Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

A New RAT Named GobRAT Targeting Linux Routers in Japan

Date of Publication	Admiralty Code	TA Number
May 30, 2023	A1	TA2023249

Summary

First appeared: February, 2023
Attack Region: Japan
Affected Platform: Linux
Malware: GobRAT
Attack: GobRAT, a new RAT, is infecting Linux routers in Japan through vulnerable web interfaces, granting attackers remote control and the ability to execute commands.

Attack Regions

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

Attack Details

#1

In February 2023, there was an attack on routers in Japan that infected them with a type of malicious software called GobRAT. The attackers targeted routers that had their WEBUI (web user interface) accessible to the public. They used scripts to exploit vulnerabilities in these routers and installed the GobRAT malware.

#2

GobRAT disguises itself as the Apache daemon process to avoid detection. The malware communicates with a remote server using TLS and can execute up to 22 different encrypted commands, including obtaining machine information, executing reverse shells, and configuring new command-and-control settings.

#3

The attackers used a special script called the Loader Script to download and execute GobRAT on the infected routers. This script had functions like disabling the firewall and creating a persistent connection to ensure the malware would continue running. The GobRAT malware itself was designed to look like a legitimate process called "apached" It communicated with a central command-and-control (C2) server using a secure connection called TLS.

#4

GobRAT had various commands it could execute on the infected routers. These commands allowed the attackers to gather information about the routers, manipulate files, and configure communication settings. The malware used encryption to protect its communication with the C2 server. By decrypting the encrypted strings, security experts were able to analyze the commands and understand what the attackers were trying to do.

Recommendations

Secure Configuration: Implement secure configurations on routers, including strong passwords, disabling unnecessary services, and keeping firmware up to date. Additionally, employ specific measures to detect and prevent GobRAT attacks, such as monitoring for suspicious communication with GobRAT C2 servers and identifying GobRAT-specific indicators of compromise.

Network Segmentation: Utilize network segmentation to isolate routers from the rest of the network, limiting the potential impact of a GobRAT infection. Apply access control measures to restrict communication to and from routers, reducing the attack surface. Consider implementing intrusion prevention systems (IPS) that can detect and block GobRAT-related traffic.

Ongoing Monitoring and Intrusion Detection: Deploy robust monitoring and intrusion detection systems to detect GobRAT activity and indicators of compromise. Monitor network traffic, logs, and behavior patterns for signs of GobRAT infections, such as communication with known GobRAT C2 servers or abnormal command execution. Implement real-time alerting and response mechanisms to address identified threats promptly.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0008 Lateral Movement
TA0042 Resource Development	T1132.001 Standard Encoding	T1090 Proxy	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1021 Remote Services	T1059 Command and Scripting Interpreter
T1021.004 SSH	T1543 Create or Modify System Process	T1543.004 Launch Daemon	T1562 Impair Defenses
T1562.004 Disable or Modify System Firewall	T1083 File and Directory Discovery	T1027 Obfuscated Files or Information	T1132 Data Encoding
T1140 Deobfuscate/Decode Files or Information	T1041 Exfiltration Over C&C Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	https[:]//su.vealcat[.]com http[:]//su.vealcat[.]com:58888 https[:]//ktlvz.dnsfailover[.]net http[:]//ktlvz.dnsfailover[.]net:58888
Domains	su.vealcat[.]com ktlvz.dnsfailover[.]net wpksi.mefound[.]com
SHA256	060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a 3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1 60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3 a8b914df166fd0c94106f004e8ca0ca80a36c6f2623f87a4e9afe7d86b5b2e3a aeed77896de38802b85a19bfcb8f2a1d567538ddc1b045bcdb29cb9e05919b60 6748c22d76b8803e2deb3dad1e1fa7a8d8ff1e968eb340311fd82ea5d7277019 e133e05d6941ef1c2e3281f1abb837c3e152fdeaffefde84ffe25338fe02c56d 43dc911a2e396791dc5a0f8996ae77ac527add02118adf66ac5c56291269527e af0292e4de92032ede613dc69373de7f5a182d9cbba1ed49f589ef484ad1ee3e 2c1566a2e03c63b67fbdd80b4a67535e9ed969ea3e3013f0ba503cfa58e287e3 98c05ae70e69e3585fc026e67b356421f0b3d6ab45b45e8cc5eb35f16fef130c 300a92a67940cfafeed1cf1c0af25f4869598ae58e615ecc559434111ab717cd a363dea1efda1991d6c10cc637e3ab7d8e4af4bd2d3938036f03633a2cb20e88 0c280f0b7c16c0d299e306d2c97b0bff3015352d2b3299cf485de189782a4e25 f962b594a847f47473488a2b860094da45190738f2825d82afc308b2a250b5fb 4ceb27da700807be6aa3221022ef59ce6e9f1cda52838ae716746c1bbdee7c3d

TYPE	VALUE
SHA256	3e1a03f1dd10c3e050b5f455f37e946c214762ed9516996418d34a246daed521 3bee59d74c24ef33351dc31ba697b99d41c8898685d143cd48bccdff707547c0 c71ff7514c8b7c448a8c1982308aaffed94f435a65c9fdc8f0249a13095f665e

References

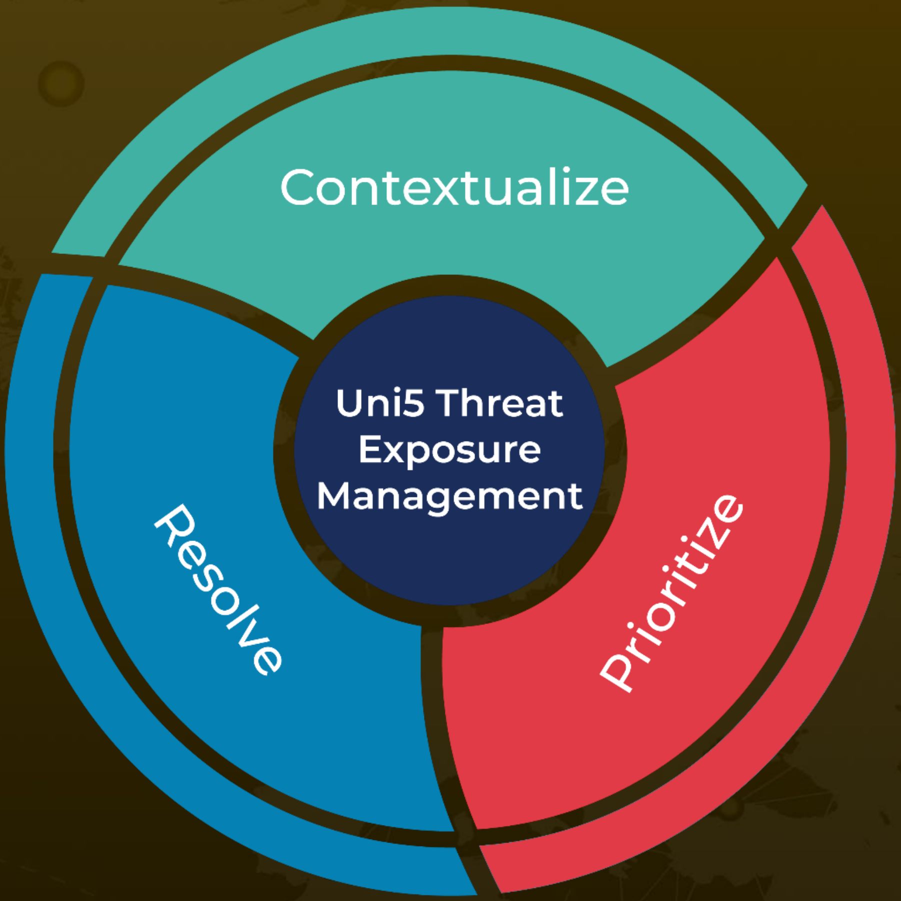
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

https://securityaffairs.com/146795/malware/gobrat-targets-routers-japan.html

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

May 30, 2023 • 3:30 AM

More at www.hivepro.com