vmware

3 Cyber Threats

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

In the past **5** years, Linux has become the most common OS in multi-cloud environments

Threat Deep Dive

1 Implants and Remote Access Tools (RATs)

RAT Spotlight: Cobalt Strike

- **OVER 14,000** active Cobalt Strike team servers on the internet since the end of February 2020[1]
- **56%** of Cobalt Strike customer IDs are cracked and leaked[1]
- **>50%** of Cobalt Strike users are using illegitimately obtained versions of the commercial software[1]

Cybercriminals use implants to perform two types of attacks

- Deploy cryptomining components
- Execute ransomware

2 Ransomware

Ransomware = Real-World Threats

Nine ransomware families that target Linux systems were analyzed by the VMware Threat Analysis Unit.

9

The report found that defense evasion (59%) was the most common tactic used by the ransomware families examined.[2]

59%

Ransomware attacks against cloud deployments are targeted, not opportunistic.

Unlike ransomware, the advantage of targeting cryptocurrencies is that successful attacks can be immediately and directly turned into (cyber) cash.

3 Cryptomining or Cryptojacking

Cryptojacking in Linux-Based Systems

- **XMR** Most cryptojacking attacks focus on mining the Monero cryptocurrency (or XMR)[1]
- **89%** of the cryptominer programs analyzed relied on XMRig-related libraries[1]
- Cryptojacking attacks focus on monetizing stolen CPU cycles to mine cryptocurrencies

Cyber Vigilance Is Required

Secure your multi-cloud.

DOWNLOAD THE FULL REPORT

1. VMware. "Exposing Malware in Linux-Based Multi-Cloud Environments." 2022.
2. VMware. "Ransomware Attacks and Techniques – Analysis from VMware Threat Report." Roger Park. March 9, 2022.