Threat Actor deploys Mythic's Athena Agent to target Russian Semiconductor Suppliers

Supple.com/blog/threat-actor-deploys-mythics-athena-agent-to-target-russian-semiconductor-suppliers/

October 10, 2023



Key Takeaways

- Cyble Research and Intelligence Labs (CRIL) recently came across a new spear phishing email targeting a leading Russian semiconductor supplier.
- In this targeted attack, we observed Threat Actors (TAs) leveraging a Remote Code Execution (RCE) vulnerability, identified as <u>CVE-2023-38831</u>, to deliver their payload on compromised systems.
- The objective of this attack is to gain complete control over the compromised system using a second-stage payload known as "Athena," an agent of the <u>Mythic</u> C2 framework.
- This Agent is equipped with a wide range of pre-installed commands designed to execute various actions on the compromised system. These actions include injecting assembly, executing Shellcode, capturing authentication details, loading Beacon Object Files (BOFs), and a variety of other functionalities.
- The identity of the Threat Actor responsible for this attack remains unknown, and we currently cannot link it to any known APT groups.

Overview

On July 10, 2023, the Group-IB Threat Intelligence unit discovered an undisclosed vulnerability related to ZIP file processing in WinRAR. Rapidly responding to the alert from the Group-IB team, the RARLAB team quickly addressed this vulnerability. A beta version of the patch was made available on July 20,

2023, and the final updated iteration of WinRAR (version 6.23) was officially released on August 2, 2023.

On August 23, Group-IB officially documented their initial detection of DarkMe malware leveraging this vulnerability (<u>CVE-2023-38831</u>). Moreover, they observed that several other malware families, including GuLoader and Remcos RAT, were also utilizing the same exploit as a means of delivery, which they have elaborated on in their <u>blog</u> post.

Later, it was also observed that several malware developers had initiated the sale of exploits on dark web forums. An example of such a user is AegisCrypter, who was offering this exploit for \$100 on a cybercrime forum, as shown below.

	27.04.2023					
AcgisCrypter Encyst Registation : 22.05.2023 Messages : 58 Reactions : 18	Hi att We are ready to provide you with an exploit for the WINRAR archive. The archive itself download occurs without any detections or threats. Price for WINRAR EXPLOIT - \$100 I'll answer a few questions					
	What name and extension can be given to files that are in the archiver? - Any name and extension, be it pdf png doc or others, there is no difference in this, the same thing can be done with the names of files and					
	What needs to be done for the exploit to work? You need to run the archive and double-click on the file "GoogleMaps.gng (the name and extension can be any)" then your virus will immediately launch and the k					
	- Is it possible to make my build launch at startup and also a picture/document/PDF project? - Yes, this can also be done so that the victim's suspicion is minimal and she takes it at face value.					
	What is needed for the exploit to work? — To do this, it is necessary that the winnar archiver be installed on the victim's computer; most people have it installed and they will be able to run it without any compliants.					
	- Can I see a video demonstration of the exploit in action? - Yes, video of the exploit in action at the Ink - [Institute institute in the Ink - [Institute institute in the Ink - [Institute institute in the Ink - [Institute institut					
	Watch on These watches and the second					

Figure 1 – TA's post about the sale of Exploit in CyberCrime Forum

At the same time, a Proof-of-Concept (POC) for this exploit became publicly available on GitHub. Subsequently, multiple TAs began to adopt and integrate this exploit into their toolkits. The image below shows an X (formerly known as Twitter) <u>post</u> from a security researcher that reveals White Snake Stealer TAs enhancing their builder to include this WinRAR exploit.

White Snake



White Snake

WINRAR | CVE-2023-38831

White Snake update 1.6.0.10

- Added WinRar Oday exploit builder (CVE-<u>2023-38831</u>)

Fixed problems with IPLogger when serveo tunnel didn't created.
Added 7 new fake signatures.
Added 8 new icons.

Figure 2 – WhiteSnake Stealer Telegram Post (Source: @g0njax)

We have also observed a YouTube video providing instructions on constructing an njRAT binary using a builder and utilizing the CVE-2023-38831 vulnerability to generate malicious WinRAR files. The figure below shows a screenshot of a YouTube video utilizing this WinRAR vulnerability to deliver njRAT malware.



Figure 3 – YouTube video showing the njRAT builder Furthermore, on August 31, 2023, the Computer Emergency Response Team of Ukraine (CERT-UA) <u>released</u> a warning regarding the ongoing misuse of CVE-2023-38831 for cyber-espionage operations directed at Ukrainian and Central Asian organizations. These activities were linked to the UAC-0063 group, which also operates under the name "GhostWriter".

CRIL has recently identified and <u>analyzed</u> a campaign that is actively distributing various types of malware, including Apanyan Stealer, Murk-Stealer, and AsyncRAT. These malicious payloads are also delivered through this WinRAR vulnerability.

While investigating the increasing number of incidents involving TAs exploiting this WinRAR Vulnerability to deliver their payloads, CRIL identified a spear phishing email via <u>VirusTotal</u> on September 27. This phishing attempt focuses on targeting Russian entities and involves the distribution of a deceptive archive file via an attachment exploiting the same WinRAR vulnerability (CVE-2023-38831).

The aforementioned vulnerability allows the WinRAR application to extract and execute the malicious script when a user tries to open a benign file within the archive.

This capability initiates the download of a malicious executable onto the victim's system. The downloaded payload is one of the Mythic Agents known as "Athena". Athena is a cross-platform agent designed using the cross-platform version of .NET.

Once installed on the targeted system, Athena provides TAs with a versatile set of functionalities through its predefined commands. These commands include both default commands, such as ipconfig, ls, ps, sleep, etc., as well as custom commands, such as coff, farmer, crop, and so on.

We observed that Mythic Agents had been utilized by the APT-36 group in their operations. One such Agent is "Poseidon." This Advanced Persistent Threat group, based in Pakistan, is notorious for its targeting of Indian government organizations, military personnel, and defense contractors.

Initial Infection

CRIL came across a spear-phishing email targeting a leading semiconductor supplier in Russia. It was sent with the subject line (translated into English) "Regarding the Proposal to Incorporate R&D in the 2024-2025 Work Plan." The sender's identity was manipulated to appear as a consultant from the Ministry of Industry and Trade of Russia. The image below shows this spear-phishing email.

АС О проведении совещания по вопросу включения НИР в план работ на 2024-2025 годы
resultati_sovehchaniya_11_09_2023.rar 246 KB
Egeneer Commente Comm

Figure 4 – Spear Phishing Email

The email contains an attachment named "resultati_sovehchaniya_11_09_2023.rar," which translates to "meeting results." This RAR file contains a PDF file and a folder.

The PDF file and the folder within the archive have identical names. However, there's a deliberate addition of a trailing space at the end of the PDF file's name, as highlighted in the image below.

File Commands Tools Favorites Options Help		
Add Extract To Test View Delete Find Wizard Info VirusSo	an Comment	4
1 International		Figure 5 –
Name	Size	
resultati_sovehchaniya_11_09_2023.pdf resultati_sovehchaniya_11_09_2023.pdf	3,039 255,665	

Contents of the crafted archive file

The PDF file is benign, and the folder serves as a container for the malicious CMD Script file. The image below displays the malicious CMD file present inside the folder.

🙀 resul File Co	resultati_sovehchaniya_11_09_2023.rar (evaluation copy) File Commands Tools Favorites Options Help											
die Add	Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX											
↑	🏪 resultati_so	ovehchani	iya_11_09_2	2023.rar\re	sultati_sove	ehchaniya	_11_09_202	3.pdf - ZIF	archive, unpacked si	ze 258,704 bytes		
Name		^					Size	Packed	Туре	Modified	CRC32	
- File folder												
resultati_sovehchaniya_11_09_2023.pdf .cmd				3	3,039	1,946	Windows Comma	22-09-2023 08:17	81165262			

Figure 6 – Malicious CMD script file

These characteristics of the RAR file can be related to the known security vulnerability CVE 2023-38831.

Technical Analysis

Vulnerability Name: RARLAB WinRAR Code Execution Vulnerability

CVE ID: CVE-2023-38831

CVSS Version 3.1 Sore: 7.8

Severity: High

Vulnerable WinRAR Version: RARLab WinRAR before 6.23

Vulnerability Description: WinRARProcessing error in opening a file in the ZIP archive.

When a user attempts to open the benign PDF file within a specially crafted archive that includes trailing spaces in its name, WinRAR exhibits some unusual behavior. Instead of extracting the intended PDF file, WinRAR also extracts a malicious CMD script file into the temporary folder. This occurs because both components within the archive share identical filenames. The image below shows the extracted files.



Figure 7 – WinRAR extracted files in the temp location

After extracting these files, WinRAR proceeds to execute the PDF file by providing the PDF file name (with trailing space) as one of the parameters in the SHELLEXECUTEINFO structure to the *ShellExecute()* API. The image below shows the PDF file name with the trailing space passed to the

ShellExecute() function.

48:895C24 10 48:897424 18	MOV QWORD PTR SSI ASP+10 .RBX MOV QWORD PTR SS: ASP+18 .RSI	ShellExecuteExW	N Nide FPU
48:897C24 20 55 41:54	MOV QHORD PTR SS: RSP+20 ,RDI PUSH RSP PUSH R12		RAX 00000202078E4AE L"resultati_sovehchaniya_11_09_2023.pdf " BaX 00000000000000
41:56 48:8D6C24 80 48:81EC 80010000	LEA RSP, QWORD PTR SS: RSP-80 SUB RSP, 180		RDX 0000002D278E440 L"CI\\USers\\
48:3304	XOR RAX, RSP	raxic resultati_sovenchaniya_11_0	v Default (x64 fastcal) v s 0

Figure 8 – ShellExecute Function with PDF file name

However, due to the added trailing space in the file name, the ShellExecute() function fails to find the exact file within the extracted files path. As a result, it skips the extracted PDF file and, instead, identifies and runs the malicious script file with a similar name.

"resultati_sovehchaniya_11_09_2023.pdf.cmd".

The executed malicious script file contains a Base64-encoded PowerShell script. The image below shows the de-obfuscated content of the Script file.



Figure 9 – De-obfuscated PowerShell script

Once the PowerShell script is executed, it performs the following actions:

The script attempts to retrieve an identical benign PDF file from the URL

"hxxp://45[.]142[.]212[.]34:80/Resultati soveschaniya30 08 2023[.]pdf" and saves it in the script's working directory. Subsequently, the script opens and presents the contents of the benign PDF file. This is done to use the PDF as a decoy, aiming to divert and confuse users. The image below shows the contents of this PDF file.



ЕВРАЗИЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

Смоленский б-р, д. 3/5, стр. 1, Москва, 119121, тел. 8 (495) 669-24-00, доб. 4133

« 11 » сентября 2023 г.

№ 11-179

По списку рассылки

О проведении совещания по вопросу включения НИР в план работ на 2024-2025 годы

11 сентября на площадке Евразийской экономической комиссии прошло совещание по вопросу включения НИР по теме: «Разработка обзора о тенденциях и перспективах развития технологий, рынков инновационных товаров в мире и в рамках ЕАЭС и выработка предложений о перспективных направлениях технологического сотрудничества в рамках Союза, мерах его поддержки» в План научно-исследовательских работ Евразийской экономической комиссии на 2024-2025 годы.

Направляется в порядке информации.

Figure 10 – Decoy PDF file

Following that, the script proceeds to download a malicious executable file from the URL "hxxp://45[.]142[.]212[.]34:80/aimp2[.]exe" and saves it with the name "aimp2.exe" in the directory "AppData\Local\Microsoft\Windows\Ringtone\". The image below shows the open directory that is hosting the malicious files utilized in this attack.

← → C ▲ Not secure 45.142.212.34	
Directory listing for /	
 <u>AiMP2.ExE</u> <u>AIMP2.eXe</u> <u>Pismo_ishodjashhee_61301-1_8724_ot_27_09_2023_Rassylka_Ministerstva_promyshlennosti.pdf</u> <u>rEsultAti_soVEscHANiyA_11_09_2023.PDF</u> 	

Figure 11 – Open directory

I

Then, it schedules a task to run the downloaded executable every 10 minutes using Windows Task Scheduler, with the task name "aimp2", as shown in the image below.

		(r			
1) Task Scheduler (Local)	Name	Status	Triggers	Next Run Time
ř	Microsoft	🕒 aimp2	Ready	At 12:17 on 06-10-2023 - After triggered, repeat every 10 minutes indefinitely.	06-10-2023 12:27:00
L	Office	O Brandbelle	an, Banky	histophe stype of the st	In the second state of
l	> 🧮 OneCore	() Bandada	na Rada	WWW.com by Washigard, spain as Tran Intelligent Ling.	
L	a 📕 Mandana	C. Contractor	in the	had the second data of the secon	
Entropy Charles Set					
Canada Counter Dandy. Milean Alexandria anandria an medified					
General Triggers Actions Conditions Settings History (disabled)					
		When you	ı create a task,	you must specify the action that will occur when your task starts. To change the	ese actions, open the ta
l		Action		Details	
		Start a pro	ogram	C:\Users\\\AppData\Local\Microsoft\Windows\ringtones\aimp2.	exe

Figure 12 – Task Scheduler entry

Finally, the script proceeds to execute the downloaded executable, which has been identified as the "Athena", one of the <u>agents</u> of Mythic C2 Framework.

Mythic Agent

<u>Mythic</u> is a cross-platform, post-exploit, red teaming framework designed to provide a collaborative and user friendly interface for operators with extensive support for a variety of Agents, as shown in the image below.

MYTHIC	Mythic Agents A centralized area for installable Mythic Agents based on https://github.com/its-a-feature/Mythic_External_Agent									
Overview) Overview 📮 Repositories 21 🗄 Projects 2 😚 Packages 🕆 People 3									
README.md Mythic Name	MythicAgents Organization Image Active Dev (Past Year) SOCKS5 Support C2 Channels Windows macOS x64 macOS M-series Linux									
Apfell	JXA		×	HTTP	×	~	~	×		
Apollo	C# (.NET Framework 4.0)			HTTP, TCP, SMB		×	×	×		
Athena	C# (.NET 6)		V	HTTP, Websockets, Slack, SMB		Z				
<u>freyja</u>	Golang			HTTP, Websockets, freyja_tcp						
hermes	Swift 5		×	HTTP	×	~		×		
<u>Leviathan</u>	Javascript (Chrome Extension)		×	Websockets	×	×	×	×		

Figure 13 – List of Mythic Agents

Mythic provides an advanced web-based C&C interface that allows users or potential TAs to interact with the above-mentioned Agent deployed on compromised systems.

In this specific attack scenario, TAs have employed the <u>Athena</u> Agent, which is developed using a cross-platform version of .NET and specifically designed for compatibility with Mythic versions 3.0 and later.

The file size of the Agent, at 34 MB, is an indicator that it was compiled using the 'self-contained' option. This choice entails the inclusion of the entire .NET runtime within the binary, resulting in a larger file size. The image below displays all the size-related options utilized during the compilation of the Agent.

Agent Size 🖉

There are multiple ways Athena can be built which have a large effect on the final size of the payload

- Standard
 - The smallest option. This contains just the base agent code, and requires you to package all of the DLLs with the agent. Not great for phishing, but the option is there if you want it.
 - File Size: 114KB
- Self Contained
 - The largest option. This contains the base agent code, and the entire .NET framework. This file will be very large, but will allow for the most flexibility when operating. Compression shrinks this size down dramatically
 - File Size: 63MB
 - Compressed Size: 33.8MB
- Self-Contained Trimmed
 - Medium option. This contains the base agent code, and only the required libraries. This file is smaller than the regular self contained option, however you may encounter some difficulties with custom executeassembly assemblies. You will need to load their dependencies manually using load-assembly even if they're usually built into the framework

2

- File Size: 18.5MB
- Compressed Size: 12.8MB

Figure 14 – Size-related options present in Athena Agent

Athena agent comes with a predefined set of commands, as mentioned below, to execute on the compromised host and return the output to the remote server.

Task	Description
arp	Performs arp scan
cat	Display the contents of a file to the terminal
cd	Change working directory
coff	Execute coff file in the agent process
ср	Copy a file from one location to another
crop	Drop a file for collecting hashes on a network
drives	View the connected drives on the host
env	Display the environmental variables on the host
farmer	collects NetNTLM hashes in a Windows domain
get-clipboard	Display the contents of the user clipboard
get-localgroup	Enumerate local groups on a machine
get-sessions	Perform an NetSessionEnum on the provided hosts
get-shares	Perform an NetShareEnum on the provided hosts
hostname	Display the machines hostname

ifconfig	Get IP information of the underlying host
mkdir	Create a new directory
mv	Move a file from one location to another
nslookup	NSLookup a specific host or list of hosts
Patch	check and revert AMSI and ETW for x64 process
ps	Display a process listing on the host
pwd	Print the working directory
reg	Display the contents of the user clipboard
rm	Remove a file
screenshot	Captures screenshot
sftp	Connect to a host and perform actions using SFTP
shell	Execute a shell command with the current default shell
shellcode	Execute a shellcode buffer within the agent
test-port	Perform an NetShareEnum on the provided hosts
timestomp	Match the timestamp of a source file to the timestamp of a destination file
uptime	View the current uptime values of the host

The Athena Agent is integrated with the C3 (Custom Command and Control) framework, enabling communication through a variety of C2 channels to connect with the remote server. The image below showcases the available C2 channels supported by Athena.

HTTP 🖉

Athena can act as an egress channel over the default http Profile in use by Mythic.

Note: All taskings and Responses are done via POST requests. So the GET URI parameter is unnecessary at this time.

Websockets @

Athena can act as an egress channel over the websocket profile. This is the recommended profile to use when making use of the SOCKS5 functionality.

Slack 🖉

Athena can communicate over slack channels.

Note: Due to slack API rate limiting, the number of agents that can be executed at once using a specific workspace/token combination is limited. A lower sleeptime supports more agents.

Discord @

Athen can communicate over discord channels.

Note: Due to slack API rate limiting, the number of agents that can be executed at once using a specific workspace/token combination is limited. A lower sleeptime supports more agents.

SMB 🖉

Athena supports SMB communications for internal comms over named pipes.

Figure 15 – C2 Channels supported by Athena Agent

In this specific case, C3 communications are facilitated via a Discord Channel after the Agent starts sending back the victim's data to the remote server.

Conclusion

Phishing emails with malicious attachments continue to be the preferred tactic for threat actors. The use of crafted archives exploiting the WinRAR vulnerability adds an extra layer of challenge to defense mechanisms.

In the current threat landscape, vulnerabilities are discovered and patched with remarkable frequency. However, among the countless vulnerabilities that come and go, there are a select few that persist, defying even the most diligent efforts on the part of vendors to eradicate them. The WinRAR vulnerability we've discussed in this analysis falls into this category—a vulnerability that remains a potent threat even after it has been patched.

Furthermore, the delivery of this powerful Agent allows attackers to take control of compromised systems and conduct remote monitoring, making it a formidable weapon in the hands of threat actors.

Recommendations

• The initial infection happens via spam emails or phishing websites; thus, enterprises should use security products to detect phishing emails and websites.

- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Update WinRAR to the latest update as soon as possible if not patched.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Procedure
Initial Access <u>(TA0001)</u>	Phishing (<u>T1566.001</u>)	TAs send spearphishing emails with malicious Attachments
Execution (TA0002)	User Execution (<u>T1203</u>)	Exploitation for Client Execution
Execution (TA0002)	Command and Scripting Interpreter (<u>T1059</u>)	cmd.exe is used to run a CMD malicious script file
Execution (TA0002)	Command and Scripting Interpreter (T1059.001)	PowerShell commands are used to download and execute additional payloads on the system
Persistence <u>(TA0003)</u>	Registry Run Keys / Startup Folder (<u>T1547.001</u>)	Malware adding run entry/Startup for persistence.
Defense Evasion (<u>TA0005)</u>	Masquerading (<u>T1036.006</u>)	Adding Space after Filename
Defense Evasion (<u>TA0005)</u>	Masquerading (<u>T1036.007</u>)	Adding Double File Extension
Collection (TA0009)	Data from Local System (<u>T1005</u>)	The malware collects sensitive data from victim's system.
Command and Control (TA0011)	Application Layer Protocol: Web Protocols (<u>T1437.001</u>)	Communicated with C&C server using HTTP
Exfiltration (TA0010)	Exfiltration Over C2 Channel (<u>T1041</u>)	Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

Indicators	Indicator	Description
	Туре	
0fead8db0ee27f906d054430628bd8fd3b09ca75ff6067720a5b179f6a674c12	SHA256	Phishing Email
5261425cf389ed3a77ec5f03f73daf711e80d4918be3f0fba0152b424af7b684	SHA256	Malicious RAR File

07f8af85b8bbfb432d98b398b4393761c37596ee2cf3931564784bd3e8c2b1cc	SHA256	Malicious .cmd File
45[.]142[.]212[.]34	IP	Malicious IP
86079a2d12b28a340281453efa0a7fd31c65ead11bab98edd94fe19aaff436eb	SHA256	Athena – Mythic Agent
162[.]159[.]137[.]232	IP	Malicious Discord IP
162[.]159[.]129[.]233	IP	Malicious Discord IP
162[.]159[.]122[.]233	IP	Malicious Discord IP
162[.]159[.]128[.]233	IP	Malicious Discord IP
17269514f520cda20ecc78bdb0b3341a97bb03e155640704a87efff832555b14	SHA256	Malicious RAR File
79c78466d61b05466289f91122d2b7dbd56e895c15fe80d385885f9eddf31ca5	SHA256	Malicious .cmd File

References

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/exploring-winrar-vulnerability-cve-2023-38831/

Yara Rule

{

```
rule Athena_Mythic Agent
meta:
author = "Cyble"
description = "Detects Agent Athena"
date = "2023-10-09"
os = "Windows"
threat_name = "Mythic Athena Agent"
scan_type = "file"
severity = 90
reference_sample = "86079a2d12b28a340281453efa0a7fd31c65ead11bab98edd94fe19aaff436eb"
```

strings:

- \$a = "Athena.Commands" ascii wide
- \$b = "Athena.Handler.Dynamic" ascii wide
- \$c = "get-clipboard" ascii wide
- \$d = "get-sessions" ascii wide
- \$e = "shellcode" ascii wide

condition:

uint16(0) == 0x5a4d and all of them

}