Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

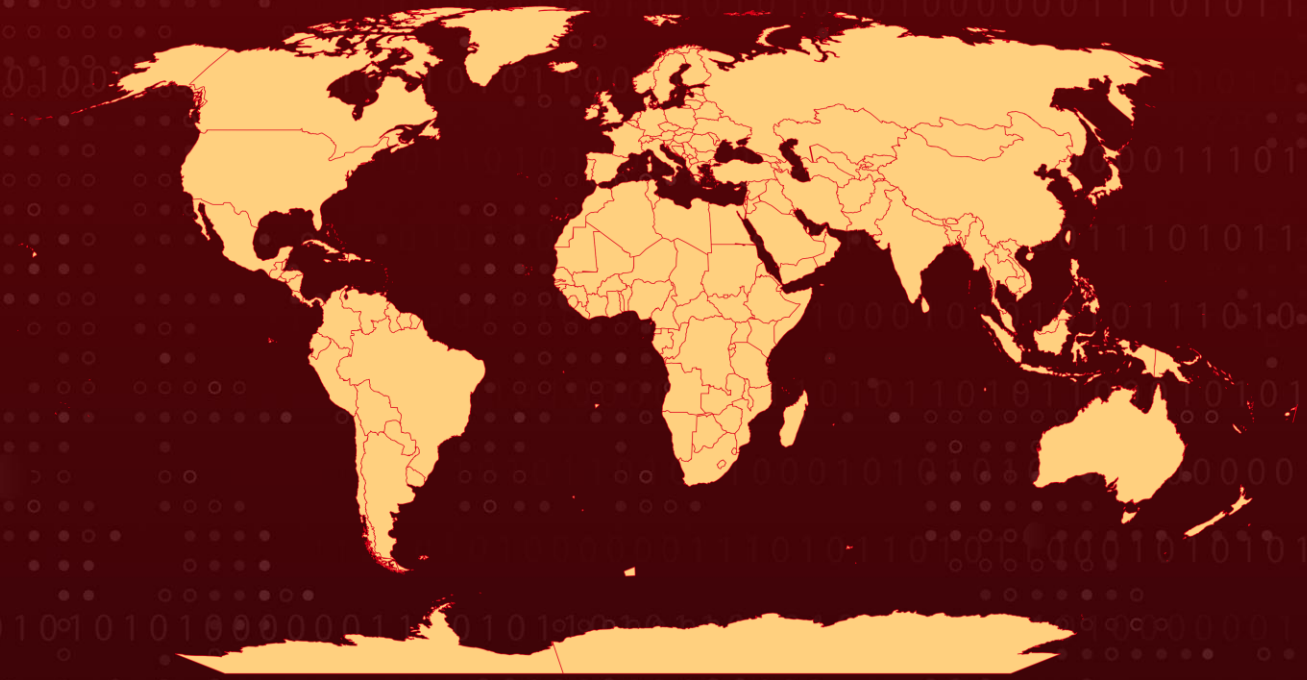
Sysrv Harnessing Google Subdomains to Circulate XMRig

Date of Publication	Admiralty Code	TA Number
March 27, 2024	A1	TA2024120

Summary

First Seen: 2020
Malware: Sysrv Botnet, XMRig Miner
Attack Region: Worldwide
Attack: Sysrv, an advanced botnet, employs a Golang worm to infiltrate devices and distribute XMRig cryptocurrency miners, leveraging network vulnerabilities and undergoing constant evolution through operator refinement.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-9805	Apache Struts Deserialization of Untrusted Data Vulnerability	Apache Struts	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Atlassian Confluence Data Center and Server	✗	✓	✓
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Server and Data Center	✗	✓	✓

Attack Details

#1 Sysrv operates as a sophisticated botnet, employing a Golang worm to infiltrate devices and deploy XMRig crypto miners. It spreads by exploiting network vulnerabilities and undergoes continuous refinement by its operators.

#2 Initially documented in 2020, Sysrv has since evolved into a potent threat, generating conspicuous bot traffic that targets numerous sites across various countries. It endeavors to exploit well-known web vulnerabilities in Apache Struts (CVE-2017-9805) and Atlassian Confluence (CVE-2023-22527 and CVE-2021-26084).

#3 Utilizing a seemingly legitimate domain associated with a recognized Malaysian academic institution, which hosts the institution's digital archive via the Duraspace platform, marks a notable strategy in the Sysrv botnet campaign. The perpetrators have compromised the site to host their malicious files.

#4 Upon downloading, the malware manifests as a dropper bash script, initializing several variables pertinent to the retrieval of the second-stage binary. Prior to downloading and executing the second-stage binary, the script undertakes various commands to terminate processes and remove programs associated with endpoint protection and prior malware infections.

#5 Of particular interest is the utilization of a Google subdomain to fetch the second-stage binary, which subsequently deploys the XMRig crypto miner on infected devices. A noteworthy difference from previous iterations of this campaign is the incorporation of additional functionalities in the malicious downloader script, aimed at preparing diverse CPU architectures for the impending mining operation.

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.

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Secure Configuration Management: Enforce secure configurations for servers, network devices, and applications, following industry best practices and security baselines to reduce the attack surface.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0040 Impact	TA0011 Command and Control
TA0010 Exfiltration	T1204.002 Malicious File	T1070 Indicator Removal	T1560 Archive Collected Data

T1059 Command and Scripting Interpreter	T1057 Process Discovery	T1083 File and Directory Discovery	T1005 Data from Local System
T1027 Obfuscated Files or Information	T1036 Masquerading	T1001 Data Obfuscation	T1027.010 Command Obfuscation
T1027.002 Software Packing	T1584 Compromise Infrastructure	T1562 Impair Defenses	T1496 Resource Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
XMR wallet	483F2xjkCUegxPM7wAexam1Be67EqDRZpS7azk8hcGETSustmuxd1Agffa3XSHFyzeFprLyHKm37bTPShFUTKgctMSBVuuK
URLs	hxxp[://]redacted/jspui/ldr.sh, hxxp[://]redacted/jspui/cron, hxxp[://]92.60.39[.]76:9991/ldr.sh, hxxp[://]92.60.39[.]76:9991/cron, hxxps[://]sites.google[.]com/view/osk05/osk/E, hxxps[://]sites.google[.]com/view/osk05/osk/d, hxxps[://]gulf.moneroocean[.]stream:10128, hxxps[://]109.123.233[.]251:443
SHA256	6fb9b4dced1cf53a9533ed497f38550915f9e448e62a6f43e9d8b696bd5375dc, f0a299b93f1a2748edd69299f694d3a12edbe46485d29c1300172d4ac4fd09d4, 1ba8f42d8db461bb45f9d3e991c137b7b504aee5213cfe7a12cd4b366512696e, 495500dcd8b3fa858335f0c85ddcc265f09ed638d87226e8bce8b53ef626464e, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b

Patch Links

https://cwiki.apache.org/confluence/display/WW/S2-052

https://jira.atlassian.com/browse/CONFSERVER-93833

https://jira.atlassian.com/browse/CONFSERVER-67940

References

https://www.imperva.com/blog/new-sysrv-botnet-variant-makes-use-of-google-subdomain-to-spread-xmrig-miner/

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.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

March 27, 2024 • 4:30 AM

More at www.hivepro.com