

HiveForce Labs

THREAT ADVISORY

**ACTOR REPORT**

Magnet Goblin Strikes Public-Facing Servers

Date of Publication

March 15, 2024

Admiralty code

A1

TA Number

TA2024102

Summary

First Appearance: September 2023

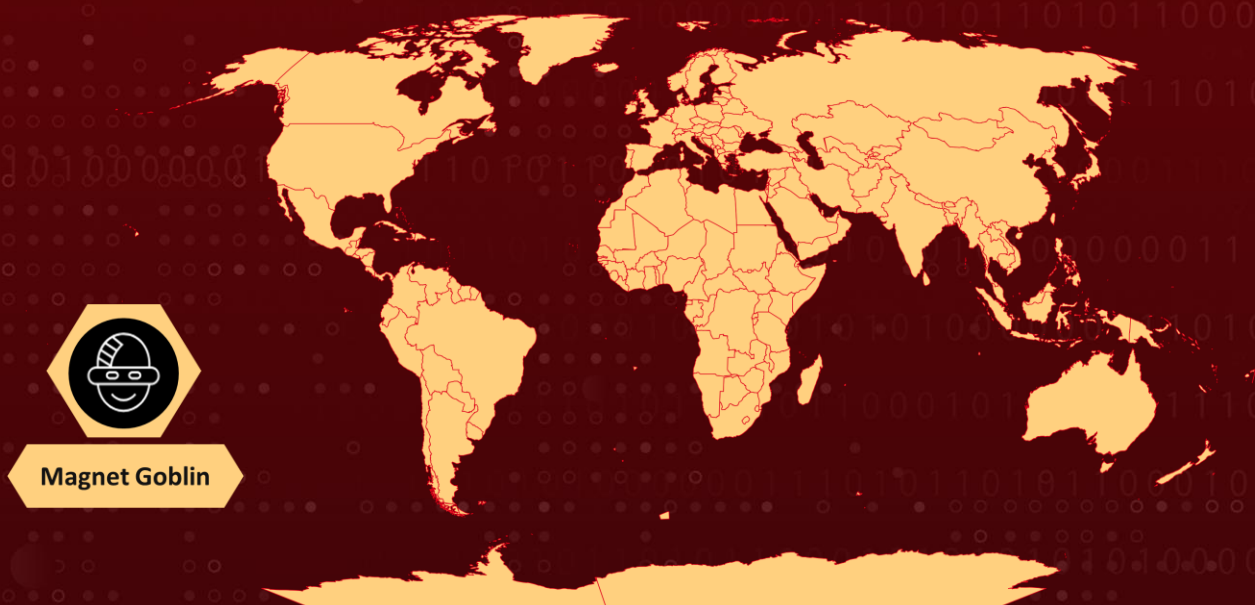
Threat Actor: Magnet Goblin

Malware: NerbianRAT, WARPWIRE, MiniNerbian

Affected Products: Ivanti, Magento, Qlink Sense, and Apache ActiveMQ




Target Region: Worldwide

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2022-24086	Adobe Commerce and Magento Open-Source Improper Input Validation Vulnerability	Adobe Commerce and Magento Open Source	✓	✓	✓
CVE-2023-41265	Qlik Sense Enterprise Privilege escalation Vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-41266	Qlik Sense Enterprise path traversal Vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-48365	Qlik Sense Enterprise remote code execution Vulnerability	Qlik Sense Enterprise for Windows	✗	✗	✓
CVE-2024-21888	Ivanti Privilege Escalation Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	✗	✗	✓
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	✓	✓	✓

Actor Details

#1

Magnet Goblin embodies a financially motivated threat entity that exploits zero-day vulnerabilities in publicly accessible services as its primary means of infiltration. This malicious actor utilizes malware derived from a bespoke family known as Nerbian.

#2

Within this lineage, NerbianRAT stands as a versatile remote access trojan (RAT), customized for both Windows and Linux environments, accompanied by MiniNerbian, a compact yet potent Linux-based backdoor. Originating in 2022, Magnet Goblin initiated its operations by capitalizing on the CVE-2022-24086 vulnerability within Magento servers.

#3

Subsequently, the group expanded its reach by targeting weaknesses in Qlik Sense and Ivanti Connect Secure VPN devices, thereby implanting malware into compromised systems. Upon successful exploitation, Magnet Goblin deploys its signature cross-platform RAT, Nerbian RAT, which offers a variety of variants tailored for different operating systems, alongside MiniNerbian, a streamlined Linux backdoor.

#4

The latter represents a simplified version of NerbianRAT, primarily designed for executing commands, with evident shared coding elements between the two. Diversifying its arsenal, the threat actor introduces a customized version of WARPWIRE, a JavaScript-based credential theft tool, alongside MiniNerbian, enhancing its toolkit with additional Linux-specific capabilities.

#5

This group exhibits agility in exploiting zero-day vulnerabilities to disseminate their customized Linux-based malware, often operating surreptitiously within edge device environments. Magnet Goblin distinguishes itself through its swift exploitation of emerging vulnerabilities, with malware developed within a mere day following the publication of proof-of-concept (PoC) exploits, thus solidifying its position as a formidable entity within the cybersecurity landscape.

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Magnet Goblin	-	Worldwide	All
	MOTIVE		
	Financial Gains		

Recommendations



Patch and Update Vulnerable Software: Regularly update and patch all software and systems, particularly addressing known vulnerabilities. Ensure your software remains up to date by regularly checking for and applying the latest security updates and patches from the vendor patches can help prevent exploitation by threat actors like Magnet Goblin.



Enhance Network Monitoring: Invest in robust network monitoring and intrusion detection systems to quickly detect and respond to suspicious activities. Early detection can mitigate the damage caused by potential breaches.



Harden Server Configurations: Apply server hardening techniques to reduce the attack surface by disabling unnecessary services, closing unused ports, and following industry best practices for server security.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery

<u>TA0009</u> Collection	<u>TA0011</u> Command and Control	<u>TA0010</u> Exfiltration	<u>T1041</u> Exfiltration Over C2 Channel
<u>T1190</u> Exploit Public-Facing Application	<u>T1059.007</u> JavaScript	<u>T1059</u> Command and Scripting Interpreter	<u>T1027</u> Obfuscated Files or Information
<u>T1573.001</u> Symmetric Cryptography	<u>T1071.001</u> Web Protocols	<u>T1573</u> Encrypted Channel	<u>T1071</u> Application Layer Protocol
<u>T1588.006</u> Vulnerabilities	<u>T1588.001</u> Malware	<u>T1105</u> Ingress Tool Transfer	

✂ Indicator of Compromise (IOCs)

TYPE	VALUE
IPv4	91[.]92[.]240[.]113, 45[.]9[.]149[.]215, 94[.]156[.]71[.]115, 172[.]86[.]66[.]165, 45[.]153[.]240[.]73
URLs	hxxp[:]//[91.92.240[.]113/auth.js, hxxp[:]//[91.92.240[.]113/login.cgi, hxxp[:]//[91.92.240[.]113/aparche2, hxxp[:]//[91.92.240[.]113/agent, hxxp[:]//[45.9.149[.]215/aparche2, hxxp[:]//[45.9.149[.]215/agent, hxxp[:]//[94.156.71[.]115/lxrt, hxxp[:]//[94.156.71[.]115/agent, hxxp[:]//[94.156.71[.]115/instali.ps1, hxxp[:]//[94.156.71[.]115/ligocert.dat, hxxp[:]//[94.156.71[.]115/angel.dat, hxxp[:]//[94.156.71[.]115/windows.xml, hxxp[:]//[94.156.71[.]115/instal1.ps1, hxxp[:]//[94.156.71[.]115/Maintenance.ps1, hxxp[:]//[94.156.71[.]115/baba.dat, hxxp[:]//[oncloud-analytics[.]com/files/mg/elf/RT1.50.png, hxxp[:]//[cloudflareaddons[.]com/assets/img/Image_Slider15.1.png, www.fernandestechnical[.]com/pub/health_check.php, biondocenere[.]com/pub/health_check.php, www.miltonhouse[.]nl/pub/opt/processor.php, hxxps[:]//[theroots[.]in/pub/media/avatar/223sam.jpg

TYPE	VALUE
Domain	mailchimp-addons[.]com, allsecurehosting[.]com, dev-clientservice[.]com, oncloud-analytics[.]com, cloudflareaddons[.]com, textsmsonline[.]com, proreceive[.]com
SHA256	027d03679f7279a2c505f0677568972d30bc27daf43033a463fafee0d7234f6, 9cb6dc863e56316364c7c1e51f74ca991d734dacef9029337ddec5ca684c1106, 9d11c3cf10b20ff5b3e541147f9a965a4e66ed863803c54d93ba8a07c4aa7e50, d3fbae7eb3d38159913c7e9f4c627149df1882b57998c8acaac5904710be2236, df91410df516e2bddfd3f6815b3b4039bf67a76f20aecabccffb152e5d6975ef, 99fd61ba93497214ac56d8a0e65203647a2bc383a2ca2716015b3014a7e0f84d, 9ff0dcce930bb690c897260a0c5aaa928955f4ffba080c580c13a32a48037cf7, 3367a4c8bd2bcd0973f3cb22aa2cb3f90ce2125107f9df2935831419444d5276, f23307f1c286143b974843da20c257901cf4be372ea21d1bb5dea523a7e2785d, f1e7c1fc06bf0ea40986aa20e774d6b85c526c59046c452d98e48fe1e331ee4c, 926aeb3fda8142a6de8bc6c26bc00e32abc603c21acd0f9b572ec0484115bb89, 894ab5d563172787b052f3fea17bf7d51ca8e015b0f873a893af17f47b358efe, 1079e1b6e016b070ebf3e1357fa23313dcb805d3a6805088dbc3ab6d39330548, E134e053a80303d1fde769e50c2557ade0852fa827bed9199e52f67bac0d9efc, 7967def86776f36ab6a663850120c5c70f397dd3834f11ba7a077205d37b117f, 9895286973617a79e2b19f2919190a6ec9afc07a9e87af3557f3d76b252292df, bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e, b35f11d4f54b8941d4f1c5b49101b67b563511a55351e10ad4ede17403529c16, 7b1d1e639d1994c6235d16a7ac583e583687660d7054a2a245dd18f24d10b675,

TYPE	VALUE
SHA256	8fe1ed1e34e8758a92c8d024d73c434665a03e94e5eb972c68dd661c5e252469, fa317b071da64e3ee18d82d3a6a216596f2b4bca5f4d3277a091a137d6a21c45

Patch Details

<https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways>

<https://helpx.adobe.com/security/products/magento/apsb22-12.html>

<https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801>

<https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801>

<https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510>

<https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure>

References

<https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/>

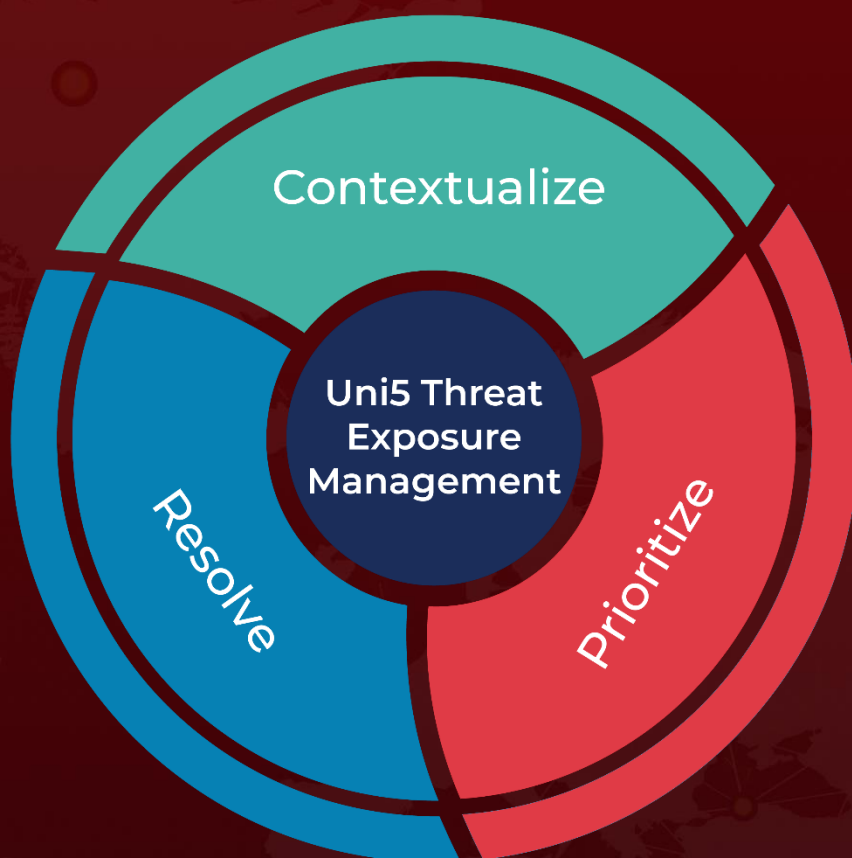
<https://www.hivepro.com/threat-advisory/ivanti-gateways-under-attack-by-cybercriminals-patch-now/>

<https://www.hivepro.com/threat-advisory/cactus-ransomware-exploits-vulnerabilities-in-qlik-sense/>

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

March 15, 2024 • 2:00 AM

© 2024 All Rights are Reserved by HivePro



More at www.hivepro.com