THREAT HUNTING

LAB

Telnet CVE-2026-24061

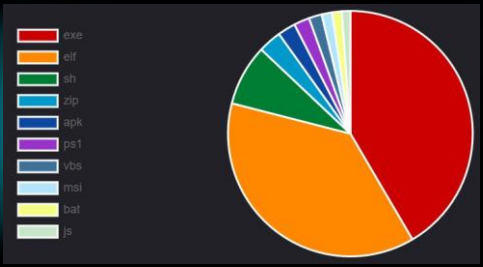
PUBLIC

Index

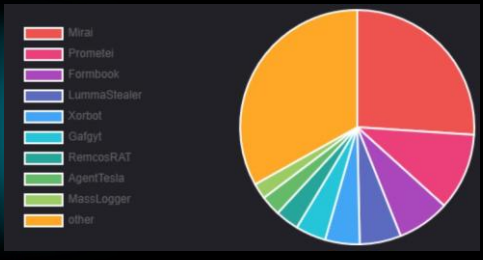
Global Weekly Threat Overview

Threat actors with ties to China have been observed using an updated version of a backdoor called COOLCLIENT in cyber espionage attacks in 2025 to facilitate comprehensive data theft from infected endpoints. The activity has been attributed to Mustang Panda (aka Earth Preta, Fireant, HoneyMyte, Polaris, and Twill Typhoon) with the intrusions primarily directed against government entities located across campaigns across Myanmar, Mongolia, Malaysia, and Russia. COOLCLIENT was typically delivered alongside encrypted loader files containing encrypted configuration data, shellcode, and in-memory next-stage DLL modules. These modules relied on DLL side-loading as their primary execution method, which required a legitimate signed executable to load a malicious DLL.

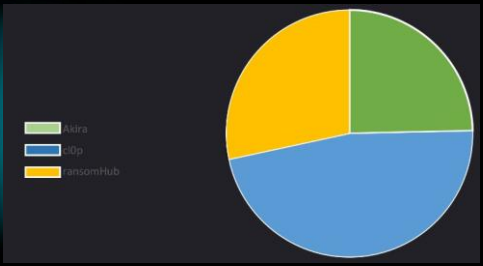
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Microsoft issued out-of-band security patches for a high-severity Microsoft Office zero-day vulnerability exploited in attacks. The vulnerability, tracked as CVE-2026-21509, carries a CVSS score of 7.8. It has been described as a security feature bypass in Microsoft Office. Reliance on untrusted inputs in a security decision in Microsoft Office allows an unauthorized attacker to bypass a security feature locally. The update addresses a vulnerability that bypasses OLE mitigations in Microsoft 365 and Microsoft Office, which protect users from vulnerable COM/OLE controls. Successful exploitation of the flaw relies on an attacker sending a specially crafted Office file and convincing recipients to open it.

Global Weekly Notable One

Modify Authentication Process: defense evasion

Telnet, a legacy network protocol from the 1970s, enables remote terminal access over TCP port 23 by transmitting plain-text data streams between client and server. Its simplicity once made it vital for Unix-like systems and early network management, but it lacks encryption, exposing credentials and commands to interception via packet sniffing or man-in-the-middle attacks. Telnet remains critically important today due to its persistence in legacy IoT devices, industrial systems, and unpatched embedded Linux environments serving as prime targets for botnets and ransomware.

The latest high-profile vulnerability, CVE-2026-24061, affects GNU InetUtils telnetd (versions 1.9.3 to 2.7). This critical authentication bypass (CVSS 9.8) exploits Telnet's option negotiation phase per RFC 854 and RFC 1572's NEW-ENVIRON suboption (IAC SB NEW-ENVIRON SEND/INFO VAR VALUE). Vulnerable telnetd implementations propagate unsanitized client-supplied environment variables directly to the underlying /usr/bin/login process invoked with -a or --login flags.

Threat Hunting Activity

TACTIC

Defense Evasion

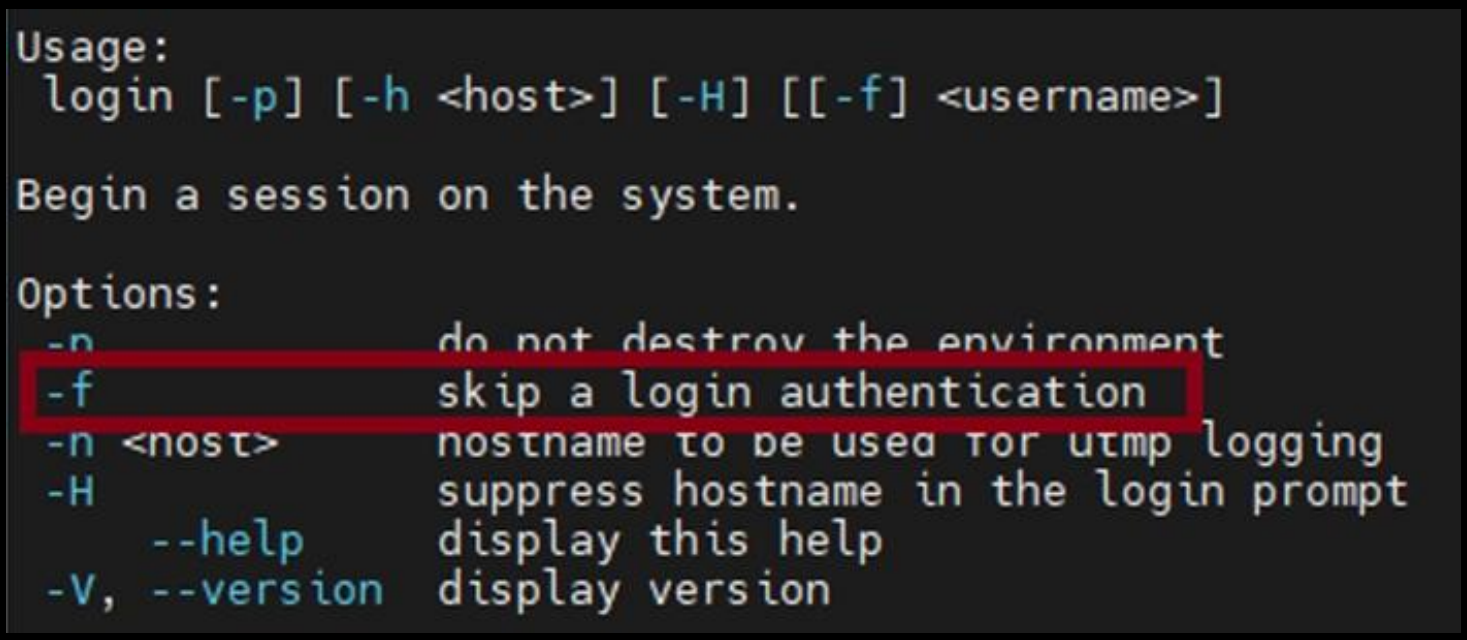
TECHNIQUES

T1556 – Modify Authentication Process

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using Valid Accounts.

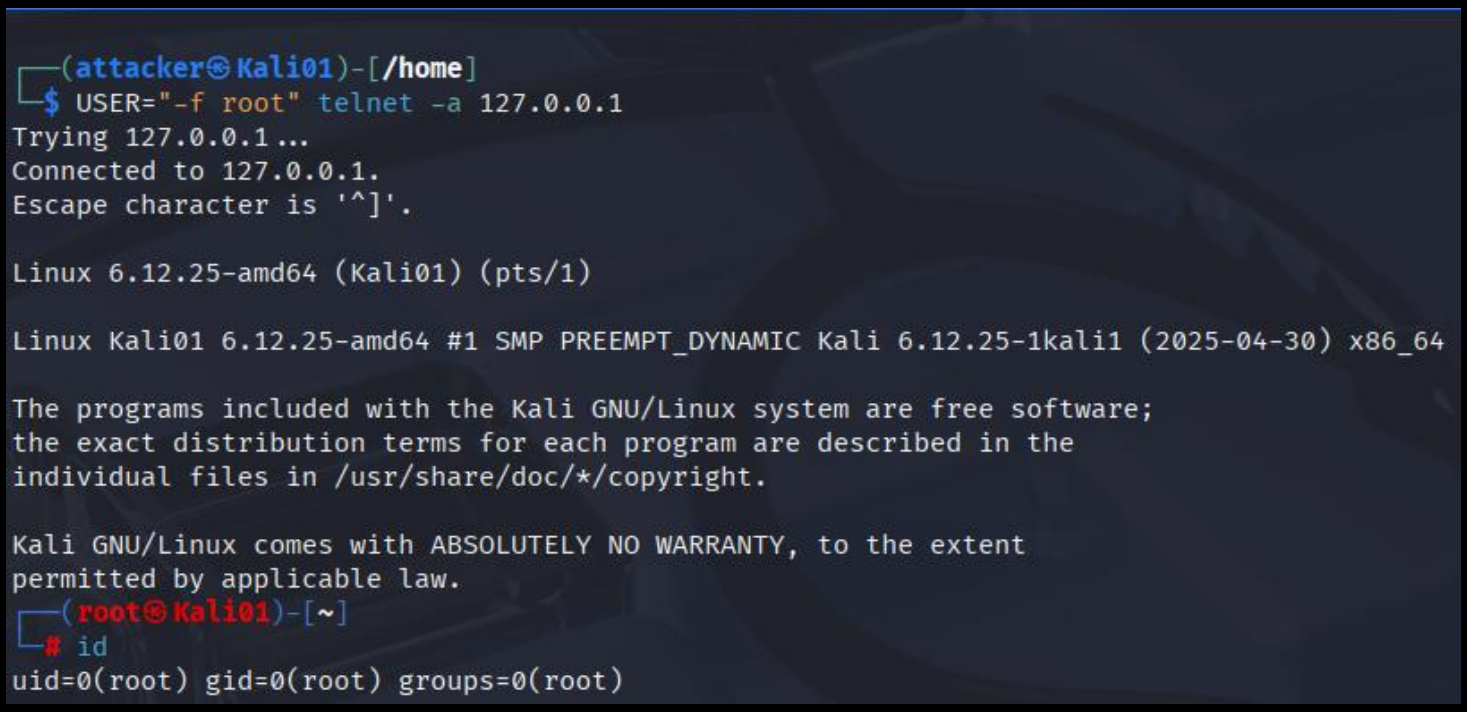
Threat Hunting Activity

During session initialization, attackers craft Telnet sequences that inject environment variables like USER into the negotiation phase. The server-side telnetd relays these unaltered to login, which misinterprets flags. Looking at login binary flags, -f can be leverage to authenticate as other users skipping authentication checks.



Threat Hunting Activity

Exploitation of the vulnerability results in an unrestricted root shell accessible solely via network reachability to TCP/23 (or alternate ports), without requiring valid credentials.



Threat Hunting Activity

Detection can be made monitoring process events

```
type=EXECVE msg=audit(1770126030.392:3673): argc=5 a0="sudo" a1="grep" a2="
-E" a3="EXE_NAME=telnet.*a1=-f|a1=-f.*EXE_NAME=login" a4="/var/log/audit/au
dit.log"
type=EXECVE msg=audit(1770126030.404:3679): argc=4 a0="grep" a1="-E" a2="EX
E_NAME=telnet.*a1=-f|a1=-f.*EXE_NAME=login" a3="/var/log/audit/audit.log"
type=EXECVE msg=audit(1770126129.484:4535): argc=5 a0="sudo" a1="grep" a2="
-E" a3="EXE_NAME=telnet.*a1=-f|a1=-f.*EXE_NAME=login" a4="/var/log/audit/au
dit.log"
type=EXECVE msg=audit(1770126141.124:4657): argc=4 a0="grep" a1="-E" a2="EX
E_NAME=telnet.*a1=-f|a1=-f.*EXE_NAME=login" a3="/var/log/audit/audit.log"
```

PUBLIC