Targeting Linux-Based Multi-Cloud Environments

Insights from the new technical threat report from the VMware Threat Analysis Unit™: “Exposing Malware in Linux-Based Multi-Cloud Environments.”

Focus on Linux

- 90% of the cloud runs on Linux
- 79% of the most popular websites are powered by Linux
- Linux has become the most common OS in multi-cloud environments

Threat Deep Dive

1. Implants and Remote Access Tools (RATs)

- 14,000 active Cobalt Strike team servers on the internet since the end of February 2020
- Over 56% of Cobalt Strike customer IDs are cracked and leaked
- Over 50% of Cobalt Strike users are using illegitimately obtained versions of the commercial software

2. Ransomware

- Nine ransomware families that target Linux systems were analyzed by the VMware Threat Analysis Unit.
- The report found that defense evasion (59%) was the most common tactic used by the ransomware families examined.
- Ransomware attacks against cloud deployments are targeted, not opportunistic.

3. Cryptomining or Cryptojacking

- 89% of the cryptominer programs analyzed relied on XMRig-related libraries
- Cryptojacking attacks focus on monetizing stolen CPU cycles to mine cryptocurrencies

Cybercriminals use implants to perform two types of attacks

RAT Spotlight: Cobalt Strike

- Nine ransomware families that target Linux systems were analyzed by the VMware Threat Analysis Unit.
- The report found that defense evasion (59%) was the most common tactic used by the ransomware families examined.
- Ransomware attacks against cloud deployments are targeted, not opportunistic.

Most cryptojacking attacks focus on mining the Monero cryptocurrency (or XMR).

Cyber Vigilance Is Required

Secure your multi-cloud.

DOWNLOAD THE FULL REPORT