

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

RAT Spotlight: Cobalt Strike

1 Implants and Remote Access Tools (RATs)



- OVER 14,000 active Cobalt Strike team servers on the internet since the end of February 2020¹
- 56% of Cobalt Strike customer IDs are cracked and leaked¹
- >50% of Cobalt Strike users are using illegitimately obtained versions of the commercial software¹

Deploy cryptomining components → Cybercriminals use implants to perform two types of attacks → Execute ransomware

Ransomware = Real-World Threats

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.²

Ransomware attacks against cloud deployments are targeted, not opportunistic.

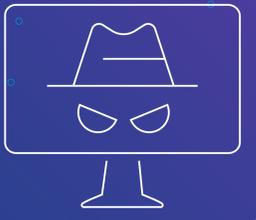
- 9 ransomware families target Linux systems
- 59% of ransomware attacks use defense evasion
- 2 types of attacks performed by cybercriminals using implants

2 Ransomware



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 libraries¹
- 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.