Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

The Rising Diicot Threat Group with Diverse Attack Capabilities

Date of Publication	Admiralty Code	TA Number
June 20, 2023	A1	TA2023270

Summary

First appeared: July 2021
Attack Region: Worldwide
Affected Platform: Linux
Actor Name: Diicot (aka Mexals)
Malware: Mirai, Cayosin, XMRig
Attack: A Romanian threat group “Diicot” has been actively employing SSH brute-forcing and deploying malware loaders to compromise systems for the purpose of cryptocurrency mining. The campaign involves exploiting OpenWRT systems and deploying customized XMRig variants alongside aliases and disguised network scanners.

Attack Regions

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

Attack Details

#1

Diicot is an emerging threat actor that has recently gained attention for its diverse attack capabilities. This threat group, also known as "Mexals", has been involved in various malicious activities, including cryptojacking, doxxing, and distributed denial-of-service (DDoS) attacks. With origins believed to be in Romania, Diicot has displayed a range of sophisticated techniques to carry out its campaigns.

#2

Diicot was discovered by cybersecurity researchers during a crypto-jacking campaign in July 2021. The group utilized a Go-based SSH brute-forcing tool, Diicot Brute, and has since exhibited a resurgence of activity starting from October 2022, resulting in significant illicit profits.

#3

In the recent attack campaigns orchestrated by Diicot involve a complex execution chain comprising multiple interdependent payloads. To evade detection, the group employs obfuscation techniques, such as using the Shell Script Compiler (shc) and modifying the UPX header. Their command and control (C2) infrastructure is based on Discord, utilizing webhook URLs for data exfiltration and campaign statistics.

#4

Diicot's notable payloads include custom tools like "aliases" for SSH brute-forcing and loaders such as "payload" and ".diicot" for cryptocurrency mining. They also deploy the Cayosin botnet agent and the Mirai and XMRig variant "cutie.<arch>" for further propagation. Additionally, Diicot employs the Chrome scanner, a modified version of Zmap, for internet scanning to identify vulnerable systems.

Recommendations

Implement Strong Authentication Mechanisms: Since Diicot primarily relies on SSH brute-forcing as an initial access method, it is crucial to enforce strong authentication mechanisms. This includes using complex and unique passwords or passphrase-based authentication, implementing two-factor authentication (2FA), and regularly updating and rotating SSH keys. Additionally, implementing rate limiting and account lockout policies can help mitigate brute-force attacks.

Employ Network Monitoring and Intrusion Detection Systems: Deploying network monitoring and intrusion detection systems can help detect and block malicious activities associated with Diicot. These systems can identify suspicious network traffic, unauthorized access attempts, and communication with known malicious IP addresses or C2 servers.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0006 Credential Access	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0001 Initial Access	TA0009 Collection	TA0011 Command and Control
TA0040 Impact	T1027 Obfuscated Files or Information	T1110 Brute Force	T1106 Native API
T1059 Command and Scripting Interpreter	T1496 Resource Hijacking	T1082 System Information Discovery	T1102 Web Service
T1056 Input Capture	T1190 Exploit Public-Facing Application	T1095 Non-Application Layer Protocol	T1071 Application Layer Protocol
T1071.004 DNS	T1048 Exfiltration Over Alternative Protocol	T1003 OS Credential Dumping	T1595.002 Vulnerability Scanning
T1021.004 SSH	T1583 Acquire Infrastructure	T1583.005 Botnet	T1595 Active Scanning
T1021 Remote Services	T1498 Network Denial of Service		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	139[.]99[.]123[.]196 84[.]54[.]50[.]198 45[.]88[.]67[.]94
Domains	arhivehaceru[.]com multi-user[.]target
URLs	http://139[.]99[.]123[.]196:80 http://45[.]88[.]67[.]94/[.]x/aliases http://45[.]88[.]67[.]94/diicotapi/skema0803 http://45[.]88[.]67[.]94/payload http://45[.]88[.]67[.]94:7777

TYPE	VALUE
URLs	http://84[.]54[.]50[.]198/pedalcheta/bins[.]sh http://arhivehaceru[.]com/payload http://arhivehaceru[.]com:2121/api?haceru=$haceru
MD5	0874c80875045b0f40b9d2a2fbac1bbc 42141fe8a449f0513dc5ec8c21f7fa74 946689ba1b22d457be06d95731fcbcac a57667f72436624c86fe9f5e95c7613f d45ab42f54d3345381388b87584ab562 e50059b13c04ec93c53dd3709539597f
SHA1	02d5a7503ba65be4acd228b7c77dfee6c6fcbae8 332ca416559fb99b12fcabdbd419b380a93eea14 9fdcb34c96b7b78d17d599f76e64a6151399adc7 a5e524e6689040a8f76e34864354b47790d54a0d e998494f91b08b52b28fe3304e9322962e3d1b58 ee1c59595732ca21c9e4e793b4c20e1c39a5071f
SHA256	14779e087a764063d260cafa5c2b93d7ed5e0d19783eeaea6abb12d17561949a 180d30bf357bc4045f197b26b1b8941af9ca0203226a7260092d70dd15f3e6ab 437af650493492c8ef387140b5cb2660044764832d1444e5265a0cd3fe6e0c39 6bce1053f33078f3bbbd526162d9178794c19997536b821177f2cb0d4e6e6896 7389e3aada70d58854e161c98ce8419e7ab8cd93ecd11c2b0ca75c3cafed78cb 7d93419e78647d3cdf2ff53941e8d5714afe09cb826fd2c4be335e83001bdabf a163da5c4d6ee856a06e4e349565e19a704956baeb62987622a2b2c43577cdee aabf2ef1e16a88ae0d802efcb2525edb90a996bb5d280b4c61d2870351e3fba4 d0e8a398a903f1443a114fa40860b3db2830488813db9a87ddcc5a8a337edd73 de6dff4d3de025b3ac4aff7c4fab0a9ac4410321f4dca59e29a44a4f715a9864 e9bbe9aecfaea4c738d95d0329a5da9bd33c04a97779172c7df517e1a808489c

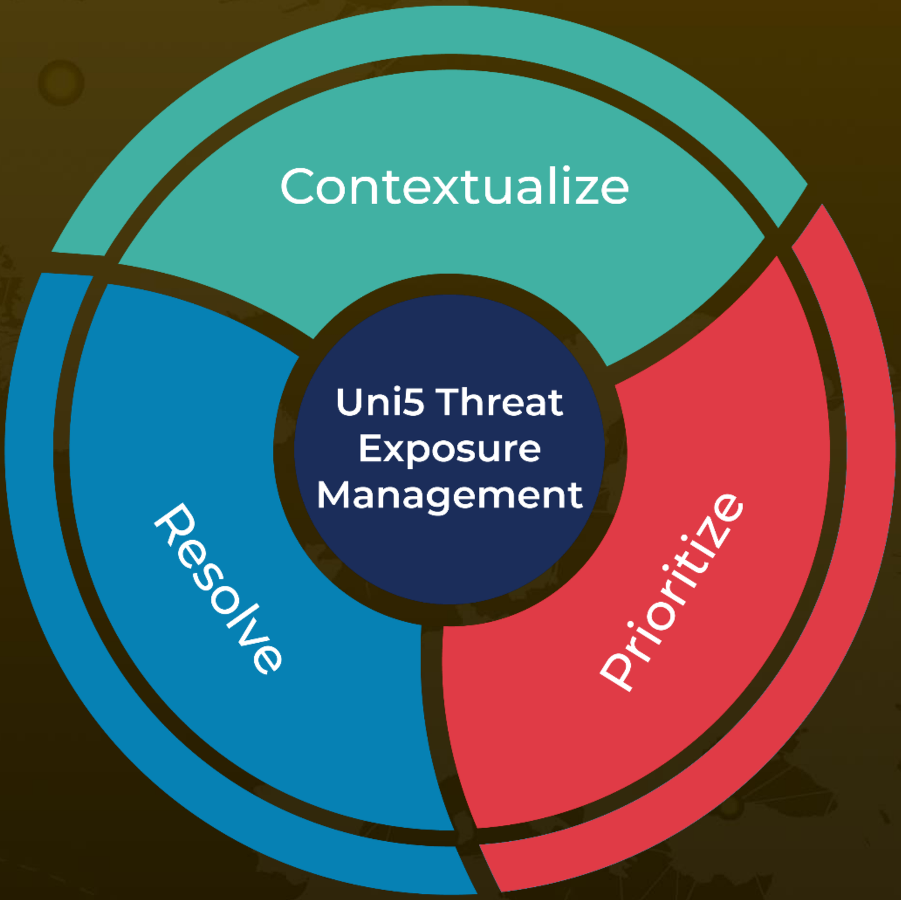
References

https://www.cadosecurity.com/tracking-diicot-an-emerging-romanian-threat-actor/

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

June 20, 2023 • 5:30 AM

More at www.hivepro.com