

NightEagle targets Russian companies

SL securelist.com/tr/nighteagle-apt-ghostcontainer-and-tunneling/121323

Stanislav Larinsky, Kaspersky Security Services

September 16, 2026



Over the past year, our Global Emergency Response Team (GERT) has investigated several incidents involving the NightEagle group (also tracked as [APT-Q-95](#)). This group has been active since at least 2023 and originally focused on organizations in Asia. We have now identified attacks by the group targeting businesses in Russia. This post examines both known and new tools NightEagle used in its latest campaign.

Initial access

In most incidents, the attackers used compromised valid credentials to gain access to corporate VPNs. VPN connections originated from IP addresses in the Russian segment linked to Cloudflare WARP tunnels, as well as from IP addresses associated with European virtual infrastructure providers.

GhostContainer on Microsoft Exchange

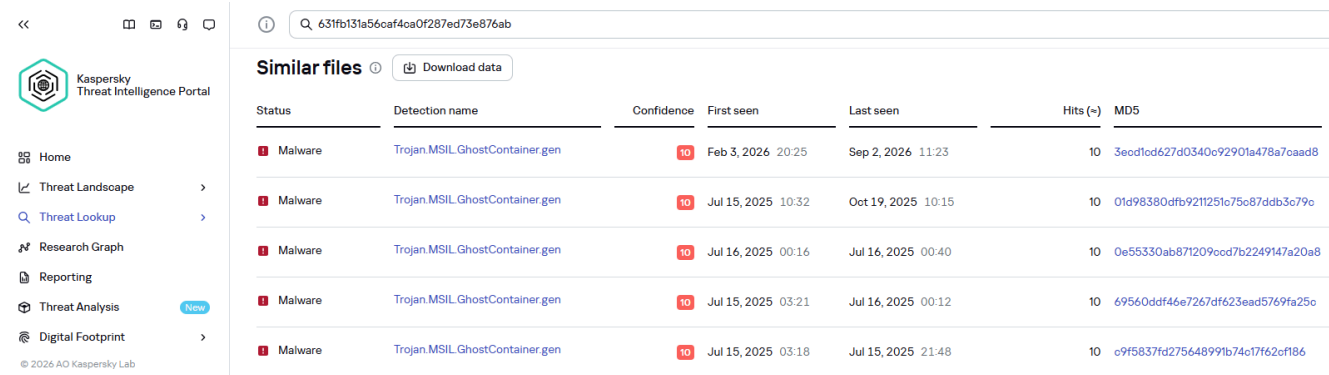
Both during the initial access stage and as the attack progressed, the attackers deployed the [GhostContainer backdoor](#) on Microsoft Exchange servers. It incorporates components from several open-source projects, including the Neo-reGeorg tunnel, an exploit for the CVE-2020-0688 vulnerability, and the GhostWebShell class from the ysoserial utility. All of these components are publicly available on GitHub.

We were unable to determine the exact method the attackers used to deliver the backdoor to Microsoft Exchange servers. We believe with a high degree of confidence that they applied a [technique already familiar to us](#): extracting the cryptographic keys used by Microsoft Exchange from the ASP.NET configuration, overwriting the VIEWSTATE framework parameter, and injecting a payload into it, which then launched the GhostContainer backdoor in memory.

The backdoor is a .NET assembly containing three classes that implement its core functionality:

- Stub: processes C2 commands delivered to the infected system through the x-owa-urlpostdata headers and evades detection by the Antimalware Scan Interface (AMSI) and Windows Event Log mechanisms by overwriting addresses in `amsi.dll` and `ntdll.dll`.
- App_Web_843e75cf5b63: accepts the `fakePath` and `fakePageName` parameters and creates virtual paths that redirect requests to the App_Web_8c9b251fb5b3 class.
- App_Web_8c9b251fb5b3: implements network traffic redirection (proxying) and socket forwarding functionality.

Kaspersky products detect the GhostContainer backdoor as Trojan.MSIL.GhostContainer.gen.



The screenshot shows the Kaspersky Threat Intelligence Portal interface. On the left is a sidebar with navigation links: Home, Threat Landscape, Threat Lookup, Research Graph, Reporting, Threat Analysis (marked as 'New'), and Digital Footprint. The main area displays a search result for a file with ID 631fb131a56caf40a0f287ed73e876ab. Below the search bar, there's a section titled 'Similar files' with a 'Download data' button. A table lists five similar files, all identified as 'Trojan.MSIL.GhostContainer.gen' with a confidence of 10. The table columns are Status, Detection name, Confidence, First seen, Last seen, Hits, and MD5.

Status	Detection name	Confidence	First seen	Last seen	Hits (→)	MD5
Malware	Trojan.MSIL.GhostContainer.gen	10	Feb 3, 2026 20:25	Sep 2, 2026 11:23	10	3e0d10d627d0340c92901a478a7caad8
Malware	Trojan.MSIL.GhostContainer.gen	10	Jul 15, 2025 10:32	Oct 19, 2025 10:15	10	01d98380dfb9211251c75c87ddb3c79c
Malware	Trojan.MSIL.GhostContainer.gen	10	Jul 16, 2025 00:16	Jul 16, 2025 00:40	10	0e55330ab871209cdd7b2249147a20a8
Malware	Trojan.MSIL.GhostContainer.gen	10	Jul 15, 2025 03:21	Jul 16, 2025 00:12	10	69560dd46e7267df623ead5769fa25c
Malware	Trojan.MSIL.GhostContainer.gen	10	Jul 15, 2025 03:18	Jul 15, 2025 21:48	10	c9f5837fd27564899fb74c17f62cf186

GhostContainer samples identified by the Similarity technology from Kaspersky Threat Analysis

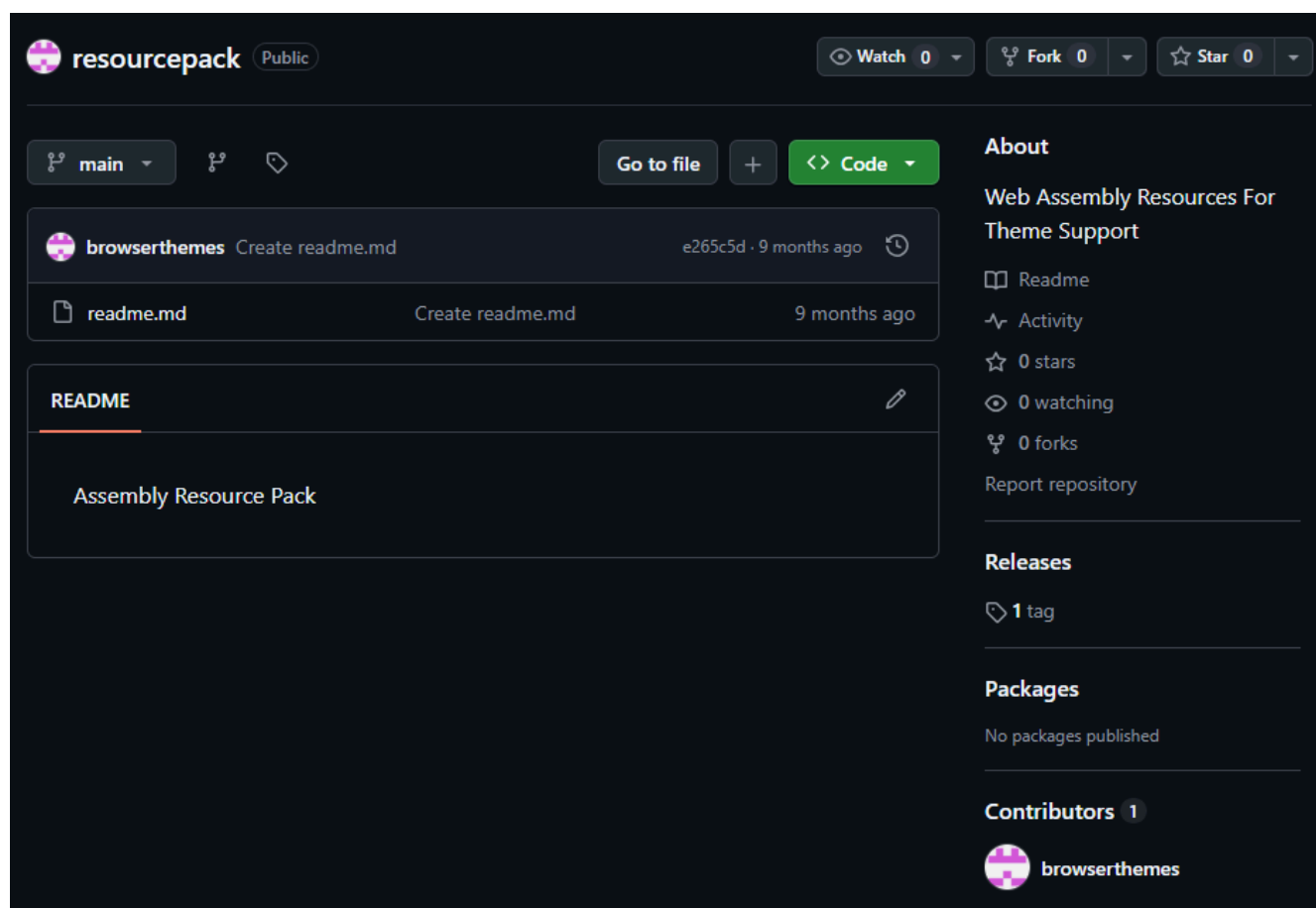
Traffic redirection

Once the attackers gain sufficient privileges during an attack, they leverage RDP to move laterally within the internal network segment. To do this, they download and run tools for tunneling and redirecting network traffic.

The attackers used GitHub repositories to host their archived tools. The names of the repositories and archives were disguised to look legitimate:

- <https://github.com/mirror-js/mirror-js/refs/heads/main/js/js-webpack.zip>
- <https://github.com/mirror-js/mirror-js/refs/heads/main/js/jsonp-pack.zip>

- <https://github.com/browserthemes/resourcepack/releases/download/main/resource-pack.zip>



One of the repositories used for storing network tools

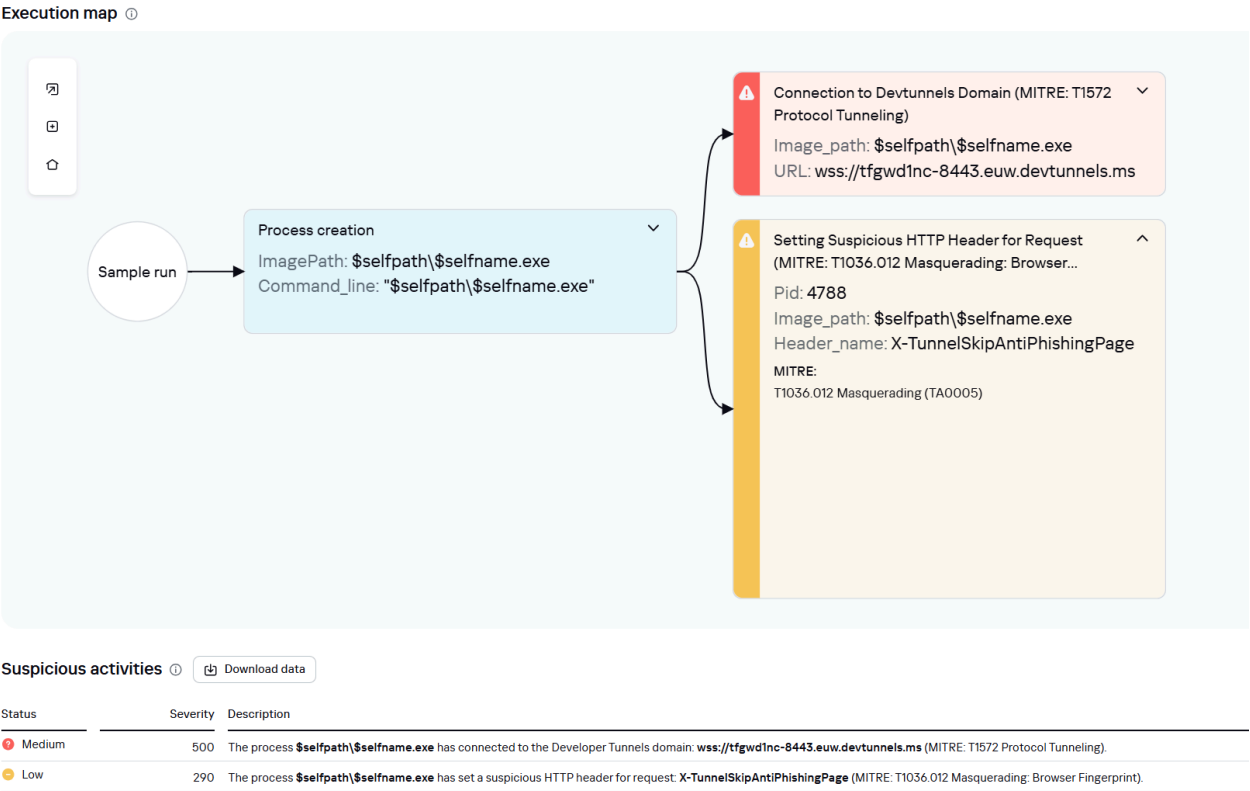
The files contained within the archives were also given names mimicking known legitimate software, though unrelated to the archive names:

- adobe_32.exe;
- AdobeSync.exe;
- trueconf.exe;
- lcbroker.exe;
- lc-office-plugin.exe;
- trueconf-broker.exe.

Across the incidents we investigated, we found two tools that the attackers combined for traffic tunneling.

1. 1 Microsoft dev tunnels

This is a [legitimate Microsoft mechanism](#) that allows local web services to be published for internet access on *.*.devtunnels.ms domains. The attackers used this tunneling capability to expose port 3389 (RDP) on the compromised system.



Execution graph of adobe_32.exe in Kaspersky Research Sandbox

2. 2 rdp2tcp

This is a [publicly available tool](#) for tunneling TCP traffic over an established RDP connection. It includes a server component that runs on the target system and a client component that runs on the attacker's side.

When virtual channels are opened and closed, corresponding events with IDs 132 (channel opened) and 148 (channel closed) are logged in the *Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational.evtx* Windows log. These events contain the names of the channels (such as XPSRD, clipdr, Microsoft::Windows::RDS::DisplayControl, and others) used by the RemoteFX module, which extends the capabilities of the RDP protocol.

When the rdp2tcp tool is used, events with IDs 132 and 148 will contain the channel name rdp2tcp or other random alphanumeric combinations chosen by the attackers.

Level	Date and Time	Source	Event ID	Task Category
Information	8/10/2026 5:23:27 PM	RemoteDesktopServices-RdpCoreTS	132	RemoteFX module
Information	8/10/2026 5:23:24 PM	RemoteDesktopServices-RdpCoreTS	148	RemoteFX module

Event 132, RemoteDesktopServices-RdpCoreTS	
General	
A channel rdp2tcp has been connected between the server and the client using transport tunnel: 0.	
Log Name:	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
Source:	RemoteDesktopServices-RdpCoreTS
Event ID:	132
Level:	Information
User:	NETWORK SERVICE
OpCode:	EstablishConnection
Logged:	8/10/2026 5:23:27 PM
Task Category:	RemoteFX module
Keywords:	
Computer:	WIN-CCHBBUI5FSO

Creation event for a channel named rdp2tcp (server component startup)

The combination of Microsoft dev tunnels and rdp2tcp allows the attackers to maintain network access by using legitimate services without opening additional suspicious ports.

The attackers also used the atexec utility from the Impacket toolkit to create scheduled tasks on target systems. These tasks enabled network port forwarding through standard Windows functionality:

```
1 netsh interface portproxy add v4tov4 listenport=443 connectaddress=10.0.12.101
connectport=445
```

Lateral movement

To obtain elevated privileges and move laterally through the network, NightEagle exploited various vulnerabilities in Active Directory. The attackers used previously established tunnels to connect to internal infrastructure systems.

In one incident, they exploited a well-known RDP implementation vulnerability, CVE-2019-0708 (BlueKeep). They used the vulnerable mechanism to create a local account on the system and add it to the Administrators and Remote Desktop Users groups.

```
00000000: 37 13 E3 EF-0F AC 0D B0- USERMODE_EGG  F FF 49 7!!πno%J HìJ· I
00000010: B8 69 20 E4-EF 0F AC 0D-B0 48 81 E9-00 04 00 00 7 i Σno%J Hü0 ♦
00000020: 48 2D 00 04-00 00 48 8B-51 F8 4C 39-C2 75 EA FF H- ♦ HìQ°L9TuΩ
USERMODE_EGG 37 13 E3-EF 0F AC 0D-B0 FC 48 83-E4 F0 E8 C0 β7!!πno%J nHâΣ≡0L
00000040: 00 00 00 41-51 41 50 52-51 56 48 31-D2 65 48 8B AQAPRQVH1TeHî
00000050: 52 SHELLCODE 48 8B-52 20 48 8B-72 50 48 0F R`HîR↑HîR HîrPHo
00000060: B7 4A 4A 4D-31 C9 48 31-C0 AC 3C 61-7C 02 2C 20 7 JJM1fH1 L%<a|θ,
00000070: 41 C1 C9 0D-41 01 C1 E2-ED 52 41 51-48 8B 52 20 A┘fJAθ┘ΓφRAQHîR
00000080: 8B 42 3C 48-01 D0 8B 80-88 00 00 00-48 85 C0 74 îB<Hθ┘iÇê Hà Lt
00000090: 67 48 01 D0-50 8B 48 18-44 8B 40 20-49 01 D0 E3 gHθ┘PîH↑Dî@ IO┘π
000000A0: 56 48 FF C9-41 8B 34 88-48 01 D6 4D-31 C9 48 31 VH fAi4êHθ┘M1fH1
000000B0: C0 AC 41 C1-C9 0D 41 01-C1 38 E0 75-F1 4C 03 4C L%A┘fJAθ┘8au±L♥L
000000C0: 24 08 45 39-D1 75 D8 58-44 8B 40 24-49 01 D0 66 $E9Tu┘XDî@ $IO┘f
000000D0: 41 8B 0C 48-44 8B 40 1C-49 01 D0 41-8B 04 88 48 AîQHDî@_IO┘Aî♦êH
000000E0: 01 D0 41 58-41 58 5E 59-5A 41 58 41-59 41 5A 48 θ┘AXAX^YZAXAYAZH
000000F0: 83 EC 20 41-52 FF E0 58-41 59 5A 48-8B 12 E9 57 â∞ AR αXAYZHî↓0W
00000100: FF FF FF 5D-48 BA 01 00-00 00 00 00-00 00 48 8D JH||θ Hì
00000110: 8D 01 01 00-00 41 BA 31-8B 6F 87 FF-D5 BB E0 1D ìθθ A||1iöç Γα↔
00000120: 2A 0A 41 BA-A6 95 BD 9D-FF D5 48 83-C4 28 3C 06 *A||ð-¥ fHâ-(<♣
00000130: 7C 0A 80 FB-E0 75 05 BB-47 13 72 6F-6A 00 59 41 |Çvau+qG!!roj YA
00000140: 89 DA FF D5-6E 65 74 20-75 73 65 72-20 62 6F 73 ër fnet user
00000150: 63 68 20 4B-74 6B 31 37-33 36 32 20-2F 61 64 64 /add
00000160: 20 26 26 20-6E 65 74 20-6C 6F 63 61-6C 67 72 6F && net localgro
00000170: 75 70 20 52-65 6D 6F 74-65 20 44 65-73 6B 74 6F up Remote Deskto
00000180: 70 20 55 73-65 72 73 20-62 6F 73 63-68 20 2F 61 p Users /a
00000190: 64 64 20 26-26 20 6E 65-74 20 6C 6F-63 61 6C 67 dd && net localg
000001A0: 72 6F 75 70-20 41 64 6D-69 6E 69 73-74 72 61 74 roup Administrat
000001B0: 6F 72 73 20-62 6F 73 63-68 20 2F 61-64 64 00 00 ors /add
```

Contents of a system memory dump showing artifacts of the CVE-2019-0708 exploit

The attackers also requested Kerberos tickets with a non-standard combination of flags (Forwardable, Proxiable, Renewable) and attempted to replicate the Domain-Password object from the Active Directory database to impersonate the domain controller (a technique known as DCSync) after obtaining an account with sufficient privileges.

Through these methods, the attackers establish persistence in the infrastructure, obtain password hashes for domain accounts, use long-lived Kerberos tickets to gain legitimate access to target resources, and ultimately compromise domain controllers and the victim's entire Active Directory infrastructure.

Takeaways

To expand the geographic scope of its targets, NightEagle is updating its methods and adopting new techniques for persistence and lateral movement. Despite the group's efforts to stay hidden, timely detection of anomalies combined with a comprehensive approach to infrastructure protection can significantly hinder the attackers from achieving their goals. Since the attackers rely on known legitimate tools and infrastructure vulnerabilities, well-configured monitoring can help detect NightEagle's presence on the network.

Detection by Kaspersky solutions

Kaspersky solutions reliably identify the malicious activity described above at various stages of the attack. We showed examples above of how [Kaspersky Threat Analysis](#) detects samples of the GhostContainer backdoor and the tunneling utility. This toolkit also includes the analytical solution [Kaspersky Threat Attribution Engine](#) (KTAE), which helps SOC analysts and incident responders determine which APT groups malware can be attributed to. The solution uses a proprietary comparison method that measures the similarity between analyzed samples of suspicious files and known malicious samples in Kaspersky's collection.

The backdoor we discovered showed similarity to previously analyzed GhostContainer samples and a connection to the NightEagle APT group:

Summary 📄 Attribution

Report for file

631fb131a56caf4ca0f287ed73e876ab

📄 Export results

🚫 Malware

MD5	631fb131a56caf4ca0f287ed73e876ab	Matched attribution entities	GhostContainer (94%) >
File size	28.00 KB (28672 B)	Extracted path	—
Reset similarity thresholds	✓	Unpack	✓

Sample & Content

Status	MD5	File name	Size	Bad genotypes (matched/total)	Bad strings (matched/total)	Attribution entities
🚫 Malware	631fb131a56caf4ca0f287ed73e8	631fb131a56caf4ca0f287ed73...	28.00 KB (28672 B)	184 (184)	21 (21)	GhostContainer (94%) >

Similar samples

Status	MD5	Size	Genotypes matched (total)	Strings matched (total)	Similarity	Attribution entities	Aliases
🚫 Malware	0e55330ab871209ccd7b2249147a20a8	28.00 KB (28672 B)	184 (196)	21 (54)	94	GhostContainer >	
🚫 Malware	01d98380dfb9211251c75c87ddb3c79c	32.00 KB (32768 B)	63 (261)	21 (59)	36	GhostContainer >	

Matched genotypes

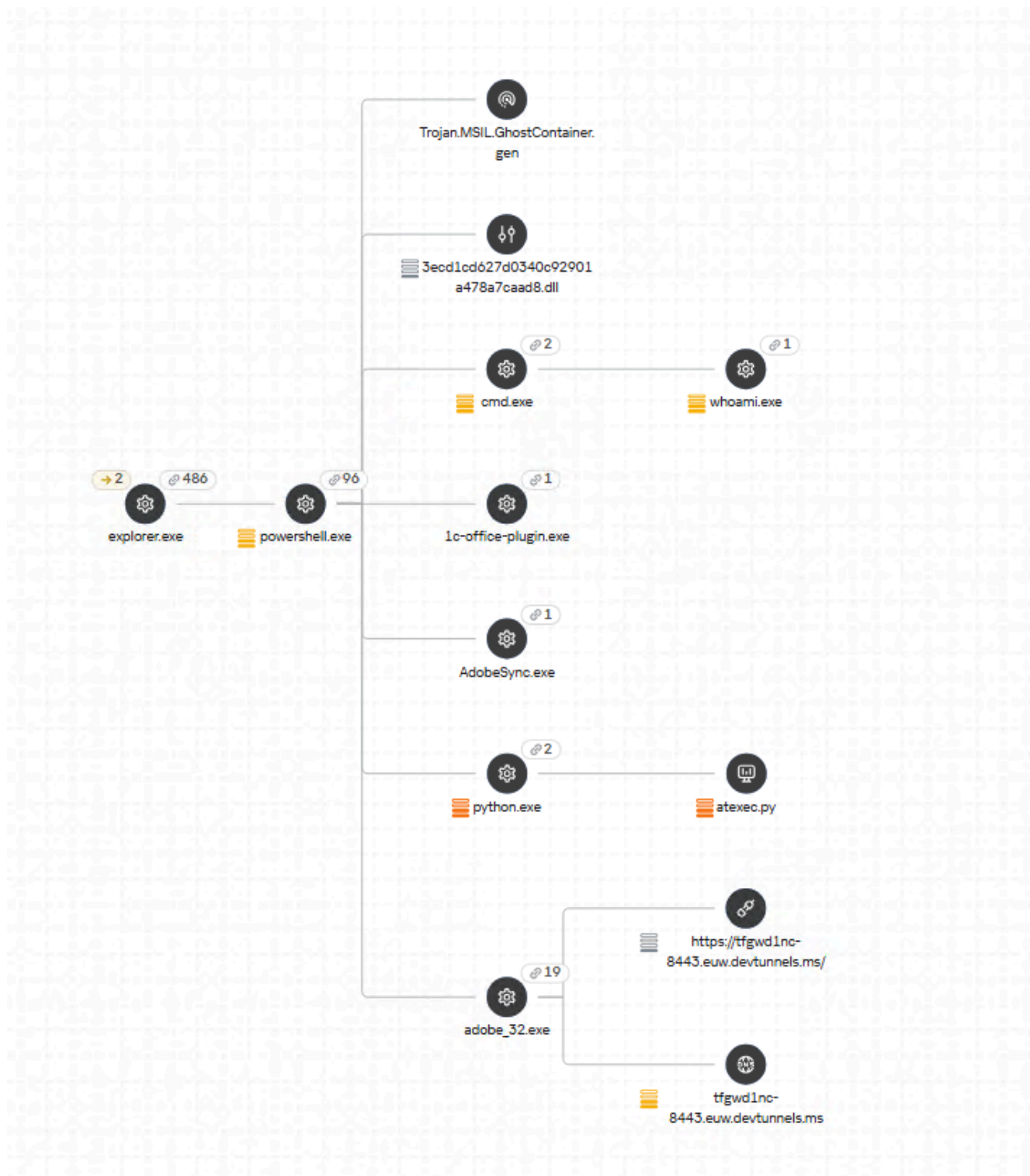
Genotype	Matched	Used by
506167654e616d650073616d706c6550	2	GhostContainer (2)
506174680066616b65506167654e616d	2	GhostContainer (2)
5061696c7a7300a87a7a7057a562e2a5	—	—

Backdoor analysis with KTAE

However, detection scenarios for this kind of attacks are not limited to file analysis. Deploying a backdoor on a target host produces numerous characteristic artifacts, which allow [Kaspersky Endpoint Detection and Response Expert](#) to alert users to anomalies in the infrastructure in a timely manner.

This malicious activity is detected by the following rules, available in the repository:

- Initial detection of the malicious signature occurs through the generic_ransomware_related_detection rule, based on EPP module events
- Detection of a malicious DLL's .NET assembly being loaded via PowerShell: [suspicious_assembly_loading_into_powershell_via_reflection](#)
- Activity of tunneling and traffic redirection tools: [detection_of_access_to_tunnel_domains_dns](#)
- Use of tools from the Impacket toolkit, such as atexec:
 - [impacket_possible_activity](#)
 - [attempt_to_download_hacktool_or_risktool_by_non_browser](#)
 - [credentials_dumping_tools_file_artifacts_creation](#)
- Attempts to replicate an Active Directory database object to impersonate a domain controller: [potential_dcsync_via_startupparameters](#)



Process tree in KEDR Expert

[Kaspersky Anti Targeted Attack \(KATA\)](#) detects this malicious activity in network traffic. For example, the [Exploit.CVE-2019-0708.TCP.C&C](#) signature allows detecting attempts to exploit the CVE-2019-0708 (BlueKeep) vulnerability.

**Kaspersky
Anti Targeted
Attack Platform**

- Dashboard
- Alerts** 109
- Network traffic events
- Custom rules ▾
- Storage
- Assets
- Network map
- Risks and anomalies
- Reports ▾
- Logs ▾
- Settings >
- Sensor servers

All alerts > Alert #11310

Show related ▾

Assign to @Me ▾

Close alert

State New

Importance High

Data source SPAN Sensor 198.19.1.1 (2026-09-09 15:44:27)

Time created 2026-09-09 15:44:27

Time updated 2026-09-09 15:44:30

Scan results

IDS Exploit.CVE-2019-0708.TCP.C&C, Exploit.Win32.CVE-2019-0708.a

IDS rule

Payload

```
length = 580

000 03 00 00 13 0E FD 00 00 00 00 00 01 00 08 00 00  ▼..!12#.....0.0..
010 00 00 00 03 00 01 FD 02 FD FD 7F 65 FD 01 FD 04  ...▼.0#0#0#0#0#0#
020 01 01 04 01 01 01 01 FD 30 19 02 04 00 00 00 00  00+0000#0+0+...
030 02 04 00 00 00 02 02 04 00 00 00 00 02 04 00 00  00+...00+...0+...
040 00 01 02 04 00 00 00 00 02 04 00 00 00 01 02 02  .00+...0+...000
050 FD FD 02 04 00 00 00 02 30 19 02 04 00 00 00 01  #00+...00+0+...0
060 02 04 00 00 00 01 02 04 00 00 00 01 02 04 00 00  00+...00+...00+...
070 00 01 02 04 00 00 00 00 02 04 00 00 00 01 02 02  .00+...0+...000
080 04 20 02 04 00 00 00 02 30 1C 02 02 FD FD 02 02  ♦ 00+...00L00#000
090 FD 17 02 02 FD FD 02 04 00 00 00 01 02 04 00 00  #1000#00+...00+...
0a0 00 00 02 04 00 00 00 01 02 02 FD FD 02 04 00 00  ..00+...000#00+...
0b0 00 02 04 FD 01 33 00 05 00 14 7C 00 01 FD 2A 00  .00+03.+.|||.0#*.
0c0 08 00 10 00 01 FD 00 44 75 63 61 FD 1C 01 FD FD  0.►.0#.Duc0#L00#
```

Rule details

Beyond this activity, KATA also detects other NightEagle actions in network traffic, such as the following:

Indicators of compromise

- [Active directory](#)
- [DLL](#)
- [GhostContainer](#)
- [Traffic tunneling](#)

Products & Services:

Table of Contents

- [Initial access](#)
- [GhostContainer on Microsoft Exchange](#)
- [Traffic redirection](#)
- [Lateral movement](#)
- [Takeaways](#)
- [Detection by Kaspersky solutions](#)
- [Indicators of compromise](#)