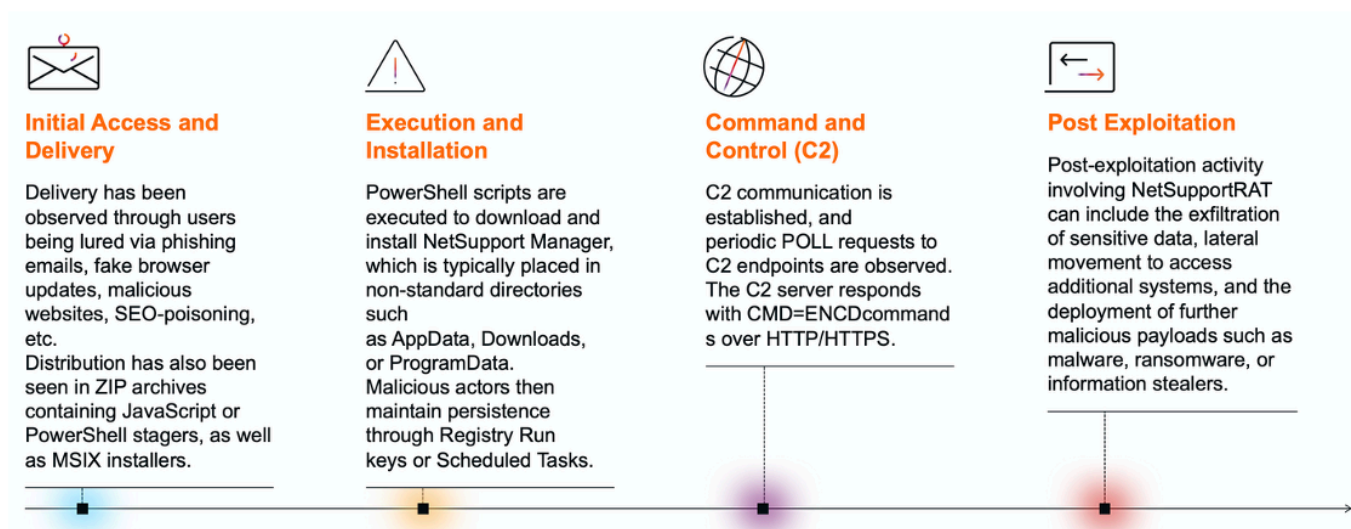


NetSupport RAT: How Legitimate Tools Can Be as Damaging as Malware

 darktrace.com/blog/netsupport-rat-how-legitimate-tools-can-be-as-damaging-as-malware

George Kim

March 10, 2026



March 10, 2026

NetSupport RAT is the malicious abuse of the legitimate NetSupport Manager remote administration tool. Originally designed for IT support, threat actors exploit it to gain unauthorized system access, exfiltrate data, and deploy malware or info-stealers, turning trusted functionality into a dangerous attack vector.

What is NetSupport Manager?

NetSupport Manager is a legitimate IT tool used by system administrators for remote support, monitoring, and management. In use since 1989, NetSupport Manager enables users to remotely access and navigate systems across different platforms and operating systems [1].

What is NetSupport RAT?

Although NetSupport Manager is a legitimate tool that can be used by IT and security professionals, there has been a rising number of cases in which it is abused to gain unauthorized access to victim systems. This misuse has become so prevalent that, in recent years, security researchers have begun referring to NetSupport as a [Remote Access Trojan \(RAT\)](#), a term typically used for malware that enables a threat actor to remotely access or control an infected device [2][3][4].

NetSupport RAT activity summary

The initial stages of NetSupport RAT infection may vary depending on the source of the initial compromise. Using tactics such as the social engineering tactic [ClickFix](#), threat actors attempt to trick users into inadvertently executing malicious PowerShell commands under the guise of resolving a non-existent issue or completing a fake CAPTCHA verification [5]. Other attack vectors such as [phishing emails](#), fake browser updates, malicious websites, search engine optimization (SEO) poisoning, malvertising and drive-by downloads are also employed to direct users to fraudulent pages and fake reCAPTCHA verification checks, ultimately inducing them to execute malicious PowerShell commands [5][6][7]. This leads to the successful installation of NetSupport Manager on the compromised device, which is often placed in non-standard directories such as AppData, ProgramData, or Downloads [3][8].

Once installed, the adversary is able to gain remote access to the affected machine, monitor user activity, exfiltrate data, communicate with the command-and-control (C2) server, and maintain persistence [5]. External research has also highlighted that post-exploitation of NetSupport RAT has involved the additional download of malicious payloads [2][5].

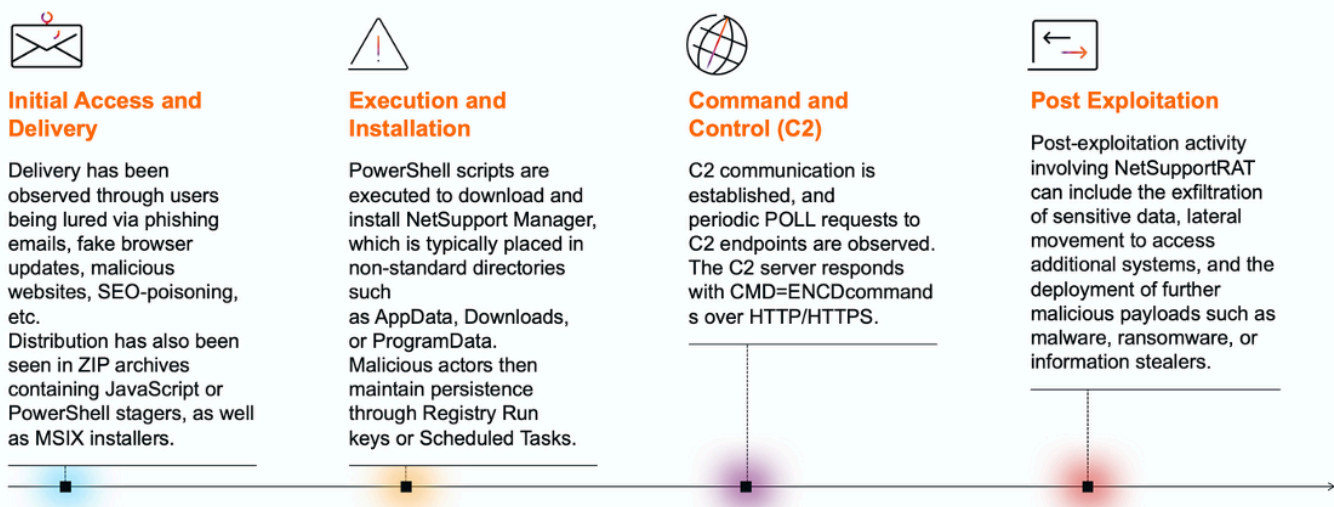


Figure 1: Attack flow diagram highlighting key events across each phase of the attack phase [2][5].

Darktrace coverage

In November of 2025, suspicious behavior indicative of the malicious abuse of NetSupport Manager was observed on multiple customers across Europe, the Middle East, and Africa (EMEA) and the Americas (AMS).

While open-source intelligence (OSINT) has reported that, in a recent campaign, a threat actor impersonated government entities to trick users in organizations in the **Information Technology**, **Government** and **Financial Services** sectors in **Central Asia** into downloading NetSupport

Manager [8], approximately a third of Darktrace's affected customers in November were based in the **US** while the rest were based in **EMEA**. This contrast underscores how widely NetSupport Manager is leveraged by threat actors and highlights its accessibility as an initial access tool.

The Darktrace customers affected were in sectors **including Information and Communication, Manufacturing** and Arts, entertainment and recreation.

The ClickFix [social engineering](#) tactic typically used to distribute the NetSupport RAT is known to target multiple industries, including Technology, Manufacturing and Energy sectors [9]. It also reflects activity observed in the campaign targeting Central Asia, where the Information Technology sector was among those affected [8].

The prevalence of affected Education customers highlights NetSupport's marketing focus on the Education sector [10]. This suggests that threat actors are also aware of this marketing strategy and have exploited the trust it creates to deploy NetSupport Manager and gain access to their targets' systems. While the execution of the PowerShell commands that led to the installation of NetSupport Manager falls outside of Darktrace's purview in cases identified, Darktrace was still able to identify a pattern of devices making connections to multiple rare external domains and IP addresses associated with the NetSupport RAT, using a wide range of ports over the HTTP protocol. **A full list of associated domains and IP addresses is provided in the Appendices of this blog.**

Although OSINT identifies multiple malicious domains and IP addresses as used as C2 servers, signature-based detections of NetSupport RAT indicators of compromise (IoCs) may miss broader activity, as new malicious websites linked to the RAT continue to appear.

Darktrace's anomaly-based approach allows it to establish a normal 'pattern of life' for each device on a network and identify when behavior deviates from this baseline, enabling the detection of unusual activity even when it does not match known IoCs or tactics, techniques and procedures (TTPs).

In one customer environment in late 2025, [Darktrace / NETWORK](#) detected a device initiating new connections to the rare external endpoint, thevaluemetrics[.]com (74.91.125[.]57), along with the use of a previously unseen user agent, which it recognized as highly unusual for the network.

Figure 2: Darktrace's detection of HTTP POST requests to a suspicious URI and new user agent usage.

Darktrace identified that user agent present in connections to this endpoint was the '**NetSupport Manager/1.3**', initially suggesting legitimate NetSupport Manager activity. Subsequent investigation, however, revealed that the endpoint was in fact a malicious NetSupportRAT C2 endpoint [12]. Shortly after, Darktrace detected the same device performing HTTP POST requests to the URI **fakeurl[.]htm**. This pattern of activity is consistent with OSINT reporting that details communication between compromised devices and NetSupport Connectivity Gateways functioning as C2 servers [11].

Conclusion

As seen not only with NetSupport Manager but with any legitimate or open-source software used by IT and security professionals, the legitimacy of a tool does not prevent it from being abused by threat actors. Open-source software, especially tools with free or trial versions such as NetSupport Manager, remains readily accessible for malicious use, including network compromise. In an age where remote work is still prevalent, validating any anomalous use of software and remote management tools is essential to reducing opportunities for unauthorized access.

Darktrace's anomaly-based detection enables security teams to identify malicious use of legitimate tools, even when clear signatures or indicators of compromise are absent, helping to prevent further impact on a network.

Credit to George Kim (Analyst Consulting Lead – AMS), Anna Gilbertson (Senior Cyber Analyst)

Edited by Ryan Traill (Analyst Content Lead)

Appendices

Darktrace Model Alerts

- Compromise / Suspicious HTTP and Anomalous Activity
- Compromise / New User Agent and POST
- Device / New User Agent
- Anomalous Connection / New User Agent to IP Without Hostname
- Anomalous Connection / Posting HTTP to IP Without Hostname
- Anomalous Connection / Multiple Failed Connections to Rare Endpoint
- Anomalous Connection / Application Protocol on Uncommon Port
- Anomalous Connection / Multiple HTTP POSTs to Rare Hostname
- Compromise / Beaconing Activity To External Rare
- Compromise / HTTP Beaconing to Rare Destination
- Compromise / Agent Beacon (Medium Period)
- Compromise / Agent Beacon (Long Period)

- Compromise / Quick and Regular Windows HTTP Beacons
- Compromise / Sustained TCP Beacons Activity To Rare Endpoint
- Compromise / POST and Beacon to Rare External

Indicators of Compromise (IoCs)

Indicator	Type	Description
/fakeurl.htm	URI	NetSupportRAT C2 URI
thetavalumetrics[.]com	Connection hostname	NetSupportRAT C2 Endpoint
westford-systems[.]icu	Connection hostname	NetSupportRAT C2 Endpoint
holonisz[.]com	Connection hostname	NetSupportRAT C2 Endpoint
heaveyduyl[.]com	Connection hostname	NetSupportRAT C2 Endpoint
nsgatetest1[.]digital	Connection hostname	NetSupportRAT C2 Endpoint
finalnovel[.]com	Connection hostname	NetSupportRAT C2 Endpoint
217.91.235[.]17	IP	NetSupportRAT C2 Endpoint
45.94.47[.]224	IP	NetSupportRAT C2 Endpoint
74.91.125[.]57	IP	NetSupportRAT C2 Endpoint
88.214.27[.]48	IP	NetSupportRAT C2 Endpoint
104.21.40[.]75	IP	NetSupportRAT C2 Endpoint
38.146.28[.]242	IP	NetSupportRAT C2 Endpoint
185.39.19[.]233	IP	NetSupportRAT C2 Endpoint
45.88.79[.]237	IP	NetSupportRAT C2 Endpoint
141.98.11[.]224	IP	NetSupportRAT C2 Endpoint
88.214.27[.]166	IP	NetSupportRAT C2 Endpoint
107.158.128[.]84	IP	NetSupportRAT C2 Endpoint
87.120.93[.]98	IP	Rhadamanthys C2 Endpoint

References

1. <https://mispalliance.com/netsupport-debuts-netsupport-24-7/>
2. <https://blogs.vmware.com/security/2023/11/netsupport-rat-the-rat-king-returns.html>
3. <https://redcanary.com/threat-detection-report/threats/netsupport-manager/>
4. <https://www.elastic.co/guide/en/security/8.19/netsupport-manager-execution-from-an-unusual-path.html>
5. <https://rewterz.com/threat-advisory/netsupport-rat-delivered-through-spoofed-verification-pages-active-iocs>
6. <https://thehackernews.com/2025/11/new-evalusion-clickfix-campaign.html>
7. <https://corelight.com/blog/detecting-netsupport-manager-abuse>
8. <https://thehackernews.com/2025/11/bloody-wolf-expands-java-based.html>
9. <https://unit42.paloaltonetworks.com/preventing-clickfix-attack-vector>
10. <https://www.netsupportsoftware.com/education-solutions>
11. <https://www.esentire.com/blog/unpacking-netsupport-rat-loaders-delivered-via-clickfix>
12. https://threatfox.abuse.ch/browse/malware/win.netsupportmanager_rat/
13. <https://www.virustotal.com/gui/url/5fe6936a69c786c9ded9f31ed1242c601cd64e1d90cecd8a7bb03182c47906c2>

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Share this post

Latest blogs



[Inside Cloud Compromise: Investigating Attacker Activity with Darktrace / Forensic Acquisition & Investigation](#)

[Cloud](#)

•

[March 4, 2026](#)

[Nathaniel Bill](#)

[Malware Research Engineer](#)



[What the Darktrace Annual Threat Report 2026 Means for Security Leaders](#)

[AI](#)

[•](#)

[February 26, 2026](#)

[Mike Beck](#)

[Global CISO](#)