Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

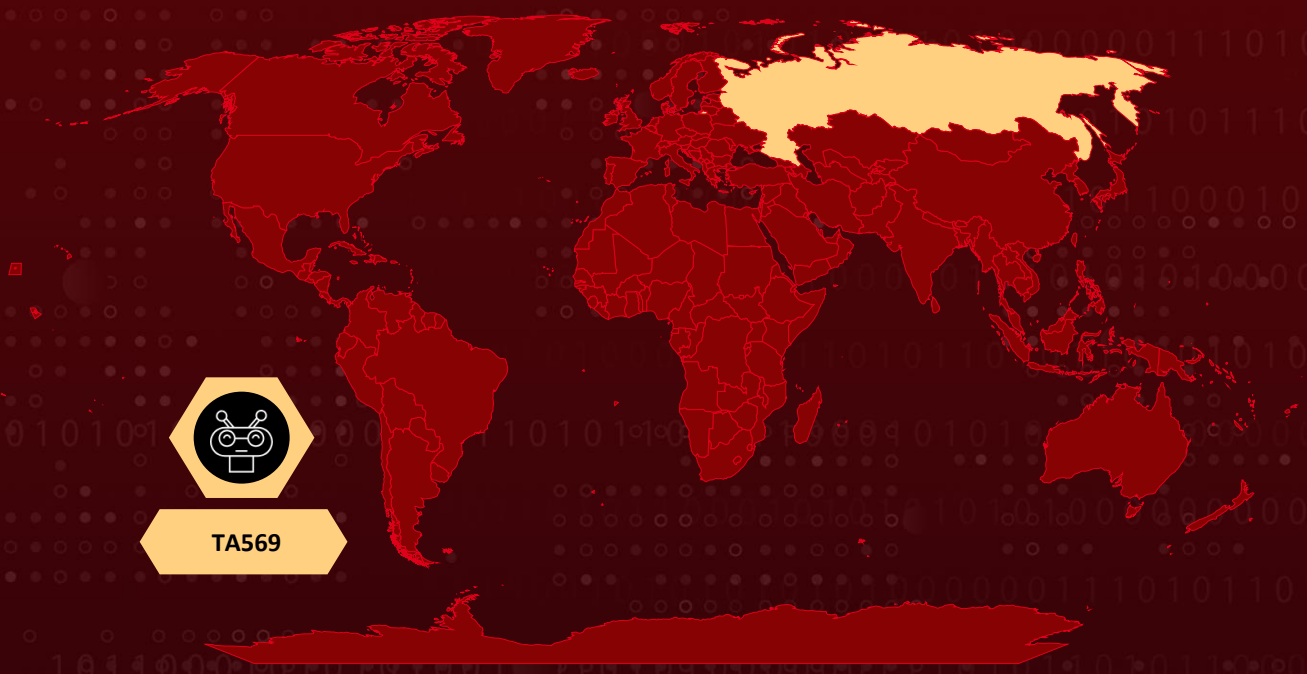
NetSupport RAT Exploited in Horns&Hooves Cyberattack

Date of Publication	Admiralty Code	TA Number
December 4, 2024	A1	TA2024450

Summary

Attack Began: March 2023
Malware: NetSupport RAT, BurnsRAT
Targeted Region: Russia
Targeted Industries: Retailers, Service Businesses, Private Users
Campaign Name: Horns&Hooves
Affected Platform: Windows
Threat Actor: TA569
Attack: The Horns&Hooves campaign, active since March 2023, targets Russian users by delivering malware disguised as legitimate business documents. Utilizing malicious JScript files, attackers aim to install the NetSupport RAT (Remote Access Trojan) on victims' systems. The campaign has evolved from HTA scripts to more sophisticated obfuscated JavaScript files to evade detection. Connections to other cybercriminal groups, particularly TA569, highlight the collaborative nature of these threats and the need for ongoing vigilance in cybersecurity.

Attack Regions



Attack Details

#1 The Horns&Hooves campaign, active since March 2023, is a cyberattack targeting primarily Russian users, retailers, and service businesses through malicious emails. These emails, disguised as legitimate business inquiries, contain ZIP archives with JScript (JS) scripts masquerading as requests for proposals, price quotes, or claims.

#2 Initially, these scripts used the HTA format before switching to JS, and their contents often included decoy documents like fake PDFs or Russian registry extracts to enhance believability. Over time, the scripts evolved to obfuscate their true nature further, embedding malicious payloads within the ZIP files or script code itself.

#3 The malware payload is primarily NetSupport RAT, a legitimate remote administration tool exploited by attackers for unauthorized control over victims' systems. The installation process involves downloading a decoy document to distract users while using Windows utilities like curl and bitsadmin to install the RAT.

#4 Additional tools, such as BurnsRAT and RMS, were briefly employed in earlier campaign phases but were later abandoned in favor of streamlined approaches. These payloads provided attackers remote access, enabling the theft of sensitive data, installation of other malware like Rhadamanthys and Meduza stealers, or resale of system access on the dark web.

#5 Attribution of the Horns&Hooves campaign points to the TA569 group, also known as Mustard Tempest or Gold Prelude, known for selling access to compromised systems. Evidence includes the reuse of license files, configuration file similarities, and shared security keys for the NetSupport client.

#6 TA569 typically leverages compromised access for ransomware deployment or data theft, but it also facilitates secondary cybercrime activities by selling access to other threat actors. The campaign underscores the risks posed by abused legitimate tools and highlights the importance of robust defenses against social engineering tactics and script-based malware.

Recommendations

Enhance Email Security: Organizations should implement advanced email filtering solutions to detect and quarantine emails with suspicious attachments, especially ZIP archives containing JavaScript or HTA files. Additionally, businesses should educate employees to identify phishing attempts by providing training on recognizing unusual requests or unsolicited proposals.

Strengthen Endpoint Protection: Deploying endpoint detection and response (EDR) solutions is essential for monitoring suspicious activities. These tools can block malicious scripts before they execute. Antivirus programs should be updated regularly to detect and neutralize emerging threats, including malware disguised as legitimate business communications.

Limit Execution of Untrusted Scripts: Restrict the execution of scripts from unknown or untrusted sources. IT administrators can enforce policies that prevent JavaScript, HTA, or other executable files from running unless explicitly approved. For additional security, consider disabling Windows utilities like bitsadmin and PowerShell on non-administrative machines.

Implement Network Monitoring: Network monitoring tools can detect anomalies, such as unexpected connections to command-and-control servers. By identifying these connections, organizations can quickly isolate affected systems to prevent further compromise. Regular audits of network traffic should be conducted to ensure no unauthorized activities occur.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0001 Initial Access	TA0042 Resource Development	TA0002 Execution	TA0009 Collection
T1059 Command and Scripting Interpreter	T1566.001 Spearphishing Attachment	T1566 Phishing	T1218.005 Mshta
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1041 Exfiltration Over C2 Channel	T1584 Compromise Infrastructure

T1059.007 JavaScript	T1059.001 PowerShell	T1059.005 Visual Basic	T1036 Masquerading
T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information	T1204 User Execution	T1204.002 Malicious File
T1123 Audio Capture	T1218 System Binary Proxy Execution	T1059.003 Windows Command Shell	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcdb6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7, 5f4284115ab9641f1532bb64b650aad6, 0fea857a35b972899e8f1f60ee58e450, 20014b80a139ed256621b9c0ac4d7076, 7f0ee078c8902f12d6d9e300dabf6aed, 63647520b36144e31fb8ad7dd10e3d21, 8096e00aa7877b863ef5a437f55c8277, 12ab1bc0989b32c55743df9b8c46af5a, 50dc5faa02227c0aefa8b54c8e5b2b0d, e760a5ce807c756451072376f88760d7, b03c67239e1e774077995bac331a8950, ba69cc9f087411995c64ca0d96da7b69, 051552b4da740a3af5bd5643b1dc239a, edfb8d26fa34436f2e92d5be1cb5901b, 3e86f6fc7ed037f3c9560cc59aa7aacc, ae4d6812f5638d95a82b3fa3d4f92861, 67677c815070ca2e3ebd57a6adb58d2e, 17a78f50e32679f228c43823faabedfd, b9956282a0fed076ed083892e498ac69, 1b41e64c60ca9dfadeb063cd822ab089

TYPE	VALUE
Domains	xoomep1[.]com, xoomep2[.]com, labudanka1[.]com, labudanka2[.]com, gribidi1[.]com, gribidi2[.]com, shetrn1[.]com, shetrn2[.]com
URLs	hxxp://193[.]42[.]32[.]138/api/, hxxp://87[.]251[.]67[.]51/api/, hxxp://31[.]44[.]4[.]40/test/bat_install.bat, hxxps://golden-scalen[.]com/files/*, hxxp://188[.]227[.]58[.]243/pretencia/www.php, hxxp://188[.]227[.]58[.]243/zayavka/www.php, hxxp://188[.]227[.]58[.]243/pretencia/installet_bat_vbs.bat, hxxp://188[.]227[.]106[.]124/test/js/www.php, hxxp://188[.]227[.]106[.]124/test/js/BLD.exe, hxxp://188[.]227[.]106[.]124/test/js/1.js, hxxp://45[.]133[.]16[.]135/zayavka/www.php, hxxp://45[.]133[.]16[.]135/zayavka/666.bat, hxxp://45[.]133[.]16[.]135/zayavka/1.yay, hxxp://golden-scalen[.]com/ngg_cl.zip

References

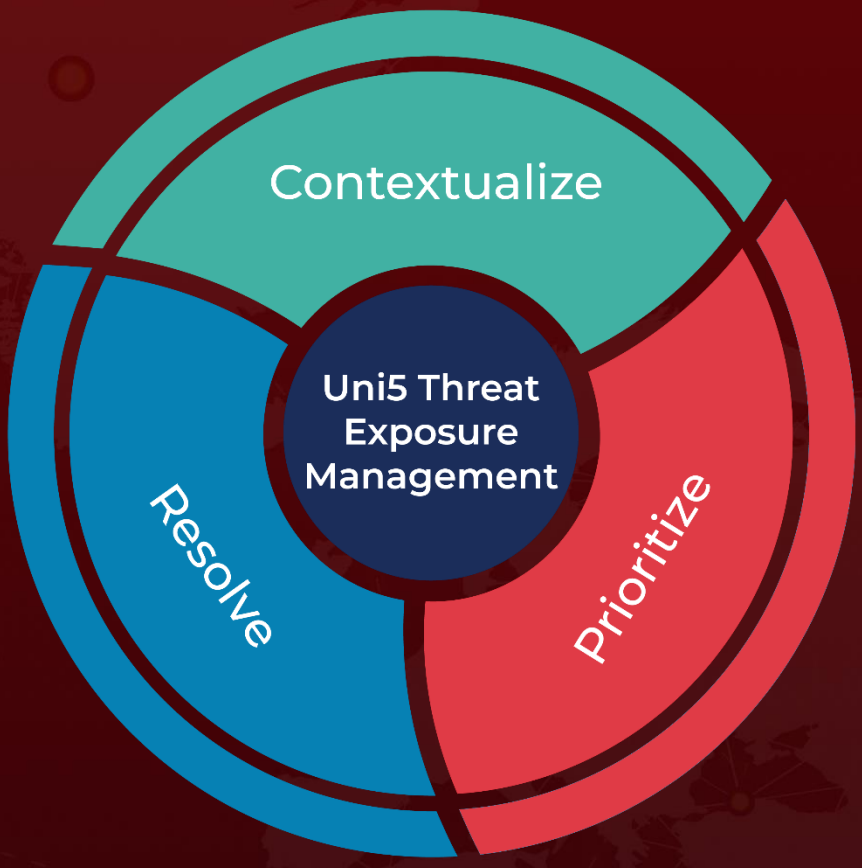
https://securelist.com/horns-n-hooves-campaign-delivering-netsupport-rat/114740/

https://www.hivepro.com/threat-advisory/the-rise-of-netsupport-rat-recent-infections-and-sector-impact/

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

December 4, 2024 . 6:30 AM

More at www.hivepro.com