Alloy Taurus and APT29

C-Suite level threat review by applicable business area addressing active threats.

Adversaries are continuously honing their skill sets to enhance the efficacy of their attacks. The two threat actors described in this report, Alloy Taurus and APT29, are demonstrations of such resourcefulness. Alloy Taurus expanded its capabilities to infect Linux systems, and APT29 employed new and modified tools in its recent campaign. Moreover, both threat actors are advanced persistent threats (APT). APTs are top-tier threat actors that employ sophisticated techniques and have vast resources supporting them. Both Alloy Taurus and APT29 are backed by nation-states.

Alloy Taurus (other aliases include Gallium and Softcell):

Alloy Taurus is an APT actor affiliated with the Chinese government that conducts cyberespionage. It targets telecommunications, financial, military and government entities in Asia, Europe, and Africa. Alloy Taurus has recently expanded its capabilities to infect not only Windows but also Linux systems through its malware PingPull, which is a remote access trojan (RAT).

APT29 (other aliases include Cozy Bear and Nobelium):

APT29 is linked to Russian intelligence agencies. A recent campaign targeting government and diplomatic entities in NATO, European Union, and African countries has been attributed to APT29. The goal of this campaign is information collection. APT29 has increased the effectiveness of its attacks in this campaign by utilizing new tools and modifying pre-existing tools to better evade detection.

Alloy Taurus

Threat Level: High

Attack:

Alloy Taurus is known to leverage external remote services to gain initial access to organizations (MITRE T1133) and use PingPull for command and control. The adversary was first observed employing PingPull malware in 2021. The malware enables the threat actor to set-up a reverse shell, remotely connecting Alloy Taurus to the victim's device (MITRE T1059). PingPull is stealthy; it can leverage 3 protocols for command-and-control (C2), raw TCP, ICMP and HTTP(S) (MITRE T1095 and MITRE T1071.001), and mimic legitimate services to avoid detection (MITRE T1036). The malware can then exfiltrate data over a C2 channel (MITRE T1041). The malware performs activities on the file system which includes, but is not limited to, read, write, delete, list folder contents, enumerate storage volumes, and create directory. The Linux version has similar functionality to that of the earlier Windows version.

Remediation:

- Implement comprehensive egress filtering.
- Apply security protections to Linux systems. Examples include ensuring your endpoint detection and response (EDR) tool protects Linux systems and segmenting Linux systems commensurate with risk.
- Monitor IPv6 traffic. PingPull utilizes IPv6 which is an obfuscation tactic since security personnel tend to scrutinize IPv6 traffic less.

APT29

Threat Level: High

Attack:

In APT29's recent campaign, initial access is gained via targeted spear-phishing emails that contain malicious links (MITRE T1566) directing users to a compromised website storing ENVYSCOUT, APT29's signature malicious script. The script utilizes a technique called HTML smuggling (MITRE T1027.006), which is when adversaries hide malicious payloads inside HTML files to evade detection. An additional evasion technique utilized in this campaign is using less common file extensions like .IMG, .ZIP, .LNK and .ISO to deliver malware. To enhance the efficacy of its campaign, APT29 is using and combining new and modified tools such as SNOWYAMBER, HALFRIG and QUARTERRIG. SNOWYAMBER and QUARTERRIG are malware droppers that assess a victim's environment to confirm it's a desired target (MITRE T1016) before delivering Cobalt Strike, a remote access tool. HALFRIG is a stager for Cobalt Strike, running it automatically. QUARTERRIG and HALFRIG are new tools. While SNOWYAMBER predated this campaign (it was first observed in October 2022), a new variant with additional anti-detection measures emerged.

Remediation:

- Security analysts should consider blocking users' ability to mount disk images on the file system. While most users do not need this capability, users that do should have a privileged role for this activity which is then actively monitored.
- Ensure that your organization blocks the ability to start-up executable files from unusual locations.
- Implement a comprehensive security awareness training program that prepares users to recognize and report suspicious emails.

Alloy Taurus Details:

- **In-depth overview of PingPull Windows functionality:** https://unit42.paloaltonetworks.com/pingpull-gallium/
- **Breakdown of PingPull Linux:** https://unit42.paloaltonetworks.com/alloy-taurus/

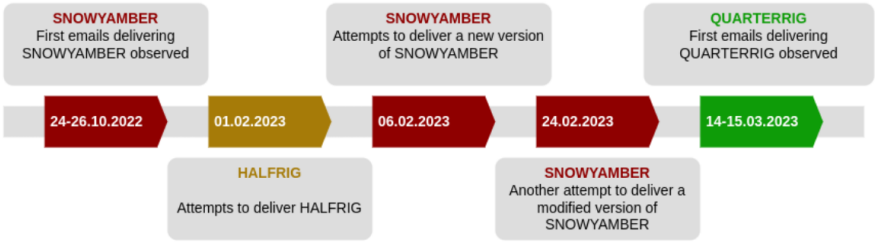
APT29 Details:

- **Advisory on APT29 by Poland's Military Counterintelligence Service and its Computer Emergency Response Team:** https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
- **High-level overview of APT29's recent campaign:** https://www.csoonline.com/article/3693252/russian-cyberspies-hit-nato-and-eu-organizations-with-new-malware-toolset.html

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity

A timeline of APT29's use of and modification of malicious tools during its most recent campaign



Source: https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services