SECURITY ADVISORY

November, 2024

CVE-2022-1040

Pygmy Goat Malware

Breaches and Hijacks Sophos Firewalls

Context

"Pygmy Goat" malware is a highly sophisticated backdoor payload engineered to facilitate unauthorized access to Linux-based network devices, with a particular focus on Sophos XG firewall appliances. Discovered as part of an ongoing series of cyber-espionage operations linked to Chinese state-sponsored threat actors, the malware is emblematic of the broader Pacific Rim campaign, a targeted assault on critical infrastructure and high-value entities. First identified by the UK's National Cyber Security Centre (NCSC), these attacks exploit known vulnerabilities, such as CVE-2022-1040, in edge devices and network appliances—especially those used by government agencies, critical infrastructure sectors, and private enterprises. Once deployed, "Pygmy Goat" grants attackers persistent, covert access to compromised systems, facilitating exfiltration of sensitive data and enabling remote control of the infected devices. The malware employs advanced evasion techniques, including the use of encrypted ICMP packets for stealthy communication and disguising malicious activity as legitimate SSH traffic, thereby circumventing traditional detection mechanisms.

Mitigation

Defending against Pygmy Goat requires proactive measures including prioritizing patches for exposed vulnerabilities:

Restrict Management Traffic: Limit SSH, HTTP/HTTPS, ICMP, and SNMP to trusted IPs only to prevent unauthorized access.

Segment Management Network: Isolate management traffic in a separate security zone using OOB access to ensure secure, dedicated paths for device management.

Limit Outbound Traffic: Restrict outbound traffic from the firewall's public IP to only necessary connections, reducing exposure to external threats.

Apply Security Controls to All Exposed Assets: Extend these principles to all exposed network devices (e.g., routers, VPN termination devices) to ensure consistent, comprehensive security across your infrastructure.

Technical Details

The Pygmy Goat malware is delivered to compromised devices, like Sophos XG firewalls, primarily through the following method:

Malware Delivery

1. Exploitation of Vulnerabilities:

The malware is initially delivered to the device after exploiting unpatched vulnerabilities in the firewall, such as those in the SSH service. The malware is likely deployed via a remote attack, possibly exploiting vulnerabilities like **CVE-2022-1040**, which allows attackers to gain unauthorized access to the firewall system.

1. Malicious Payload Injection via LD_PRELOAD

Once the attacker has access, they use the LD_PRELOAD environment variable to inject a malicious ELF shared object (**libsophos.so**) into the SSH daemon (sshd) process. This allows the malware to hook into the SSH service and execute its functions covertly, without being easily detected.

Persistence Mechanism

The attacker ensures that the Pygmy Goat malware maintains persistence on the system by setting the LD_PRELOAD variable in system startup scripts, which ensures that the malicious shared object is automatically loaded each time the SSH service (or the system) is restarted.

C2 Communication via ICMP Port Knocking

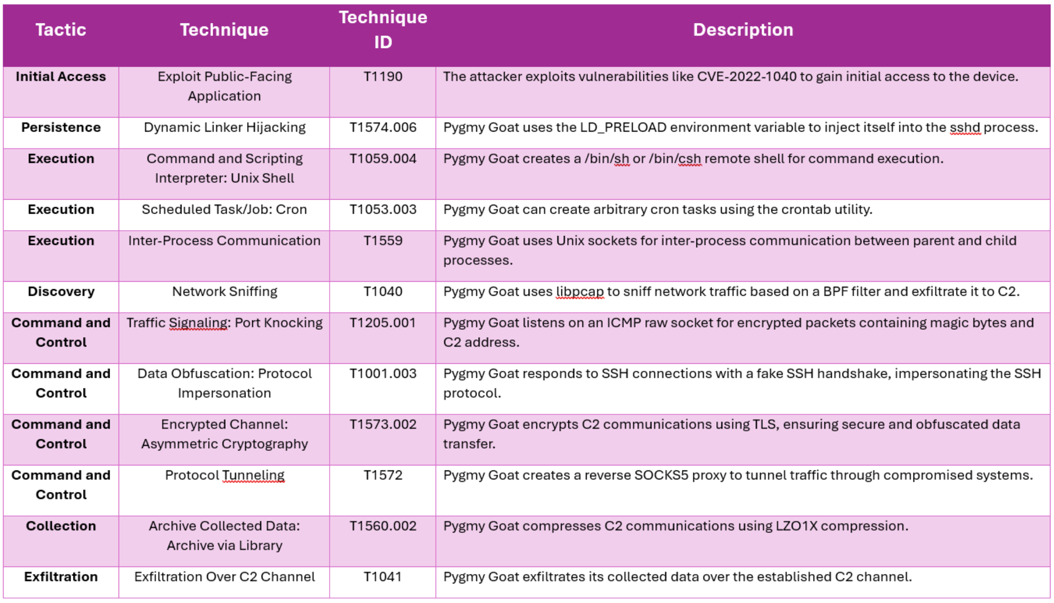
To establish communication with the command-and-control (C2) server, the malware creates a raw ICMP socket to listen for specially crafted ICMP packets. These packets contain an AES-encrypted payload that specifies the TCP callback IP address and port, which the malware uses to connect to the attacker's server.

SSH Backdoor and C2 Interaction

The malware hooks into the accept() function of the sshd binary to monitor incoming SSH traffic for a specific protocol version string (SSH-2.0-OpenSSH_5.3p1\r\n1). If the expected traffic is detected, the malware forwards the connection to a backdoor channel, allowing the attacker to remotely control the device over the compromised SSH connection.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Pygmy Goat campaign :



Tactic	Technique	Technique ID	Description
Initial Access	Exploit Public-Facing Application	T1190	The attacker exploits vulnerabilities like CVE-2022-1040 to gain initial access to the device.
Persistence	Dynamic Linker Hijacking	T1574.006	Pygmy Goat uses the LD_PRELOAD environment variable to inject itself into the sshd process.
Execution	Command and Scripting Interpreter: Unix Shell	T1059.004	Pygmy Goat creates a /bin/sh or /bin/csh remote shell for command execution.
Execution	Scheduled Task/Job: Cron	T1053.003	Pygmy Goat can create arbitrary cron tasks using the crontab utility.
Execution	Inter-Process Communication	T1559	Pygmy Goat uses Unix sockets for inter-process communication between parent and child processes.
Discovery	Network Sniffing	T1040	Pygmy Goat uses libpcap to sniff network traffic based on a BPF filter and exfiltrate it to C2.
Command and Control	Traffic Signaling: Port Knocking	T1205.001	Pygmy Goat listens on an ICMP raw socket for encrypted packets containing magic bytes and C2 address.
Command and Control	Data Obfuscation: Protocol Impersonation	T1001.003	Pygmy Goat responds to SSH connections with a fake SSH handshake, impersonating the SSH protocol.
Command and Control	Encrypted Channel: Asymmetric Cryptography	T1573.002	Pygmy Goat encrypts C2 communications using TLS, ensuring secure and obfuscated data transfer.
Command and Control	Protocol Tunneling	T1572	Pygmy Goat creates a reverse SOCKS5 proxy to tunnel traffic through compromised systems.
Collection	Archive Collected Data: Archive via Library	T1560.002	Pygmy Goat compresses C2 communications using LZO1X compression.
Exfiltration	Exfiltration Over C2 Channel	T1041	Pygmy Goat exfiltrates its collected data over the established C2 channel.

Cyber Threat Intelligence

The Pacific Rim cyber-espionage campaign, attributed to Chinese state-sponsored threat actors, has been targeting government agencies, critical infrastructure, and technology partners in the West, with a primary focus on gaining access to edge devices such as firewalls, routers, and VPN termination points. These devices have become key entry points for espionage activities, as they are integral to securing networks and communications. The campaign, active since at least 2018, has evolved in both sophistication and aggression, with a clear goal of cyber-espionage and data exfiltration.

The attackers, believed to be a group of Chinese-speaking operatives, have primarily targeted Sophos XG firewalls, leveraging vulnerabilities such as CVE-2022-1040 to gain initial access to compromised devices. The Pygmy Goat malware, identified in 2022, has become a key tool in these attacks. Designed for Linux-based devices, it provides attackers with a persistent backdoor and enables them to escalate privileges, maintain long-term access, and exfiltrate sensitive information. The malware's advanced persistence, evasion, and remote access capabilities make it a potent tool for sustained cyber-espionage campaigns.

CyberStash analysts predict that the Pygmy Goat malware will likely evolve in the coming months. Given the attackers’ demonstrated ability to adapt their techniques, it is expected that future iterations of the malware will incorporate more advanced evasion techniques to bypass detection, as well as enhanced C2 communication channels to improve reliability and reduce the chances of disruption. Additionally, the attackers are likely to target more varied and diverse network devices.

The long-term objectives of this campaign appear to be intelligence gathering, data exfiltration, and potentially creating avenues for future attacks. The Pacific Rim operation exemplifies how advanced state-sponsored threat actors can adapt to and exploit vulnerabilities in critical infrastructure, posing a significant and ongoing threat to both government entities and private-sector organizations.

References

IOCs:

- https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/pygmy-goat/ncsc-mar-pygmy-goat.pdf

Public Intelligence:

- https://www.securityweek.com/ncsc-details-pygmy-goat-backdoor-planted-on-hacked-sophos-firewall-devices/
- https://www.bleepingcomputer.com/news/security/custom-pygmy-goat-malware-used-in-sophos-firewall-hack-on-govt-network/
- https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/pygmy-goat/ncsc-mar-pygmy-goat.pdf
- https://cybersecuritynews.com/pygmy-goat-network-device-backdoor/