PALO ALTO NETWORKS PLATFORM VS. REAL-WORLD ATTACKS

Rocke Threat Group Campaign Use Case

In a rapidly evolving digital landscape, IT leaders are struggling to keep up with business demands while maintaining risk mitigation. With the internet of things (IoT) and bring-your-own-device (BYOD) policies creating new threat vectors, and sprawls of disconnected tools increasing complexity, it's no surprise that cybersecurity professionals are overwhelmed. Today's security teams often spend more time testing, integrating, and operating disconnected tools than actually stopping threats. This significantly increases business risk and decreases efficiency. Moreover, with a greater dispersion of data across multiple locations and devices, deployment seems never-ending.

Security demands a new approach. Deploying the right security tools with tight integrations and automation can help alleviate the manual lift needed to operate multiple consoles and complete routine tasks. Enter Palo Alto Networks. With a complete suite of products that protect businesses on the network, endpoint, and in the cloud, cybersecurity professionals can spend more time on detection, analytics, automated prevention, and rapid response instead of operating disparate technologies.

To understand how Palo Alto Networks products protect your organization throughout the attack lifecycle, this brief provides two use cases centered on the Rocke group, a Chinese threat actor first spotted in April 2018 that specializes in cryptojacking. This group is financially motivated and known for leveraging Git repositories to mine Monero cryptocurrency in compromised Linux-based systems.

The Rocke group's known techniques include:

- T1190 Exploit Public-Facing Application
- T1078 Valid Accounts
- T1168 Local Job Scheduling
- T1110 Brute Force
- T1222 File Permissions Modification
- T1021 Remote Services
- T1064 Scripting
- T1045 Software Packing
- T1071 Standard Application Layer Protocol
- T1099 Timestomp
- T1055 Process Injection
- T1036 Masquerading
- T1496 Resource Hijacking

Use Case No. 1: Rocke Group Cryptojacking Campaign

The Rocke group developed a new coinmining malware that penetrates vulnerable Linux servers. The main goal was to gain full administrative rights over hosts and abuse those permissions by uninstalling cloud security products in the same way a legitimate administrator would. This would then enable the malware to evade detection and infect the system. After agent-based security products are uninstalled, the threat group drops CoinMiner malware to mine cryptocurrency on the compromised server. Unit 42 analyzed NetFlow data from December 2018 to June 16, 2019, and found that 28.1% of cloud environments surveyed had at least one fully established network connection with at least one known Rocke command-and-control (C2) domain.

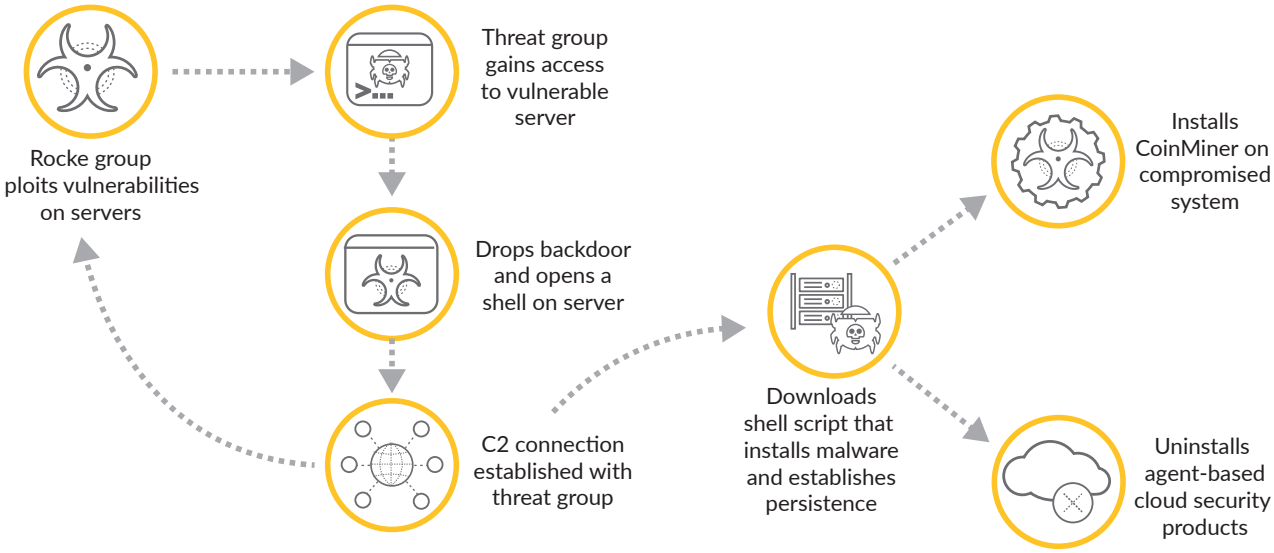

Figure 1: Cryptojacking attack flow

How Palo Alto Networks prevents this threat:

- **Prisma™ Cloud** dynamically discovers cloud resources; detects risky configurations; and identifies network threats, suspicious user behavior, malware, data leakage, abnormal CPU usage, and host vulnerabilities. Administrators are alerted to respond.
- **VM-Series** Virtualized Next-Generation Firewalls identify the malware, using **Threat Prevention**, DNS Security, and **WildFire,** and apply application-specific policies that block exploits, malware, and previously unknown threats from infecting the cloud.
- **URL Filtering** identifies and tags the Rocke group's C2 domains and IPs from the campaign as malicious. PAN-DB receives malicious URL and IP information from **URL Filtering**, preventing further C2 connections.
- **WildFire®** malware prevention service identifies new threats like Xbash and CoinMiner with advanced analysis, machine learning, and shared threat intelligence. **AutoFocus™** contextual threat intelligence service then tracks the malware, and the **VM-Series** stops it.

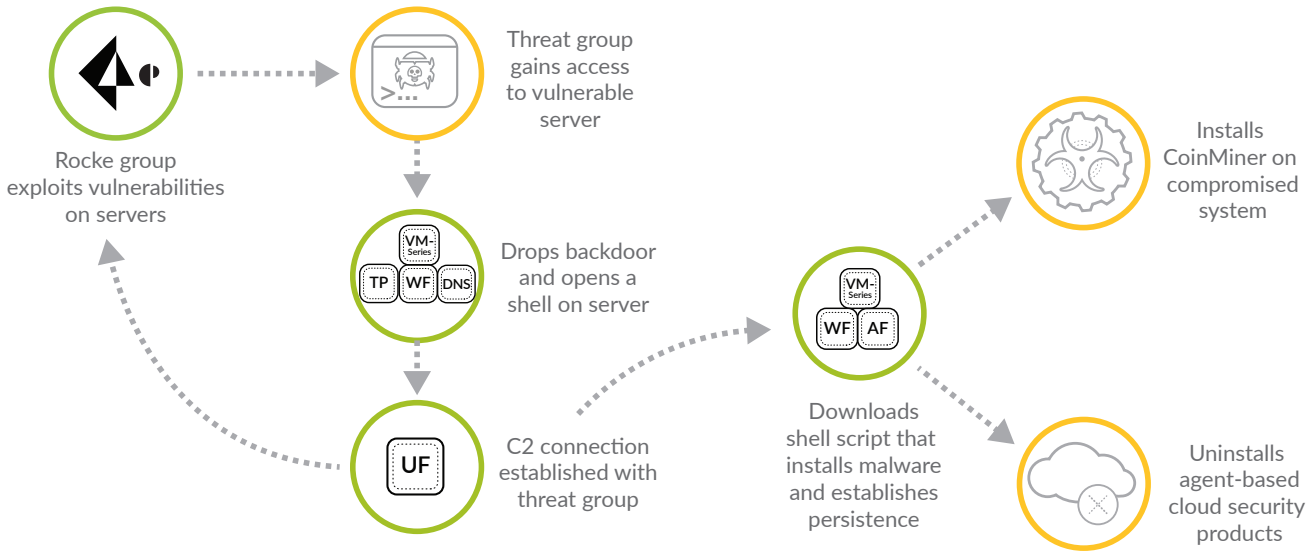

Figure 2: Palo Alto Networks in the cryptojacking attack flow

Use Case No. 2: Rocke Group Xbash Campaign

Xbash is ransomware with coinmining capabilities that targets Linux and Microsoft Windows® servers. It has self-propagating capabilities, demonstrating worm-like characteristics similar to WannaCry or Petya/NotPetya. These capabilities enable it to spread very quickly within an organization's network. While tracking Xbash, Rocke's bitcoin wallet contained 0.964 BTC (equivalent to US$10,130 today), which had been wired from approximately 48 victims to the C2 IP address. Here's what you should know about how this ransomware operates:

- Xbash spreads by attacking weak passwords and unpatched vulnerabilities.
- Xbash is data-destructive, destroying Linux-based databases as part of its ransomware capabilities.

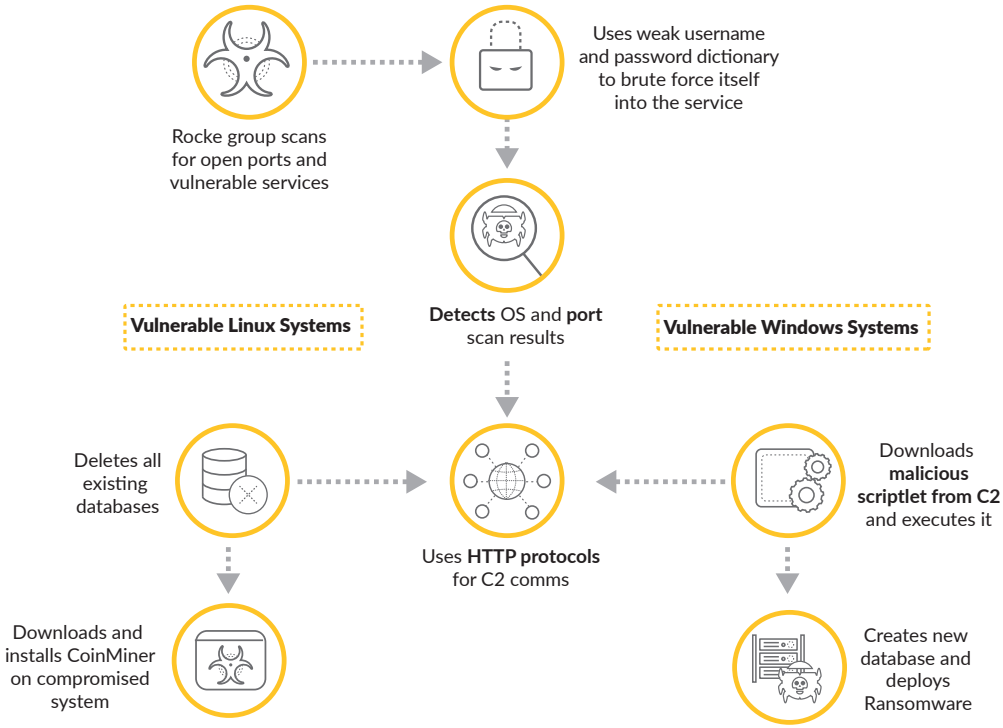

Figure 3: Xbash attack flow

How Palo Alto Networks prevents this threat:

- **Prisma Cloud** uses machine learning-based analysis to identify data risks, such as exposed ports or services with excessive privileges.
- All three Xbash vulnerabilities have been identified and are prevented via the **Threat Prevention** service and enforced by the **VM-Series**.
- **VM-Series** firewalls contain a Vulnerability Protection profile that, if enabled, includes signatures to protect against brute-force attacks.
- **URL Filtering** identifies and tags the Rocke group's C2 domains and IPs from the campaign as malicious. PAN-DB receives malicious URL and IP information from **URL Filtering**, preventing further C2 connections.
- For Linux machines:
  - **Traps™** endpoint protection and response uses behavior-based protection to identify the Linux executable and prevent it from installing.
  - **Traps** ransomware prevention safeguards against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before data loss can occur.
- For Windows machines:
  - **WildFire** uses dynamic analysis, static analysis, machine learning, and bare metal analysis to detonate the executable and identify unknown malware.
  - **Traps** uses local analysis and behavior-based prevention, and integration with **WildFire**, to quickly identify and prevent CoinMiner from compromising the system.
- **AutoFocus** tracks the malware for further prevention.

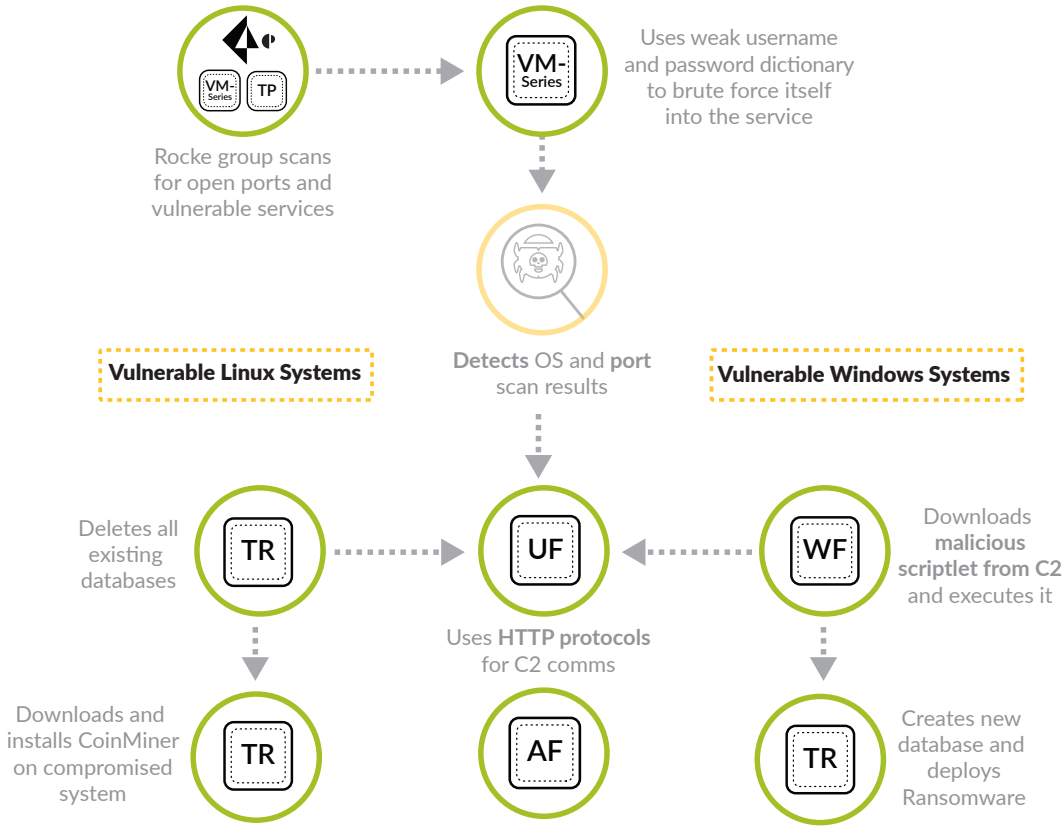

Figure 4: Palo Alto Networks in the Xbash attack flow

Regardless of where the Rocke group gets in the attack lifecycle, you can be confident that Palo Alto Networks will protect your data and mitigate risk. To stay up to date with the Rocke group's activities, read the recent blog post from Unit 42, Rocke'in the NetFlow, which details the latest campaign from this threat actor. You can also check out these other resources:

- Rocke Group Playbook
- Cloudy with a Chance of Entropy
- Malware Used by "Rocke" Group Evolves to Evade Detection by Cloud Security Products
- Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows

UNIT 42

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

palo-alto-networks-platform-vs-real-world-attacks-rocke-threat-group-campaign-uc-100719