Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

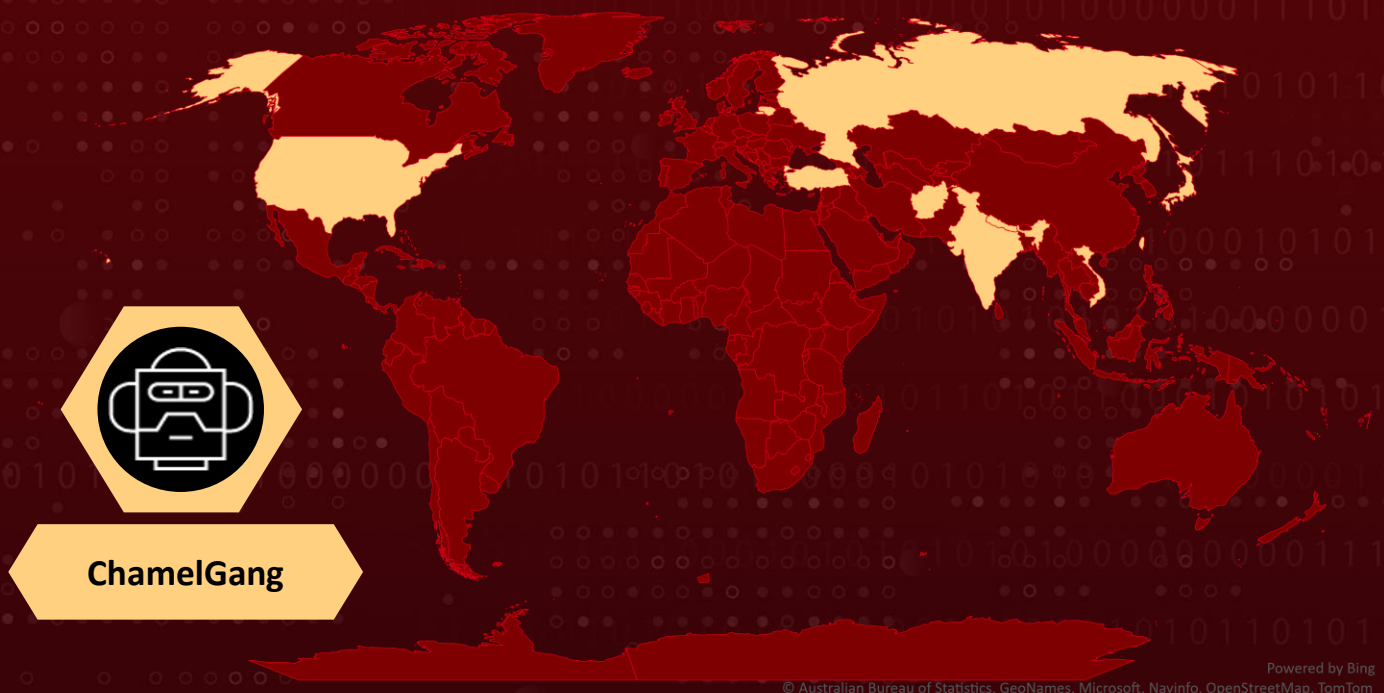
ChamelGang Evolves Introducing ChamelDoH The Stealthy Linux Malware

Date of Publication	Admiralty code	TA Number
June 16, 2023	A1	TA2023266

Summary

First Appearance: 2021
Actor Name: ChamelGang
Targeted Countries: Russia, the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania, and Nepal
Targeted Industries: Energy, aviation, and government organizations
Affected Platforms: Windows, Linux
Malware: ChamelDoH

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-12149	Red Hat JBoss Application Server Remote Code Execution Vulnerability	Red Hat JBoss Application Server	✗	✓	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓

Actor Details

#1

The Chinese threat group known as 'ChamelGang' (from the word "chameleon") has developed a new Linux malware called 'ChamelDoH.' This malware infects Linux devices and establishes communication with the attackers' servers using DNS-over-HTTPS (DoH). The use of DoH allows the malware's communication to be encrypted and disguised as regular HTTPS traffic, making it difficult to detect.

#2

The malware utilizes a JSON configuration to retrieve command and control (C2) hostnames and a list of legitimate DoH cloud providers that can be abused for malicious purposes. ChamelDoH encrypts its communications using AES128 and a modified base64 encoding. It sends DNS requests as TXT records containing encoded data to the malicious nameserver controlled by the threat actors.

#3

The C2 server responds with encoded TXT records containing commands for the malware to execute on the infected device. The malware can perform various operations such as executing files or shell commands, downloading and uploading files, deleting files, and copying files. The ChamelGang threat group, previously known for targeting Windows systems, has expanded its toolkit to include Linux malware.

#4 ChamelDoH was first identified in December 2022 and has been observed targeting energy, aviation, and government organizations in various countries. The malware's use of DoH and its integration with legitimate DoH servers from Google and Cloudflare make it challenging to block or detect malicious traffic.

#5 Notably, ChamelGang's activities in Q2 2021 involved compromising an energy company's network through supply chain penetration, DLL hijacking, and malware installation. They collected and exfiltrated data using disguised infrastructure and legitimate services.

#6 On August 16, 2021, ChamelGang targeted a Russian aviation production company, exploiting Microsoft Exchange vulnerabilities. They gained remote code execution and installed web shells and backdoors, but the threat was detected and mitigated.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
ChamelGang	China	Russia, the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania, and Nepal	Energy, aviation, and government organizations
	MOTIVE		
	Information theft and espionage		

Recommendations

Implement robust network security measures: Utilize firewalls, intrusion detection and prevention systems (IDS/IPS), and secure gateway devices to detect and block malicious network traffic associated with ChamelDoH. Monitor DNS traffic for suspicious patterns and block access to known malicious domains.

Keep systems updated and secure: Regularly apply security patches and updates to Linux devices to address vulnerabilities that could be exploited by ChamelDoH. Implement strong authentication mechanisms, such as multi-factor authentication (MFA), and enforce the principle of least privilege to reduce the risk of unauthorized access.

Patch Management and Endpoint Protection: Maintain up-to-date software and operating systems by promptly applying security patches. Deploy reliable endpoint protection solutions with anti-malware and anti-exploit capabilities to detect and remove Asylum Ambuscade's malicious software from endpoints.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0042 Resource Development	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0010 Exfiltration	TA0009 Collection	TA0011 Command and Control
T1105 Ingress Tool Transfer	T1071 Application Layer Protocol	T1189 Drive-by Compromise	T1071.004 DNS
T1059 Command and Scripting Interpreter	T1564.001 Hidden Files and Directories	T1564 Hide Artifacts	T1027 Obfuscated Files or Information
T1082 System Information Discovery	T1005 Data from Local System	T1041 Exfiltration Over C2 Channel	T1572 Protocol Tunneling

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	update[.]microsoft-support[.]net ns31[.]mayashopping[.]net ns30[.]mayashopping[.]net ns2[.]spezialsex[.]com ns2[.]marocfamily[.]com ns1[.]spezialsex[.]com ns1[.]marocfamilyx[.]com ns1[.]marocfamilym[.]com ns1[.]marocfamily[.]com
IPV4	45[.]91[.]24[.]3
SHA256	fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72 e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9 b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c 92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b 70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007 6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe 4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0 34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7

Patch Links

https://access.redhat.com/security/cve/CVE-2017-12149

https://bugzilla.redhat.com/show_bug.cgi?id=1486220

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

References

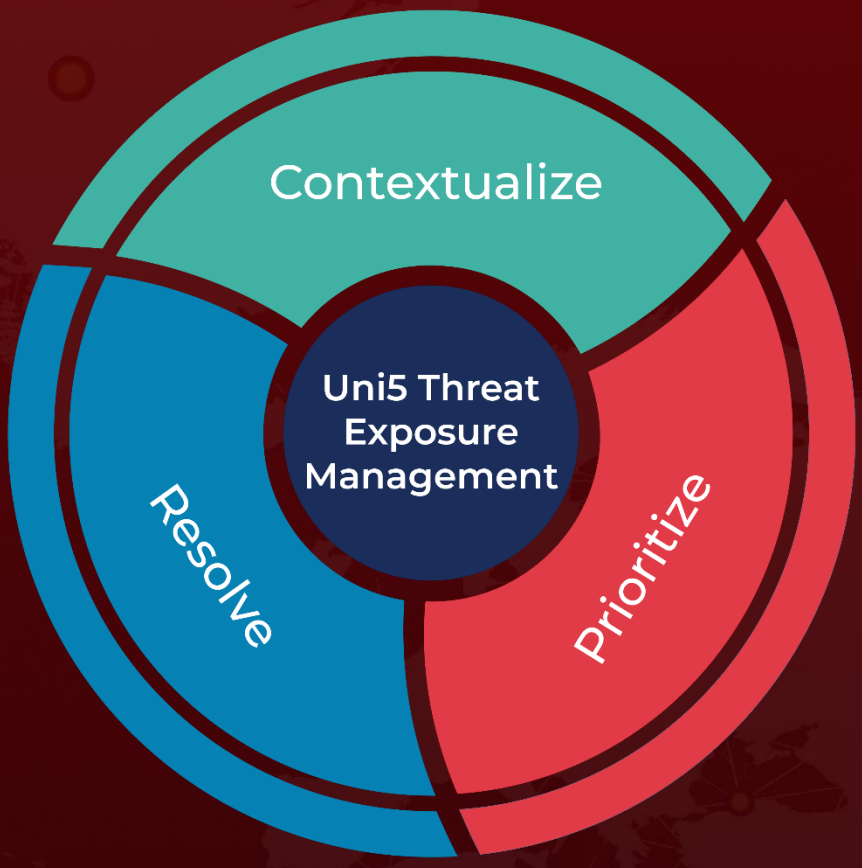
https://stairwell.com/news/chamelgang-and-chameldoh-a-dns-over-https-implant/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/

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 16, 2023. 3:30 AM

More at www.hivepro.com