

New details on TinyTurla’s post-compromise activity reveal full kill chain

By Asheer Malhotra

Published: 2024-03-21 · Archived: 2026-04-05 19:50:10 UTC

Cisco Talos is providing an update on its [two recent](#) reports on a new and ongoing campaign where Turla, a Russian espionage group, deployed their [TinyTurla-NG \(TTNG\)](#) implant. We now have new information on the entire kill chain this actor uses, including the tactics, techniques and procedures (TTPs) utilized to steal valuable information from their victims and propagate through their infected enterprises.

- Talos’ analysis, in coordination with [CERT.NGO](#), reveals that Turla infected multiple systems in the compromised network of a European non-governmental organization (NGO).
- The attackers compromised the first system, established persistence and added exclusions to anti-virus products running on these endpoints as part of their preliminary post-compromise actions.
- Turla then opened additional channels of communication via Chisel for data exfiltration and to pivot to additional accessible systems in the network.

Tracing Turla’s steps from compromise to exfiltration

Talos discovered that post-compromise activity carried out by Turla in this intrusion isn’t restricted to the sole deployment of their backdoors. Before deploying TinyTurla-NG, Turla will attempt to configure anti-virus software exclusions to evade detection of their backdoor. Once exclusions have been set up, TTNG is written to the disk, and persistence is established by creating a malicious service.

Preliminary post-compromise activity and TinyTurla-NG deployment

After gaining initial access, Turla first adds exclusions in the anti-virus software, such as Microsoft Defender, to locations they will use to host the implant on the compromised systems.

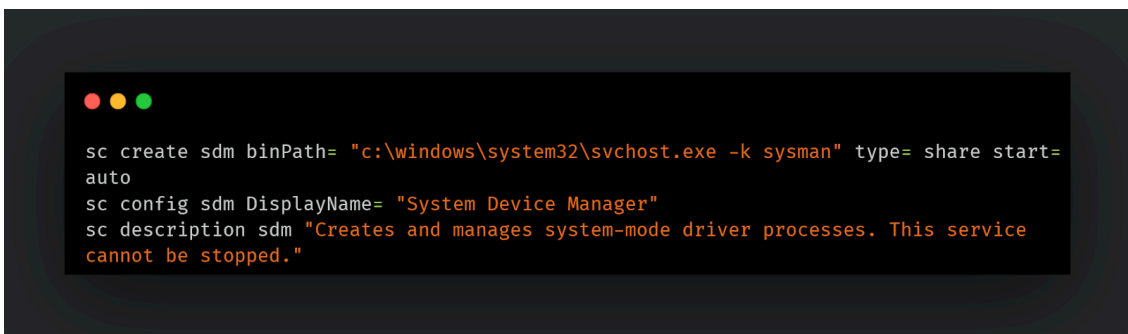
ACTION	INTENT
HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths “C:\Windows\System32\” = 0x0	[T1562.001] Impair Defenses: Disable or Modify Tools

Turla then sets up the persistence of the TinyTurla-NG implants using one or more batch (BAT) files. The batch files create a service on the system to persist the TTNG DLL on the system.

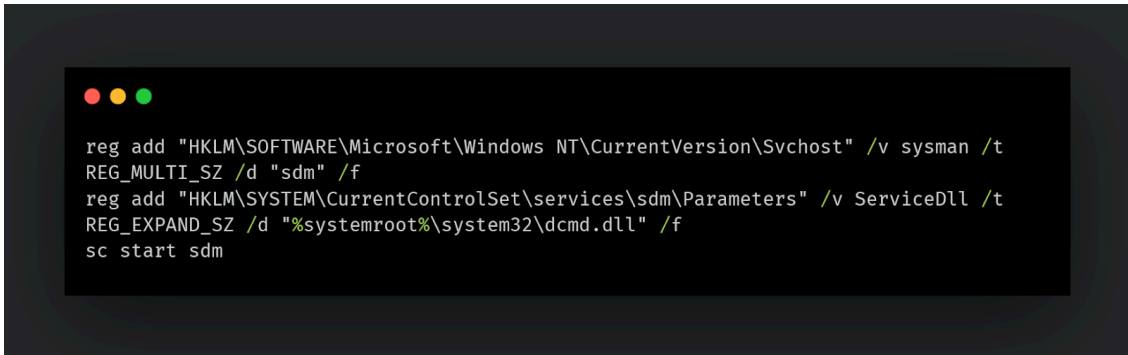
ACTION	INTENT
<pre>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v sysman /t REG_MULTI_SZ /d "sdm" /f reg add "HKLM\SYSTEM\CurrentControlSet\services\sdm\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%systemroot%\system32\dcmd.dll" /f</pre>	<p>[T1543.003] Create or Modify System Process: Windows Service</p>
<pre>sc create sdm binPath= "c:\windows\system32\svchost.exe -k sysman" type= share start= auto sc config sdm DisplayName= "System Device Manager" sc description sdm "Creates and manages system-mode driver processes. This service cannot be stopped."</pre>	<p>[T1543.003] Create or Modify System Process: Windows Service</p>

This technique is identical to that used by Turla in 2021 to achieve persistence for their [TinyTurla](#) implants. However, we're still unsure why the actor uses two different batch files, but it seems to be an unnecessarily convoluted approach to evade detections.

In the case of TTNG, the service is created with the name "sdm" masquerading as a "System Device Manager" service.



```
sc create sdm binPath= "c:\windows\system32\svchost.exe -k sysman" type= share start= auto  
sc config sdm DisplayName= "System Device Manager"  
sc description sdm "Creates and manages system-mode driver processes. This service cannot be stopped."
```



```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v sysman /t REG_MULTI_SZ /d "sdm" /f  
reg add "HKLM\SYSTEM\CurrentControlSet\services\sdm\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%systemroot%\system32\dcmd.dll" /f  
sc start sdm
```

Batch file contents.

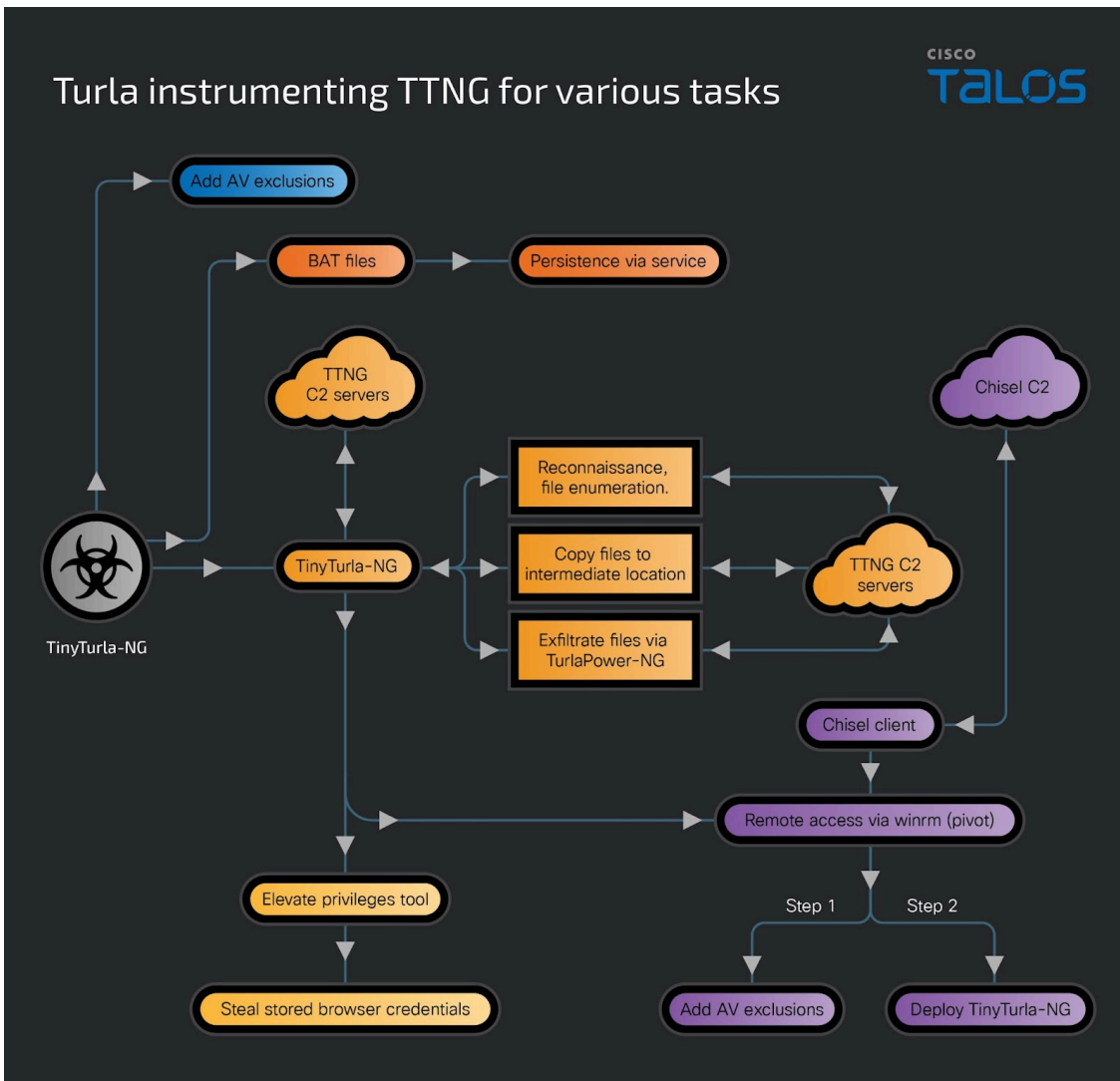
The creation and start of the malicious service kick starts the execution of the TinyTurla-NG implant via svchost[.]exe (Windows' service container). TinyTurla-NG is instrumented further to conduct additional reconnaissance of directories of interest and then copy files to a temporary staging directory on the infected system, followed by subsequent exfiltration to the C2. TinyTurla-NG is also used to deploy a custom-built Chisel beacon from the open-sourced offensive framework.

Custom Chisel usage

On deployment, Chisel will set up a reverse proxy tunnel to an attacker-controlled box [[T1573.002](#) - Encrypted Channel: Asymmetric Cryptography]. We've observed that the attackers leveraged the chisel connection to the initially compromised system, to pivot to other systems in the network.

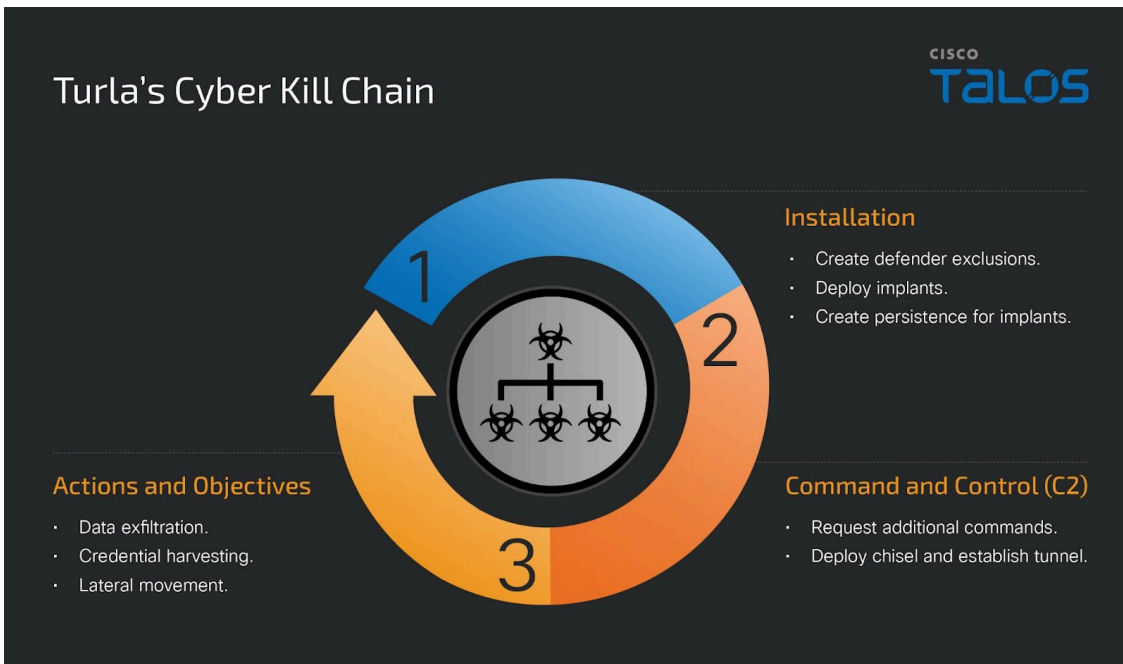
The presence of Windows Remote Management (WinRM)-based connections on the target systems indicates that chisel was likely used in conjunction with other tools, such as proxy chains and evil-winrm to establish remote sessions. [WinRM](#) is Microsoft's implementation of the WS-Management protocol and allows Windows-based systems to exchange information and be administered using scripts or built-in utilities.

The overall infection chain is visualized below.



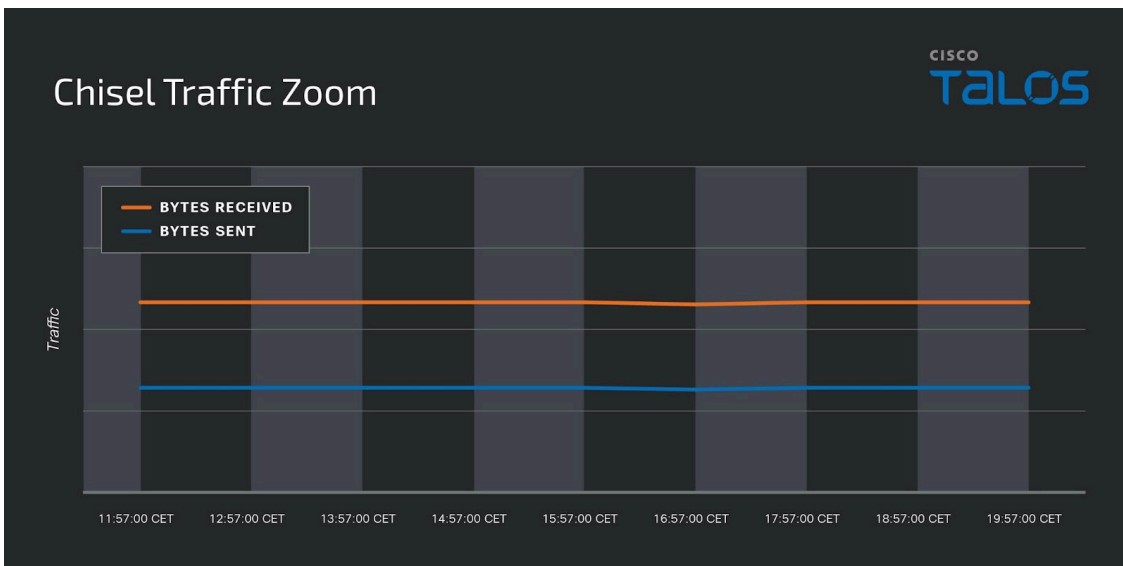
Turla tactics, tools and procedures flow.

Once the attackers have gained access to a new box, they will repeat their activities to create Microsoft Defender exclusions, drop the malware components, and create persistence, indicating that Turla follows a playbook that can be articulated as the following cyber kill chain.

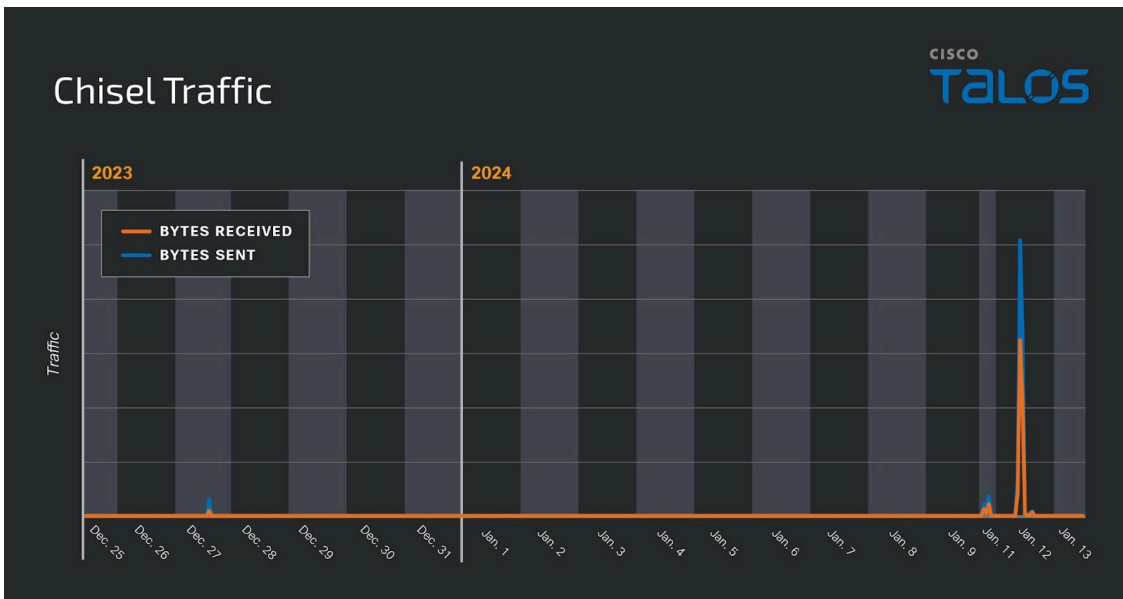


Cyber kill chain.

Analyzing the traffic originating from Chisel revealed the tool beacons back to its C2 server every hour.



While the infected systems were compromised as early as October 2023 and Chisel was deployed as late as December 2023, Turla operators conducted the majority of their data exfiltration using Chisel much later on Jan. 12, 2024 [[T1041](#) - Exfiltration Over C2 Channel].



Coverage

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

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✓	✓	✓	✓

[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 Web Appliance](#) web scanning prevents access to malicious websites and detects malware used in these attacks.

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

[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. Sign up for a free trial of Umbrella [here](#).

[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](#).

IOCS

Hashes

267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b
d6ac21a409f35a80ba9ccfe58ae1ae32883e44ecc724e4ae8289e7465ab2cf40
ad4d196b3d85d982343f32d52bffc6ebfeec7bf30553fa441fd7c3ae495075fc
13c017cb706ef869c061078048e550dba1613c0f2e8f2e409d97a1c0d9949346
b376a3a6bae73840e70b2fa3df99d881def9250b42b6b8b0458d0445dddfbc044

Domains

hanagram[.]jpthefinetreats[.]com
caduff-sa[.]chjeepcarlease[.]com
buy-new-car[.]com
carleasingguru[.]com

IP Addresses

91[.]193[.]18[.]120

Source: <https://blog.talosintelligence.com/tinyurla-full-kill-chain/>