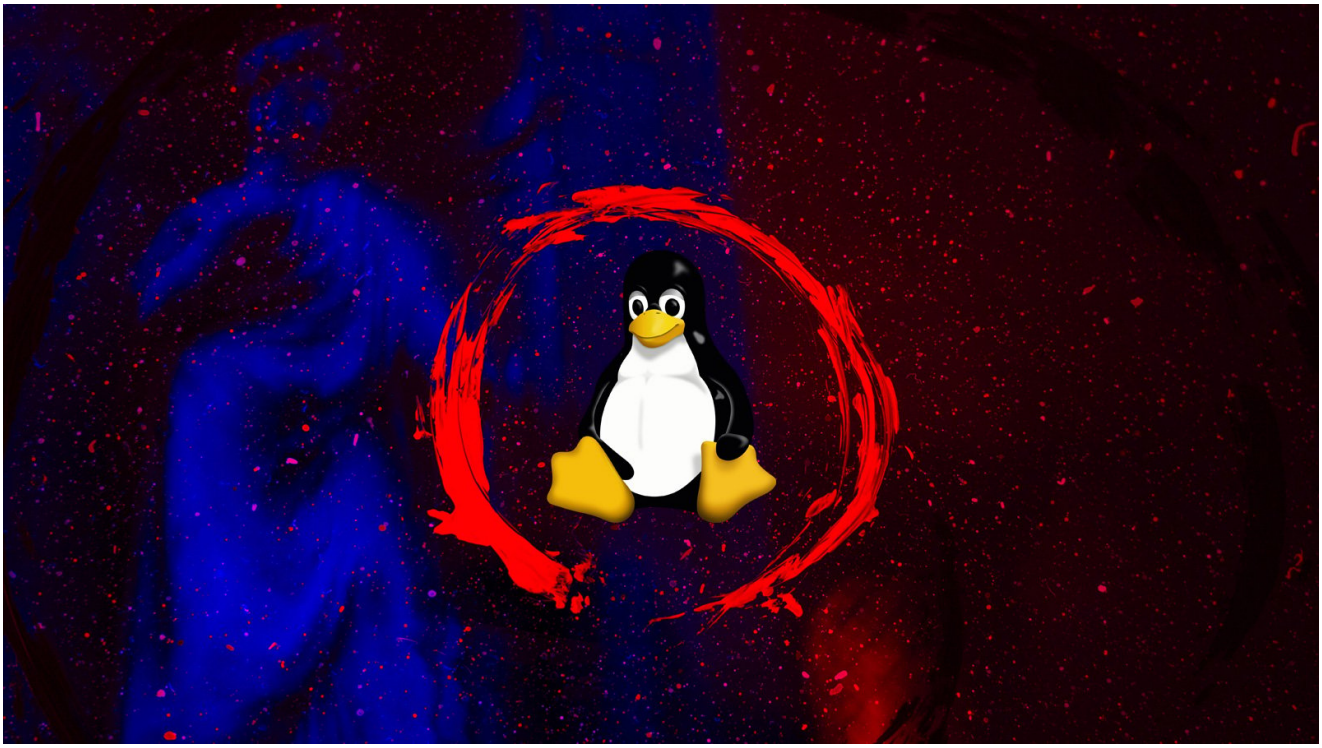
Chinese hackers use new Linux malware variants for espionage

bleepingcomputer.com/news/security/chinese-hackers-use-new-linux-malware-variants-for-espionage/

Bill Toulas

By
Bill Toulas

- April 26, 2023
- 06:00 AM
- 1



Hackers are deploying new Linux malware variants in cyberespionage attacks, such as a new PingPull variant and a previously undocumented backdoor tracked as 'Sword2033.'

PingPull is a RAT (remote access trojan) first documented by Unit 42 last summer in espionage attacks conducted by the Chinese state-sponsored group Gallium, also known as Alloy Taurus. The attacks targeted government and financial organizations in Australia, Russia, Belgium, Malaysia, Vietnam, and the Philippines.

Unit 42 continued to monitor these espionage campaigns and today reports that the Chinese threat actor uses new malware variants against targets in South Africa and Nepal.

PingPull on Linux

The Linux variant of PingPull is an ELF file that only 3 out of 62 anti-virus vendors currently flag as malicious.

Unit 42 was able to determine it's a port of the known Windows malware by noticing similarities in the HTTP communication structure, POST parameters, AES key, and the commands it receives from the threat actor's C2 server.

The commands the C2 sends to the malware are indicated by a single uppercase character in the HTTP parameter, and the payload returns the results to the server via a base64-encoded request.

The parameters and corresponding commands are:

- A – Get the current directory
- B – List folder
- C – Read text file
- D – Write a 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 a file
- J – Create a Directory
- K – Timestamp file with a specified timestamp in "%04d-%d-%d %d:%d:%d" format
- M – Run command

Unit 42 comments that the command handlers used in PingPull match those observed in another malware named 'China Chopper,' a web shell seen heavily used in attacks against Microsoft Exchange servers.

Sword2023 details

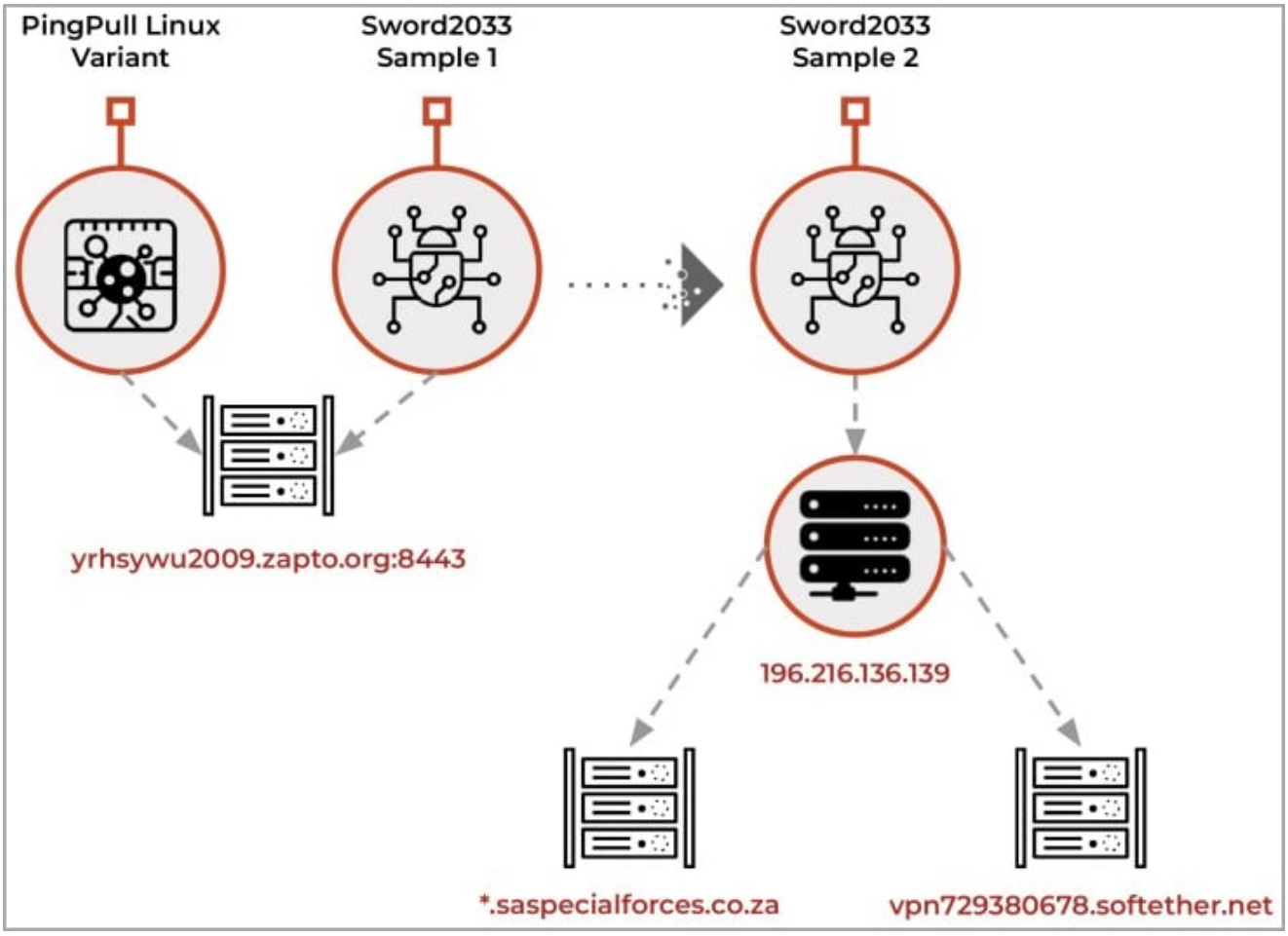
Unit 42 also found a new ELF backdoor that communicated with the same command and control server (C2) as PingPull.

This is a simpler tool with more basic functions like uploading files on the breached system, exfiltrating files, and executing a command with "; echo <random number>\n" appended to it.

The echo command adds random data on the execution log, possibly to make analysis more challenging or obfuscate its activity.

Unit 42 discovered a second Sword2023 sample associated with a different C2 address impersonating the South African military.

The same sample was linked to a Soft Ether VPN address, a product that Gallium is known to use in its operations.



Gallium's C2 map based on malware communication *(Unit 42)*

The cybersecurity firm comments that this isn't a random choice, as in February 2023, South Africa took part in joint military exercises with Russia and China.

In conclusion, Gallium continues to refine its arsenal and broadens its target range using the new Linux variants of PingPull and the newly discovered Sword2023 backdoor.

Organizations must adopt a comprehensive security strategy to effectively counter this sophisticated threat rather than relying solely on static detection methods.

Related Articles:

'Bitter' espionage hackers target Chinese nuclear energy orgs

Winter Vivern APT hackers use fake antivirus scans to install malware

YoroTrooper cyberspies target CIS energy orgs, EU embassies

SonicWall devices infected by malware that survives firmware upgrades

Newly exposed APT43 hacking group targeting US orgs since 2018

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.