase.

Source: <https://www.bleepingcomputer.com/news/legal/germany-takes-down-hydra-worlds-largest-darknet-market/>

### 3. Palo Alto Networks firewalls, VPNs vulnerable to OpenSSL bug

American cybersecurity company Palo Alto Networks warned customers on Wednesday that some of its firewall, VPN, and XDR products are vulnerable to a high severity OpenSSL infinite loop bug disclosed three weeks ago.

Threat actors can exploit this security vulnerability (tracked as CVE-2022-0778) to trigger a denial of service state and remotely crash devices running unpatched software.

Even though the OpenSSL team released a patch two weeks ago when it publicly disclosed the bug, customers will have to wait until later this month (during the week of April 18) when Palo Alto Networks plans to release security updates.

"PAN-OS, GlobalProtect app, and Cortex XDR agent software contain a vulnerable version of the OpenSSL library and product availability is impacted by this vulnerability. For PAN-OS software, this includes both hardware and virtual firewalls and Panorama appliances as well as Prisma Access customers," the company said.

"This vulnerability has reduced severity on Cortex XDR agent and GlobalProtect app as successful exploitation requires an attacker-in-the-middle attack (MITM)."

The bug impacts PAN-OS 8.1 and later releases and all versions of GlobalProtect app and Cortex XDR agent.

The cybersecurity vendor added that this vulnerability does not impact its Prisma Cloud and Cortex XSOAR products.

#### Mitigation available for some customers

While PAN-OS hotfixes are still in development, customers with Threat Prevention subscriptions can enable Threat IDs 92409 and 92411 to block known attacks for this vulnerability and "reduce the risk of exploitation from known exploits."

Luckily, even if proof-of-concept exploits are available online, Palo Alto Networks has no evidence of exploitation of this issue on any of its products.

Although attackers can abuse the OpenSSL infinite loop flaw in low complexity attacks without user interaction, the OpenSSL team says the impact of successful exploitation is limited to triggering a denial of service.

"The flaw is not too difficult to exploit, but the impact is limited to DoS. The most common scenario where exploitation of this flaw would be a problem would be for a TLS client accessing a malicious server that serves up a problematic certificate," an OpenSSL spokesperson told BleepingComputer.

"TLS servers may be affected if they are using client authentication (which is a less common configuration) and a malicious client attempts to connect to it. It is difficult to guess to what extent this will translate to active exploitation."

Last week, network-attached storage (NAS) maker QNAP also warned customers that this OpenSSL DoS bug impacts most of its NAS devices, with a patch to be released as soon as possible.

Source: <https://www.bleepingcomputer.com/news/security/palo-alto-networks-firewalls-vpns-vulnerable-to-openssl-bug/>

## 4. Microsoft: New malware uses Windows bug to hide scheduled tasks

Microsoft has discovered a new malware used by the Chinese-backed Hafnium hacking group to maintain persistence on compromised Windows systems by creating and hiding scheduled tasks.

The Hafnium threat group has previously targeted US defense companies, think tanks, and researchers in cyberespionage attacks.

It is also one of the state-sponsored groups linked by Microsoft to last year's global scale exploitation of the ProxyLogon zero-day flaws impacting all supported Microsoft Exchange versions.

### Persistence via Windows registry value removal

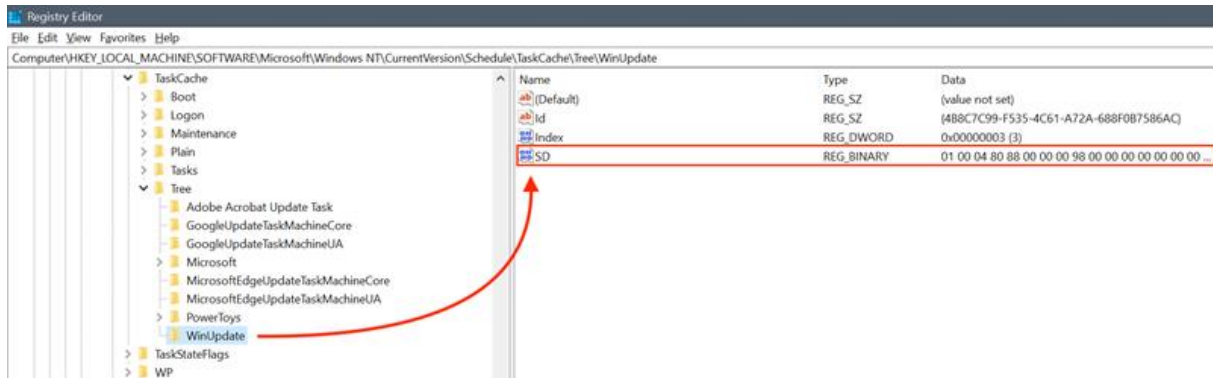
"As Microsoft continues to track the high-priority state-sponsored threat actor HAFNIUM, new activity has been uncovered that leverages unpatched zero-day vulnerabilities as initial vectors," the Microsoft Detection and Response Team (DART) said.

"Further investigation reveals forensic artifacts of the usage of Impacket tooling for lateral movement and execution and the discovery of a defense evasion malware called Tarrask that creates 'hidden' scheduled tasks, and subsequent actions to remove the task attributes, to conceal the scheduled tasks from traditional means of identification."

This hacking tool, dubbed Tarrask, uses a previously unknown Windows bug to hide them from "schtasks /query" and Task Scheduler by deleting the associated Security Descriptor registry value.

The threat group used these "hidden" scheduled tasks to maintain access to the hacked devices even after reboots by re-establishing dropped connections to command-and-control (C2) infrastructure.

While the Hafnium operators could have removed all on-disk artifacts, including all registry keys and the XML file added to the system folder to delete all traces of their malicious activity, it would have removed persistence across restarts.



*Deleting Security Descriptor to hide a scheduled task (Microsoft)*

## How to defend against Tarrask attacks

The "hidden" tasks can only be found upon closer manual inspection of the Windows Registry if you look for scheduled tasks without an SD (security descriptor) Value within their Task Key.

Admins can also enable the Security.evtx and the Microsoft-Windows-TaskScheduler/Operational.evtx logs to check for key events linked to tasks "hidden" using Tarrask malware.

Microsoft also recommends enabling logging for 'TaskOperational' within the Microsoft-Windows-TaskScheduler/Operational Task Scheduler log and monitoring for outbound connections from critical Tier 0 and Tier 1 assets.

"The threat actors in this campaign used hidden scheduled tasks to maintain access to critical assets exposed to the internet by regularly re-establishing outbound communications with C&C infrastructure," DART added.

"We recognize that scheduled tasks are an effective tool for adversaries to automate certain tasks while achieving persistence, which brings us to raising awareness about this oft-overlooked technique."

Source: <https://www.bleepingcomputer.com/news/security/microsoft-new-malware-uses-windows-bug-to-hide-scheduled-tasks/>



## 5. Free decryptor released for Yanluowang ransomware victims

Kaspersky today revealed it found a vulnerability in Yanluowang ransomware's encryption algorithm, which makes it possible to recover files it encrypts.

The Russian cybersecurity firm has added support for decrypting files locked by the Yanluowang ransomware strain to its RannohDecryptor utility.

"Kaspersky experts have analyzed the ransomware and found a vulnerability that allows decrypting files of affected users via a known-plaintext attack," the company said today.

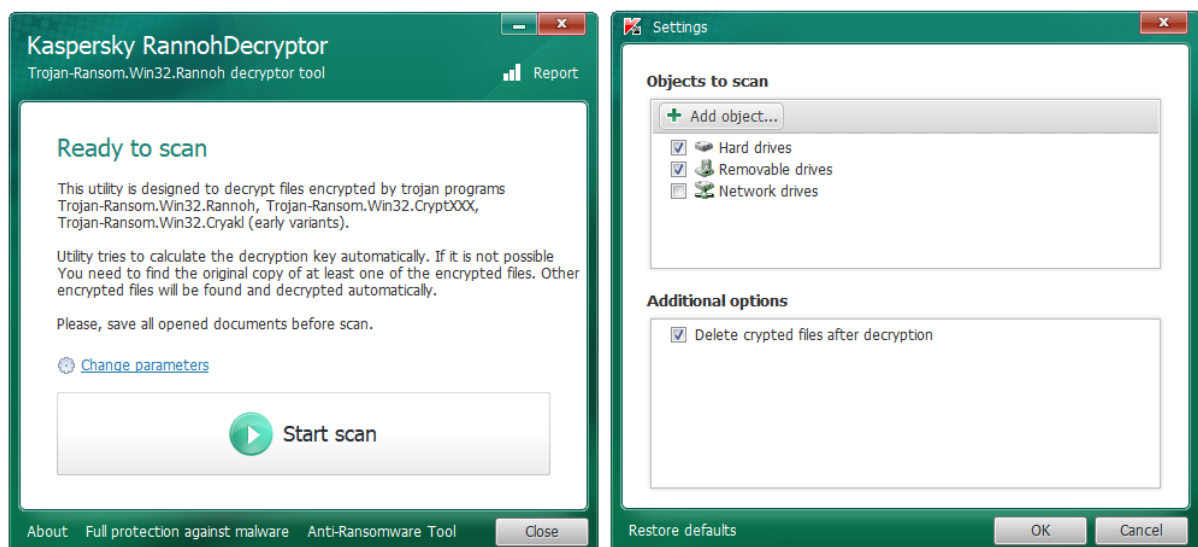
This ransomware strain encrypts files bigger than 3GB and those smaller than 3GB using different methods: larger ones are partially encrypted in 5MB stripes after every 200MB, while smaller ones are entirely encrypted from start to end.

Because of this, "if the original file is larger than 3 GB, it is possible to decrypt all files on the infected system, both big and small. But if there is an original file smaller than 3 GB, then only small files can be decrypted."

To decrypt your files, you need at least one of the original files:

- To decrypt small files (less than or equal to 3 GB), you need a pair of files with a size of 1024 bytes or more. This is enough to decrypt all other small files.
- To decrypt big files (more than 3 GB), you need a pair of files (encrypted and original) no less than 3 GB in size each. This will be enough to decrypt both big and small files.

To decrypt files encrypted by Yanluowang ransomware, you have to use the Rannoh decryption tool available for download from Kaspersky's servers.



*Kaspersky RannohDecryptor (BleepingComputer)*

## Yanluowang attacks high-profile enterprise targets

Yanluowang ransomware, first spotted in October 2021, has been used in human-operated, highly targeted attacks against enterprise entities.

One month later, one of its affiliates was observed attacking US organizations in the financial sector since at least August, using the BazarLoader malware for reconnaissance.

Based on the tactics, techniques, and procedures (TTPs) used in these attacks, this Yanluowang affiliate was linked to the Thieflock ransomware operation developed by the Fivehands group (tracked by Mandiant as UNC2447).

Once deployed on compromised networks, Yanluowang stops hypervisor virtual machines, ends all processes, and encrypts files appending the .yanluowang extension.

It also drops ransom notes named README.txt that warn victims not to contact law enforcement or ask any ransomware negotiation firms for help.

If the attackers' requests are not met, the ransomware operators threaten to launch distributed denial of service (DDoS) attacks against the victims' networks and inform their employees and business partners they were breached.

They also say they'll breach the victims' networks again "in a few weeks" and delete their data, a common tactic ransomware gangs use to pressure their victims into paying the ransom.

Source: <https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/>

### 1. Malicious web redirect service infects 16,500 sites to push malware

A new TDS (Traffic Direction System) operation called Parrot has emerged in the wild, having already infected servers hosting 16,500 websites of universities, local governments, adult content platforms, and personal blogs. [...]

Source: <https://www.bleepingcomputer.com/news/security/malicious-web-redirect-service-infected-16-500-sites-to-push-malware/>

### 2. New Android banking malware remotely takes control of your device

A new Android banking malware named Octo has appeared in the wild, featuring remote access capabilities that allow malicious operators to perform on-device fraud. [...]

Source: <https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/>

### 3. Windows 11 tool to add Google Play secretly installed malware

A popular Windows 11 ToolBox script used to add the Google Play Store to the Android Subsystem has secretly infected users with malicious scripts, Chrome extensions, and potentially other malware. [...]

Source: <https://www.bleepingcomputer.com/news/security/windows-11-tool-to-add-google-play-secretly-installed-malware/>

### 4. Lenovo UEFI firmware driver bugs affect over 100 laptop models

Lenovo has published a security advisory on vulnerabilities that impact its Unified Extensible Firmware Interface (UEFI) loaded on at least 100 of its laptop models. [...]

Source: <https://www.bleepingcomputer.com/news/security/lenovo-uefi-firmware-driver-bugs-affect-over-100-laptop-models/>

### 5. Cisco Umbrella Secure Web Gateway File Decryption Bypass Vulnerability

A vulnerability in the automatic decryption process in Cisco Umbrella Secure Web Gateway (SWG) could allow an authenticated, adjacent attacker to bypass the SSL decryption and content filtering policies on an affected system. This vulnerability is due to how the decryption function uses the TLS Server Name Indication (SNI) extension of an HTTPS request to discover the destination domain and determine if the request needs to be decrypted. An attacker could exploit this vulnerability by sending a crafted request over TLS from a client to an unknown or controlled URL. A successful exploit could allow an attacker to bypass the decryption process of Cisco Umbrella SWG and allow malicious content to be downloaded to a host on a protected network.

There are workarounds that address this vulnerability. This advisory is available at the following link: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uswg-fdbps-xtTRKpp6>

Security	Impact	Rating:	Medium
CVE:			CVE-2022-20805

Source: [https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uswg-fdbps-xtTRKpp6?vs\\_f=Cisco%20Security%20Advisory&vs\\_cat=Security%20Intelligence&vs\\_type=RSS&vs\\_p=Cisco%20Umbrella%20Secure%20Web%20Gateway%20File%20Decryption%20Bypass%20Vulnerability&vs\\_k=1](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uswg-fdbps-xtTRKpp6?vs_f=Cisco%20Security%20Advisory&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=Cisco%20Umbrella%20Secure%20Web%20Gateway%20File%20Decryption%20Bypass%20Vulnerability&vs_k=1)

## 6. Cisco Umbrella default SSH key allows theft of admin credentials

Cisco has released security updates to address a high severity vulnerability in the Cisco Umbrella Virtual Appliance (VA), allowing unauthenticated attackers to steal admin credentials remotely. [...]

Source: <https://www.bleepingcomputer.com/news/security/cisco-umbrella-default-ssh-key-allows-theft-of-admin-credentials/>

## 7. Critical bug in Android could allow access to users' media files

Security analysts have found that Android devices running on Qualcomm and MediaTek chipsets were vulnerable to remote code execution due to a flaw in the implementation of the Apple Lossless Audio Codec (ALAC). [...]

Source: <https://www.bleepingcomputer.com/news/security/critical-bug-in-android-could-allow-access-to-users-media-files/>

## 8. Docker servers hacked in ongoing cryptomining malware campaign

Docker APIs on Linux servers are being targeted by a large-scale Monero crypto-mining campaign from the operators of the Lemon\_Duck botnet. [...]

Source: <https://www.bleepingcomputer.com/news/security/docker-servers-hacked-in-ongoing-cryptomining-malware-campaign/>

## 9. Java Cryptography Implementation Mistake Allows Digital-Signature Forgeries

Interesting [implementation mistake](#):

The vulnerability, which [Oracle patched on Tuesday](#), affects the company's implementation of the [Elliptic Curve Digital Signature Algorithm](#) in Java versions 15 and above. ECDSA is an algorithm that uses the principles of [elliptic curve cryptography](#) to authenticate messages digitally.

[...]

ECDSA signatures rely on a pseudo-random number, typically notated as K, that's used to derive two additional numbers, R and S. To verify a signature as valid, a party must check the equation involving R and S, the signer's public key, and a cryptographic hash of the message. When both sides of the equation are equal, the signature is valid.

[...]

For the process to work correctly, neither R nor S can ever be a zero. That's because one side of the equation is R, and the other is multiplied by R and a value from S. If the values are both 0, the verification check translates to  $0 = 0 \times$  (other values from the private key and hash), which will be true regardless of the additional values. That means an adversary only needs to submit a blank signature to pass the verification check successfully.



Madden wrote:

Guess which check Java forgot?

That's right. Java's implementation of ECDSA signature verification didn't check if R or S were zero, so you could produce a signature value in which they are both 0 (appropriately encoded) and Java would accept it as a valid signature for any message and for any public key. The digital equivalent of a blank ID card.

More [details](#).

Source: <https://www.schneier.com/blog/archives/2022/04/java-cryptography-implementation-mistake-allows-digital-signature-forgeries.html>

## 10. Google Play Store now forces apps to disclose what data is collected

Google is rolling out a new Data Safety section on the Play Store, Android's official app repository, where developers must declare what data their software collects from users of their apps. [...]

Source: <https://www.bleepingcomputer.com/news/security/google-play-store-now-forces-apps-to-disclose-what-data-is-collected/>

## 11. Emotet malware now installs via PowerShell in Windows shortcut files

The Emotet botnet is now using Windows shortcut files (.LNK) containing PowerShell commands to infect victims computers, moving away from Microsoft Office macros that are now disabled by default. [...]

Source: <https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/>

## 12. New Nimbuspwn Linux vulnerability gives hackers root privileges

A new set of vulnerabilities collectively tracked as Nimbuspwn could let local attackers escalate privileges on Linux systems to deploy malware ranging from backdoors to ransomware. [...]

Source: <https://www.bleepingcomputer.com/news/security/new-nimbuspwn-linux-vulnerability-gives-hackers-root-privileges/>

## 13. Smarter Homes & Gardens: Smart Speaker Privacy



So is your smart speaker really listening in on your conversations?

That's the crux of a popular privacy topic. Namely, are we giving up some of our privacy in exchange for the convenience of a smart speaker that does our bidding with the sound of our voice? After all, you're using it to do everything from search for music, order online, and control the lights and temperature in your home.

What is your smart speaker really hearing—and recording?

Let's take a look at what's going on inside of your smart speaker, how it processes your requests, and what companies do with the recordings and transcripts of your voice.

### So, are smart speakers listening in?

More or less, smart speakers are listening to all the time. Each smart speaker has its own "wake word" that it listens for, like *Alexa*, *Siri*, or *Google*. When the device hears that wake word or thinks it hears it, it begins recording and awaits your verbal commands. Unless you have the microphone or listening feature turned off, your device indeed actively listens for that wake word all the time.

Here's where things get interesting, though. There's a difference between "listening" and "recording." The act of listening is passive. Your smart speaker is waiting to hear its name. That's it. Once it does hear its name, it begins recording for a few seconds to record your command. From there, your spoken command goes into the company's cloud for processing by way of an encrypted connection.

There are exceptions to when your command may go to the company's cloud for processing, like Siri on iPhones, which [according to Apple](#), "You don't sign in with your Apple ID to use Siri, and the audio of your requests is processed entirely on your iPhone." Also, [Google Assistant may process some requests without going to the cloud](#), like "When a user triggers a smart home Action that has a local fulfillment path, Assistant sends the EXECUTE intent or QUERY intent to the Google Home or Google Nest device rather than the cloud fulfillment."

In the cases where information does go to the cloud, processing entails a few things. First, it makes sure that the wake word was heard. If it's determined that the wake word was indeed spoken (or something close enough to it—more on that in a minute), the speaker follows through on the request or command. Depending on your settings, that activity may get stored in your account history, whether as a voice recording, transcript, or both. If the wake word was not detected, processing ends at that point.

Enter the issue of mistaken wake words. While language models and processing technologies used by smart speakers are constantly evolving, there are occasions where a smart speaker acts as if a wake word was heard when it simply wasn't said. Several [studies on the topic](#) have been [published in recent years](#). In the case of research from Northeastern University, it was found that dialogue from popular television shows could be interpreted as wake words that trigger recording. For example, their findings cite:

"We then looked at other shows with a similarly high dialogue density (such as *Gilmore Girls* and *The Office*) and found that they also have a high number of activations, which suggests that the number of activations is at least in part related to the density of dialogue. However, we have also noticed that if we consider just the amount of dialogue (in a number of words), *Narcos* is the one that triggers the most activations, even if it has the lowest dialogue density."

Of interest is not just the volume of dialogue, but the pronunciation of the dialogue:

"We investigated the actual dialogue that produced *Narcos*' activations and we have seen that it was mostly Spanish dialogue and poorly pronounced English dialogue. This suggests that, in general, words that are not pronounced clearly may lead to more unwanted activations."

Research such as this suggests that smart speakers at the time had room for improvement when it comes to properly detect wake words, thus leading to parts of conversation being recorded without the owner intending it. If you own a smart speaker, I wouldn't be too surprised to hear that you've had some issues like that from time to time yourself.

## **Is someone on the other end of my smart speaker listening to my recordings?**

As mentioned above, the makers of smart speakers make constant improvements to their devices and services, which may include the review of commands from users to make sure they are interpreted correctly. There are typically two types of review—machine and human. As the names suggest, a machine review is a digital analysis and human reviews entail someone listening to and evaluating a recorded command or reading and evaluating a transcript of a written command.

However, several manufacturers let you exercise some control over that. In fact, you'll find that they post a fair share of articles about this collection and review process, along with your choices for opting in or out as you wish:

- [Apple explains its review process for Siri here](#), along with ways that you can opt-out of these reviews. For more [information about their overall privacy measures](#), visit [Apple's page here](#).
- [Amazon also explains how it uses such information](#) and likewise how you can opt-out, such as by [automatically deleting your recordings](#). You can [learn more about their overall privacy measures for Alexa here](#).
- As of April 2022, Google states that it does not retain your audio recordings by default—and [you can browse or delete your Google Assistant history here](#).

## Setting up your smart speaker for better privacy

The quickest way to ensure a more private experience with your smart speaker is to disable listening—or turn it off entirely. Depending on the device, you may be able to do this with the push of a button, a voice command, or some combination of the two. This will keep the device from listening for its wake word. Likewise, this makes your smart speaker unresponsive to voice commands until you enable them again. This approach works well if you decide there are certain stretches of the day where your smart speaker doesn't need to be on call.

Yet let's face it, the whole idea of a smart speaker is to have it on and ready to take your requests. For those stretches where you leave it on, there's another step you can take to shore up your privacy.

In addition to making sure you're opted out of the review process mentioned above, you can also delete your recordings associated with your voice commands.

- For Google Assistant users, [Google provides the following article](#).
- [Siri users can follow these instructions](#) to delete their recordings.
- You can [manage your Alexa recordings](#) with these instructions as well.

Managing your voice history like this gives you yet one more way you can take control of your privacy. In many ways, it's like deleting your search history from your browser. And when you consider just how much activity and how many queries your smart speaker may see over the course of days, weeks, and months, you can imagine just how much information that captures about you and your family. Some of it is undoubtedly personal. Deleting that history can help protect your privacy in the event that information ever gets breached or somehow ends up in the hands of a bad actor.

Lastly, above and beyond these privacy tips for your smart speakers, [comprehensive online protection](#) will help you look out for your privacy overall. In the case of ours, we provide a full range of privacy and device protection, along with identity theft protection that includes \$1M identity theft coverage, identity monitoring, and identity restoration



assistance from recovery pros—and antivirus too, of course. Together, they can make your time spent online far more secure.

### **You're the smart one in this relationship**

With privacy becoming an increasingly hot topic (rightfully so!), several companies have been taking steps to make the process of managing yours easier and a more prevalent part of their digital experience. As you can see, there are several ways you can take charge of how your smart speaker uses, and doesn't use, your voice.

It used to be that many of these settings were tucked away deep in menus, rather than something companies would tout on web pages dedicated to privacy. So as far as smart speakers go, the information is out there, and I hope this article helps make the experience with yours more private and secure.

The post [Smarter Homes & Gardens: Smart Speaker Privacy](#) appeared first on [McAfee Blog](#).

Source: <https://www.mcafee.com/blogs/privacy-identity-protection/smarter-homes-gardens-smart-speaker-privacy/>

## 14. Attacker Breach 'Dozens' of GitHub Repos Using Stolen OAuth Tokens

GitHub shared the timeline of breaches in April 2022, this timeline encompasses the information related to when a threat actor gained access and stole private repositories belonging to dozens of organizations.

Source: <https://threatpost.com/github-repos-stolen-oauth-tokens/179427/>

## 15. Russian hackers launch DDoS attacks on Romanian govt sites

The Romanian national cyber security and incident response team, DNSC, has issued a statement about a series of distributed denial-of-service (DDoS) attacks targeting several public websites managed by the state entities. [...]

Source: <https://www.bleepingcomputer.com/news/security/russian-hackers-launch-ddos-attacks-on-romanian-govt-sites/>

If you want to learn more about ASOC and how we can improve your security posture, **contact us at [tbs.sales@tbs.tech](mailto: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.*