Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Matrix DDoS Campaign Exposes Alarming IoT Vulnerabilities

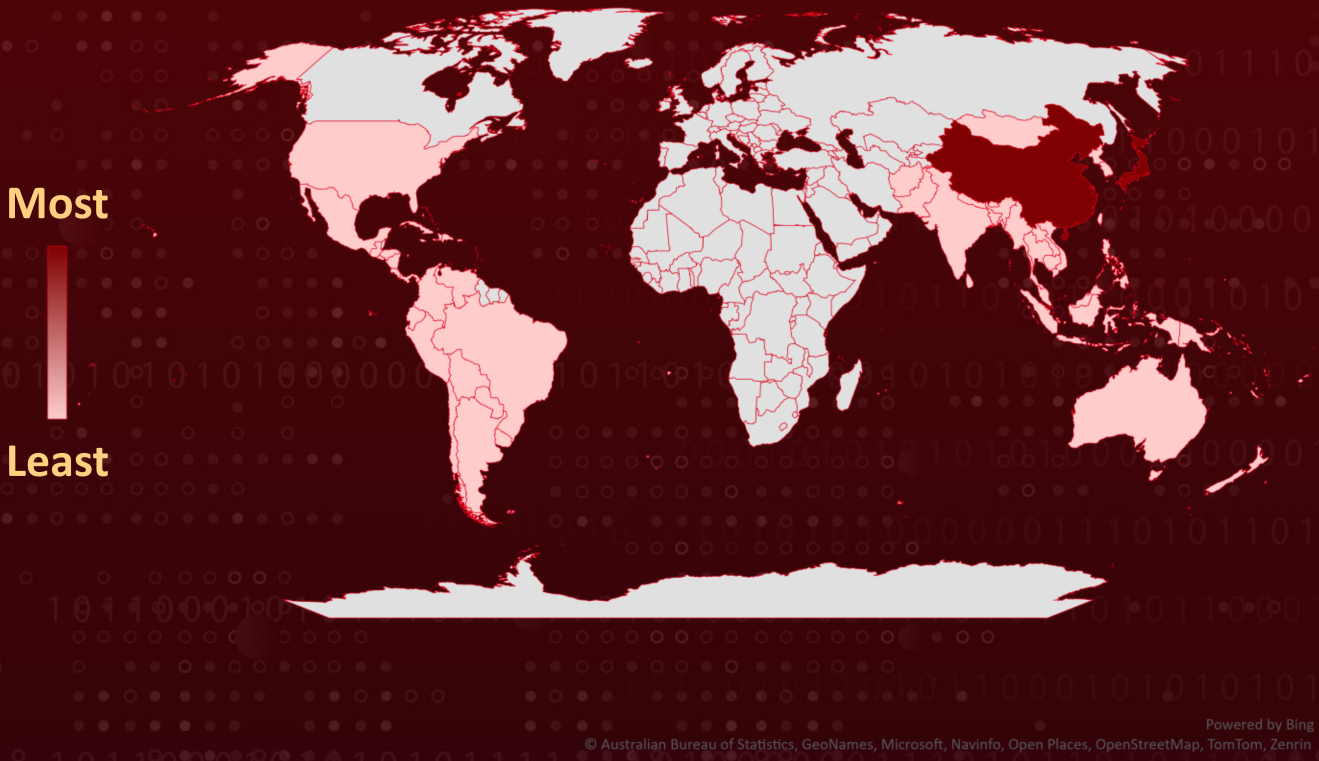
Date of Publication	Admiralty Code	TA Number
November 28, 2024	A1	TA2024446

Summary

Threat Actor: Matrix
Malware: Mirai botnet
Attack Regions: Asia, Americas

Attack: The Matrix threat actor is behind a highly disruptive Distributed Denial-of-Service (DDoS) campaign, believed to have originated from Russia, revealing critical vulnerabilities in IoT devices, routers, and enterprise systems. Utilizing brute-force attacks, weak credentials, and readily accessible hacking tools, Matrix is building a global botnet powered by the notorious Mirai malware. This campaign highlights the growing threat posed by plug-and-play cyberattack tools, empowering even novice attackers to pose significant risks in today's cybersecurity landscape.

Attack Regions


Most
Least
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A newly identified Distributed Denial-of-Service (DDoS) campaign, attributed to the Matrix threat actor, signals a troubling advancement in cyber threats. Suspected to have Russian origins, Matrix exploits vulnerabilities and misconfigurations in internet-connected devices, particularly IoT and enterprise systems.

#2 This campaign highlights the growing accessibility of AI-powered hacking tools and plug-and-play malware, which amplify the threat posed by inexperienced attackers. The operation employs publicly available scripts, brute-force techniques, and the exploitation of weak or default credentials to assemble a botnet with **global reach**.

#3 Compromised devices include IP cameras, DVRs, routers, telecom equipment, and various IoT systems. By exploiting these systems, attackers establish initial access and expand their malicious activities. Router vulnerabilities, such as those in ZTE and GPON models, are exploited through flaws like CVE-2017-18368 and CVE-2021-20090.

#4 Devices built on the Hi3520 platform are targeted for unauthorized access and remote command execution via insecure HTTP protocols. Lightweight Linux distributions, including uClinux, are exploited through default configurations and UPnP vulnerabilities in Huawei and Realtek devices.

#5 Sophisticated attacks exploit weaknesses in platforms such as Apache Hadoop's YARN and HugeGraph servers, enabling remote code execution and targeting enterprise environments. Matrix further utilizes publicly available tools, deploying malware like the **Mirai** botnet to conduct widespread DDoS attacks.

#6 Additional tools include PYbot, pynet, DiscordGo, Homo Network, and programs designed to disable Microsoft Defender Antivirus on Windows systems. The campaign also involves cryptocurrency mining, specifically targeting the ZEPHYR coin, indicating a dual-purpose operation focused on both disruption and financial gain. This combination of rudimentary techniques and deliberate targeting underscores the increasing availability and threat of cyberattack toolkits in today's digital landscape.

Recommendations

Strengthen Credential Policies: Replace default and weak credentials on IoT devices, routers, and other networked devices. Implement multi-factor authentication (MFA) wherever possible to reduce the likelihood of successful brute-force attacks. Enforce strong password policies across all devices, particularly those connected to the internet.

Regular Vulnerability Scanning & Patch Management: Continuously monitor IoT devices, routers, and enterprise systems for vulnerabilities, especially CVEs targeting default configurations, weak credentials, and unpatched systems. Utilize automated vulnerability scanning tools to identify misconfigurations and outdated software versions that may expose devices to exploitation.

Monitor for Unusual Access Patterns: Set up logging and monitoring systems to detect unusual login attempts, such as brute-force attempts or SSH/Telnet login failures. Investigate patterns of exploitation and immediately block suspicious IP addresses.

Utilize Endpoint Detection and Response (EDR) Solutions: Deploy advanced Endpoint Detection and Response (EDR) solutions across all networked devices, including IoT and enterprise systems, to monitor for anomalous activity and potential signs of compromise.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0040 Impact	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1059 Command and Scripting Interpreter	T1059.006 Python	T1543 Create or Modify System Process	T1562 Impair Defenses

T1562.001 Disable or Modify Tools	T1036 Masquerading	T1110 Brute Force	T1046 Network Service Discovery
T1210 Exploitation of Remote Services	T1563 Remote Service Session Hijacking	T1563.001 SSH Hijacking	T1005 Data from Local System
T1102 Web Service	T1573 Encrypted Channel	T1496 Resource Hijacking	T1499 Endpoint Denial of Service
T1499.002 Service Exhaustion Flood			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	df521f97af1591efff0be31a7fe8b925, 76975e8eb775332ce6d6ca9ef30de3de, 9181d876e1fcd8eb8780d3a28b0197c9, c7d7e861826a4fa7db2b92b27c36e5e2, 0e3a1683369ab94dc7d9c02adbed9d89, 9c9ea0b83a17a5f87a8fe3c1536aab2f, 53721f2db3eb5d84ecd0e5755533793a, d653fa6f1050ac276d8ded0919c25a6f, 866c52bc44c007685c49f5f7c51e05ca, 5a66b6594cb5da4e5fcb703c7ee04083, c332b75871551f3983a14be3bfe2fe79
IPv4	199[.]232[.]46[.]132, 5[.]42[.]78[.]100, 78[.]138[.]130[.]114, 85[.]192[.]37[.]173, 5[.]181[.]159[.]78, 217[.]18[.]63[.]132

CVEs

The Matrix threat actor strategically leveraged the following vulnerabilities to broaden its impact and target victims via compromised devices. For quick access, patch links for each exploited CVE are hyperlinked via the checkmarks labeled under ‘Patch Link.’

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2017-18368	Zyxel P660HN-T1A Routers Command Injection Vulnerability	Zyxel P660HN-T1A Routers	✗	✓	✓
CVE-2021-20090	Arcadyan Buffalo Firmware Path Traversal Vulnerability	Buffalo WSR firmware	✗	✓	✓
CVE-2024-27348	Apache HugeGraph-Server Improper Access Control Vulnerability	Apache HugeGraph-Server	✗	✓	✓
CVE-2022-30525	Zyxel Multiple Firewalls OS Command Injection Vulnerability	Zyxel Multiple Firewalls	✗	✓	✓
CVE-2022-30075	TP-Link Remote Code Execution	TP-Link Router AX50 firmware	✗	✗	✓
CVE-2018-10562	Dasan GPON Routers Command Injection Vulnerability	Dasan GPON home routers	✗	✓	✗
CVE-2018-10561	Dasan GPON Routers Command Injection Vulnerability	Dasan GPON home routers	✗	✓	✗
CVE-2018-9995	TBK Unauthorized Command Execution Vulnerability	TBK DVR devices	✗	✗	✗
CVE-2017-17215	Huawei HG532 RCE Vulnerability	Huawei HG532 router: All versions	✓	✗	✓
CVE-2017-17106	Zivif Webcams Information Disclosure	Zivif PR115-204-P-RS webcams	✗	✗	✗

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2014-8361	Realtek SDK Improper Input Validation Vulnerability	Realtek SDK: All versions	✗	✓	✓

References

https://www.aquasec.com/blog/matrix-unleashes-a-new-widespread-ddos-campaign/

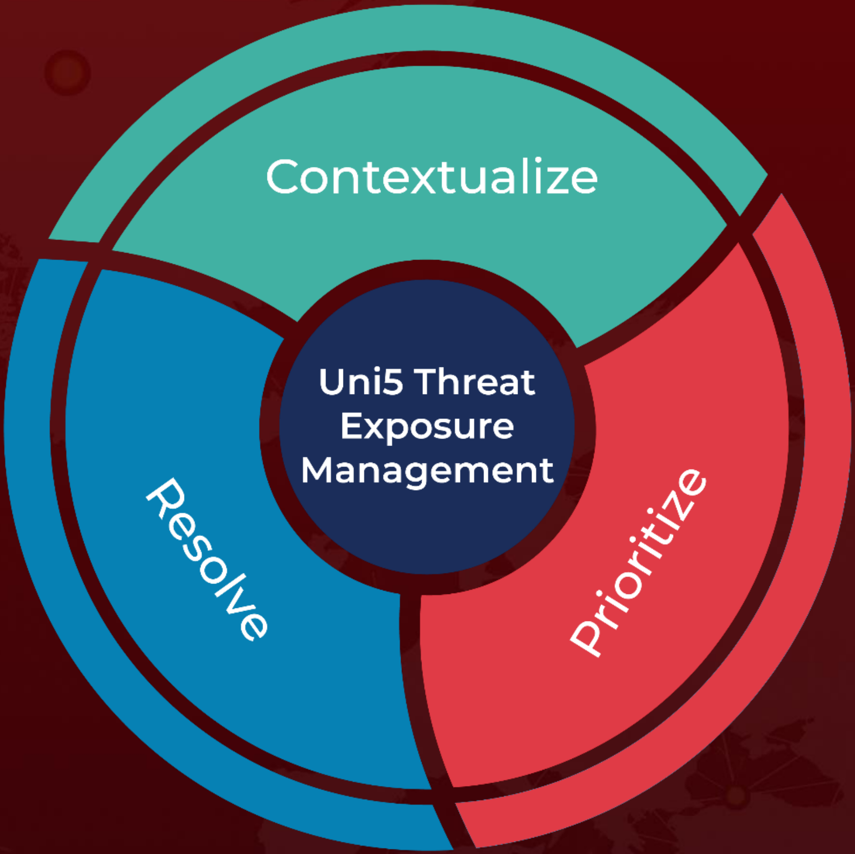
https://hivepro.com/threat-advisory/hackers-exploit-zero-day-flaw-in-eol-geovision-devices/

https://hivepro.com/threat-advisory/raptor-train-paradox-a-multi-tiered-botnet-phenomenon/

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 28, 2024 • 11:00 PM

More at www.hivepro.com