Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

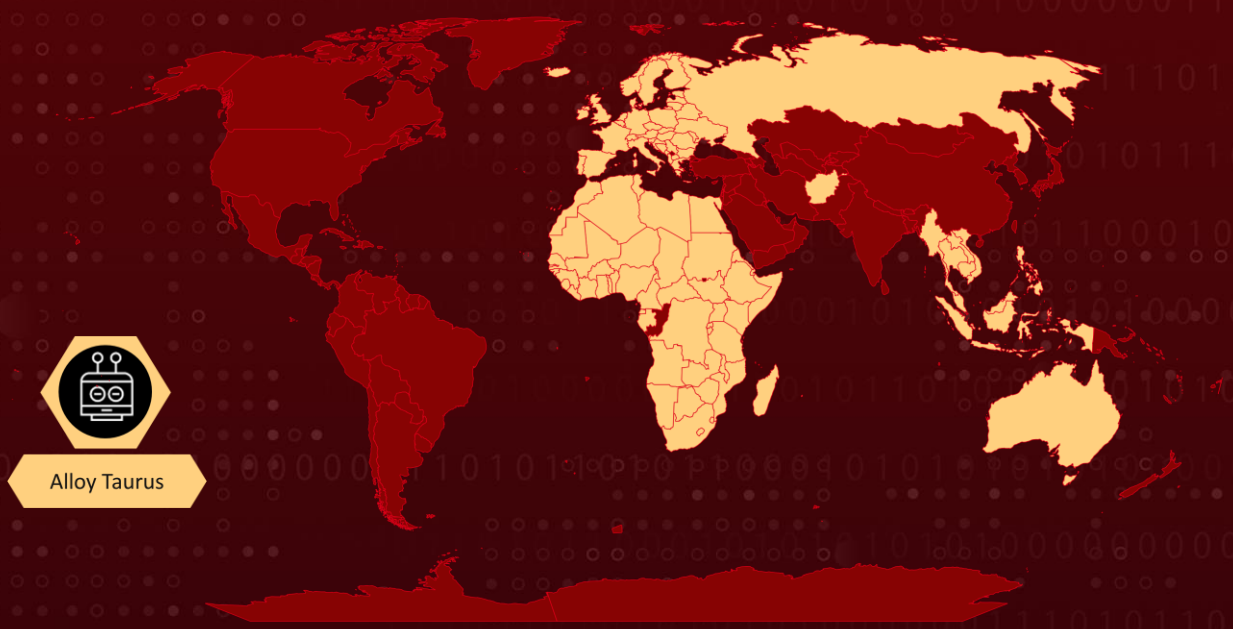
New PingPull Malware Variant Targets Linux Systems

Date of Publication	Admiralty Code	TA Number
April 27, 2023	A1	TA2023202

Summary

Attack began: March 2023
Threat Actor: Alloy Taurus (GALLIUM, Softcell, Phantom Panda)
Attack Regions: Southeast Asia, Europe and Africa
Attack Industry: Financial, Government & Telecommunications
Malware: PingPull
Attack: The PingPull malware variant that targets Linux systems is linked to Alloy Taurus, and it communicates with a domain over HTTPS to receive encrypted commands for executing specific functions.

Attack Regions



Attack Details

#1 A new version of malware, known as PingPull, has emerged with a specific focus on Linux systems. Since its discovery in September 2021, the malware has been utilized in multiple campaigns. In June 2022, researchers confirmed that the Alloy Taurus group, a Chinese advanced persistent threat (APT) group, was responsible for the malware's deployment. The Alloy Taurus group has been conducting cyberespionage campaigns since at least 2012.

#2 The PingPull variant communicates with a domain through HTTP POST requests using HTTPS. The C2 server sends data that is Base64 encoded ciphertext. This ciphertext is encrypted with AES using P29456789A1234sS as the key. The plaintext appears as HTTP parameters, and the malware will parse for specific parameters using the characters & and =.

#3 Another backdoor, named Sword2033, uses the same C2 infrastructure as PingPull. The backdoor supports three basic functions, and the command handlers for Sword2033 use the same values and functionality as PingPull. Researchers identified the C2 for Sword2033 in South Africa, and the domain name of the C2 server appears to impersonate the South African military.

Recommendations

- Keep your Linux systems updated and patched: Since this PingPull malware specifically targets Linux systems, it's important to keep your systems updated with the latest security patches and software updates.
- Use endpoint security solutions: An XDR solution that can identify malicious code through advanced machine learning and behavioral analytics can help to identify and block PingPull malware in real-time. This can help to prevent the malware from spreading throughout your network and causing damage.
- Implement network security measures: In addition to endpoint security, it's important to have network security measures in place, such as a Next-Generation Firewall (NGFW) with threat prevention, URL filtering, and DNS security capabilities. This can help to detect and block PingPull malware from communicating with its command and control (C2) server, as well as prevent users from inadvertently accessing malicious websites or downloading infected files.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**T1059** Command and Scripting Interpreter	**T1059.004** Unix Shell
T1543 Create or Modify System Process	**T1543.002** Systemd Service	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools
T1564 Hide Artifacts	**T1564.001** Hidden Files and Directories	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1071** Application Layer Protocol	**T1095** Non-Application Layer Protocol
T1571 Non-Standard Port			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae 5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507 e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253
Domains	yrhsywu2009.zapto[.]org *.saspecialforces.co[.]za vpn729380678.softether[.]net
IPV4	5.181.25[.]99 196.216.136[.]139

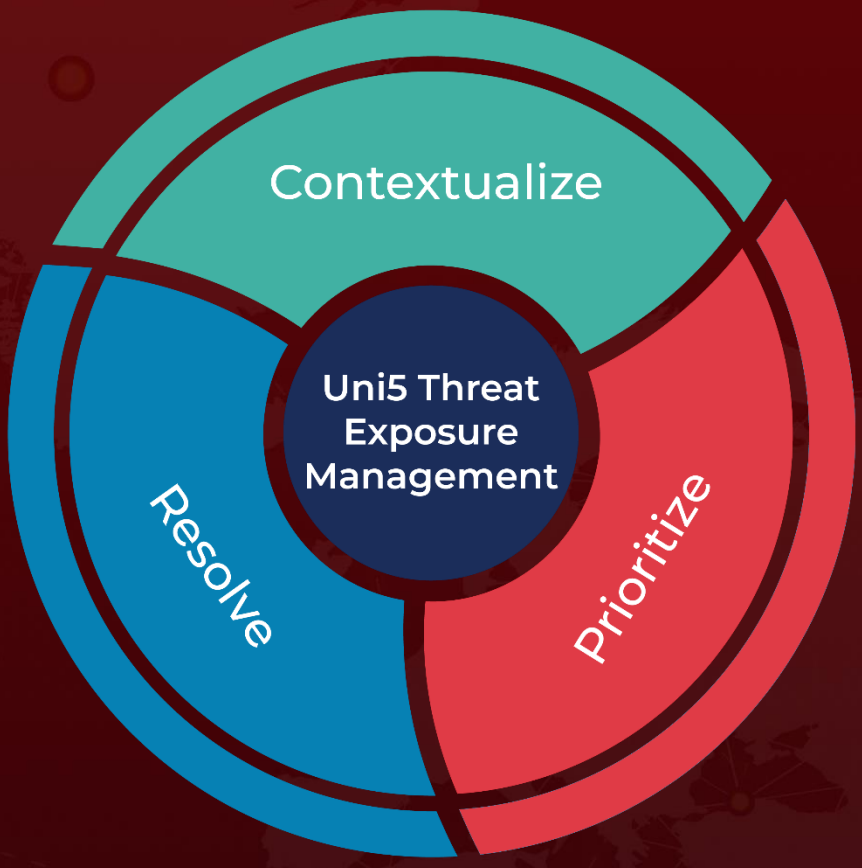
References

https://unit42.paloaltonetworks.com/alloy-taurus/

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

April 27, 2023 • 6:00 AM

More at www.hivepro.com