Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

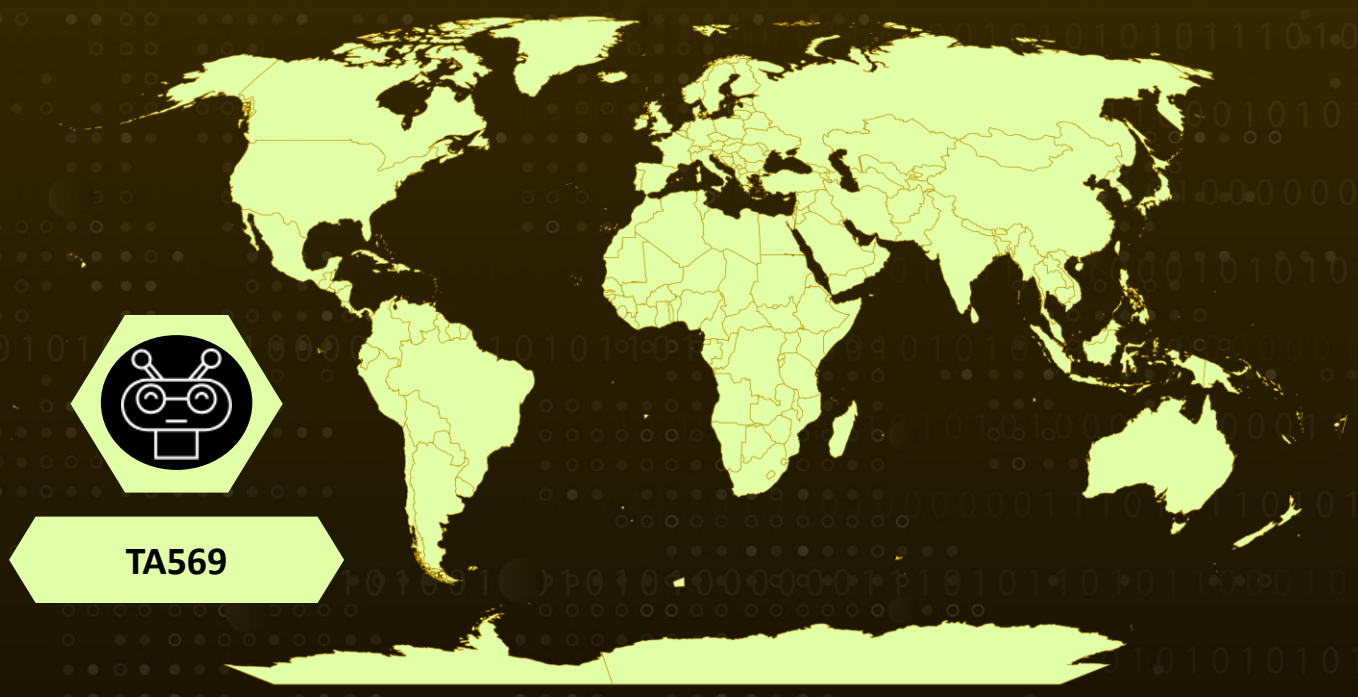
The Rise of NetSupport RAT Recent Infections and Sector Impact

Date of Publication	Admiralty Code	TA Number
November 21, 2023	A1	TA2023469

Summary

First appeared: 2017
Attack Region: Worldwide
Threat Actor: TA569
Malware: NetSupport RAT
Targted Industries: Education, Government, and Business Services
Attack: Threat actors exploit NetSupport Manager into a Remote Access Trojan (RAT), leading to a recent surge in infections across multiple sectors. The evolving attack chain involves deceptive website downloads, JavaScript payloads, and PowerShell commands, emphasizing the need for vigilant detection and response measures.

Attack Regions



Attack Details

#1

In recent years, threat actors have repurposed the legitimate NetSupport Manager software, originally designed for remote systems management, into a Remote Access Trojan (RAT) to infiltrate systems and serve as a launchpad for subsequent attacks. Researchers have observed a notable increase, with over 15 new infections related to NetSupport RAT identified in recent weeks, predominantly affecting the Education, Government, and Business Services sectors.

#2

NetSupport Manager, initially developed for remote technical support, has been exploited due to its widespread availability and legitimate nature. Various malicious entities, including TA569, have incorporated this tool into their arsenals, making it susceptible to use by a spectrum of threat actors.

#3

The history of NetSupport Manager reveals its transformation from a legitimate tool to a RAT, notably used in the 2020 COVID-19 phishing campaign. The delivery mechanisms for NetSupport RAT include fraudulent updates, drive-by downloads, malware loaders like GhostPulse, and diverse phishing campaigns. Unlike older variants, recent NetSupport RAT iterations deviate from using older methods like .BAT and .VBS files.

#4

The attack chain involves victims being deceived into downloading a fake browser update from compromised websites. A JavaScript payload, such as Update_browser_10.6336.js, connects to external servers, invokes PowerShell for executing obfuscated commands, and establishes persistence on victim devices. Once installed, NetSupport RAT enables threat actors to monitor behavior, transfer files, manipulate settings, and move laterally within networks.

Recommendations

Regular Software Audits: Conduct regular audits of installed software to identify and remove any unauthorized or unnecessary applications. This includes scrutinizing remote management tools like NetSupport Manager to ensure they are used legitimately.

Enhanced Cybersecurity Measures: Implement robust cybersecurity measures, including up-to-date antivirus software, firewalls, intrusion detection systems, and secure network configurations. Regular security updates and patches for all software and operating systems should be applied promptly to mitigate vulnerabilities.

Endpoint Security: Deploy robust endpoint security solutions that include advanced threat detection capabilities. Ensure these solutions are regularly updated to recognize and mitigate emerging threats, such as new variants of NetSupport RAT.

Monitoring and Threat Detection: Employ advanced threat detection tools and continuously monitor networks for unusual or suspicious activities. This includes monitoring network traffic for any communication with domains resembling legitimate sites and identifying potentially malicious payloads.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0001 Initial Access	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0002 Execution	TA0003 Persistence
T1566 Phishing	T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.007 JavaScript	T1055 Process Injection	T1027 Obfuscated Files or Information

T1041 Exfiltration Over C2 Channel	T1074.001 Local Data Staging	T1074 Data Staged	T1547.001 Registry Run Keys / Startup Folder
T1547 Boot or Logon Autostart Execution	T1057 Process Discovery	T1566.002 Spearphishing Link	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	104b30fef04433a2d2fd1d5f99f179fe, 1b41e64c60ca9dfadeb063cd822ab089, 252dce576f9fbb9aaa7114dd7150f320, 34dfb87e4200d852d1fb45dc48f93cfc, 6fca49b85aa38ee016e39e14b9f9d6d9, a2b46c59f6e7e395d479b09464ecdba0, c94005d2dcd2a54e40510344e0bb9435, d3d39180e85700f72aaae25e40c125ff, eab603d12705752e3d268d86dff74ed4, f70b67c2b3204b7ddd8b755799cccff0, f838fdafd0881cf1e6040a07d78e840d
SHA1	01873977c871d3346d795cf7e3888685de9f0b16, 2a35456b2f67bd12905378beb6eaf373f6a0d0d1, 35b4e73fb7c8d4c3fefb90b7e7dc19f3e653c641, 55b4a1620c5d0113811242c20bd9870a1e31d542, 92c132307dd21189b6d7912ddd934b50e50d1ec1, a42e55e328d62d11e687c167bb7049d46f0f9b26, abfcd51bb120a7eae5bbd9a99624e4abe0c9139d, b0d689c70e91d5600ccc2a4e533ff89bf4ca388b, c07f0a02c284b697dff119839f455836be39d10e, ecb08e224a2f2772d1e53675bedc4b2c50485a41, f3404ef6322f5c6e7862b507d05b8f4b7f1c7d15
IPv4	5.252.177[.]111, 91.19.150[.]63, 91.219.150[.]64

TYPE	VALUE
SHA256	213af995d4142854b81af3cf73dee7ffe9d8ad6e84fda6386029101dbf3df897, 28208baa507b260c2df6637427de82ad0423c20e2bceceb92ba5d76074dcd347, 2d6c6200508c0797e6542b195c999f3485c4ef76551aa3c65016587788ba1703, 2e4bd5557aedd1743da5fab1b6995fbc447d6e9491d9ec59fa93ab889d8bccd1, 38684adb2183bf320eb308a96cdbde8d1d56740166c3e2596161f42a40fa32d5, 3c072532bf7674d0c5154d4d22a9d9c0173530c0d00f69911cdbc2552175d899, 46bb795f28ef33412b83542c88ef17d2a2a207ad3a927ecb4678b4ac9c5a05a5, 4bfa4c00414660ba44bddde5216a7f28aeccaa9e2d42df4bbff66db57c60522b, 54b920f5b87019fcf313bec4d9f4639a932b8268e5183b29804e91e29ed6f726, 60fe386112ad51f40a1ee9e1b15eca802ced174d7055341c491dee06780b3f92, 6795d760ce7a955df6c2f5a062e296128efdb8c908908eda4d666926980447ea, 89f0c8f170fe9ea28b1056517160e92e2d7d4e8aa81f4ed696932230413a6ce1, 8c9cd7a1ac6d4cbc641b31a3c55fde5e0e5a48c9bdaf71a59a2c4c9fd98ff9e7, 956b9fa960f913cce3137089c601f3c64cc24c54614b02bba62abb9610a985dd, b6b51f4273420c24ea7dc13ef4cc7615262ccbdf6f5e5a49dae604ec153055ad, c5c974b3315602ffaab9066aeaac3a55510db469b483cb85f6c591e948d16cfe, d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368, e3665d8c5030be81a6955965c2928564fe922b9a21f9e712580d04825fa0adf1, f4e2f28169e0c88b2551b6f1d63f8ba513feb15beacc43a82f626b93d673f56d, fc6f9dbdf4b9f8dd1f5f3a74cb6e55119d3fe2c9db52436e10ba07842e6c3d7c, fedd609a16c717db9bea3072bed41e79b564c4bc97f959208bfa52fb3c9fa814

TYPE	VALUE
URLs	hxxps://gameflix[.]com/111, hxxps://gamefllix[.]com/111[.]php, hxxps://gamefllix[.]com/111[.]php?9279, hxxps://sdjfnvnbbz[.]pw:443, hxxps://gamefllix[.]com/111[.]php[?]9279, hxxps://magydostravel[.]com/cdn/zwmrqqgqnaww[.]php
Domains	arauas[.]com, gameflix[.]com, gamefllix[.]com, implacavelvideos[.]com, kgscrew[.]com, magydostravel[.]com, sdjfnvnbbz[.]pw

References

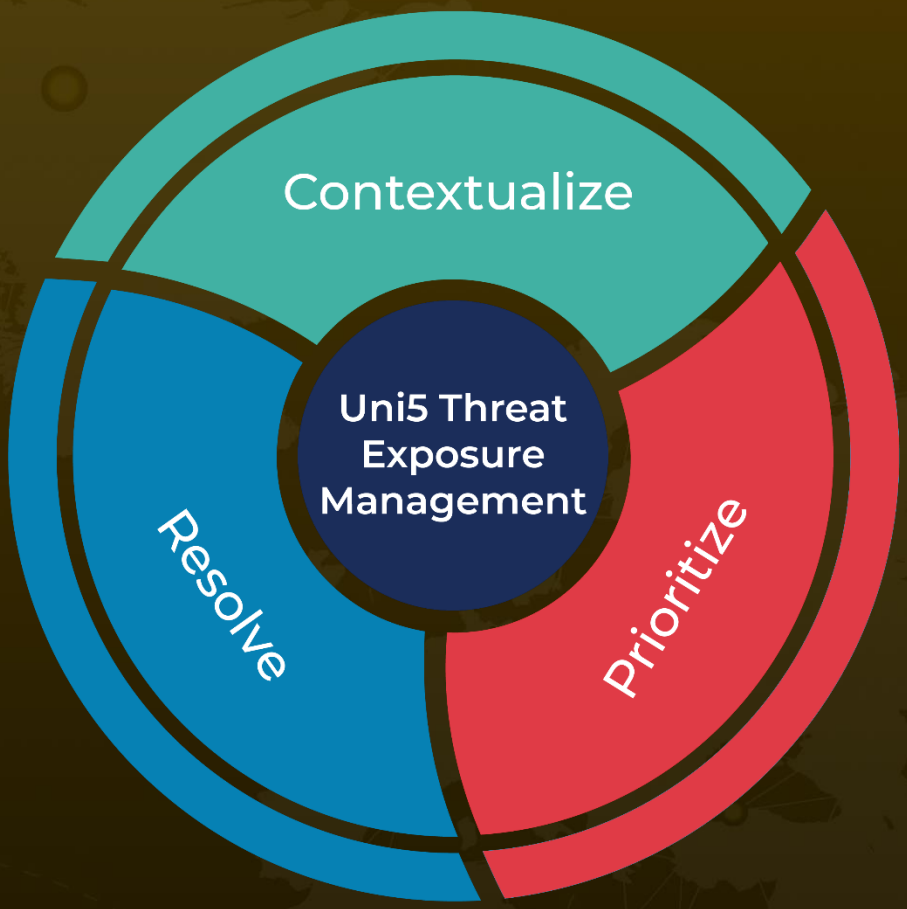
https://blogs.vmware.com/security/2023/11/netsupport-rat-the-rat-king-returns.html

https://www.hivepro.com/threat-advisory/netsupport-rat-employs-phishing-campaigns-that-incorporate-pokemon-lures/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2023 . 4:30 AM

More at www.hivepro.com