Top Linux Cloud Threats of 2020

By Intezer

Published: 2020-12-21 · Archived: 2026-04-05 13:14:21 UTC

We tagged 2019 as The Year of the Linux Threat. That trend continued in 2020 with high profile APTs launching ELF malware, and Linux versions of Windows threats emerging for the first time.

By some estimates, 2020 saw several years worth of digital transformation in just a few months. Prior to the pandemic, cloud computing was already becoming the cornerstone of technological innovation in our daily lives. Even more traditional, non-tech-oriented industries, such as banking and manufacturing, were taking the plunge and migrating to the cloud to reap the numerous benefits it offers.

From a security vantage, the increased reliance on the cloud has also meant that attackers have increased their appetite for Linux. Linux is the dominant operating system in the cloud. With the increased use of Linux workloads and containers in the cloud, it comes as no surprise that over 50% of workloads in Azure use Linux. Picking up on this trend, 2020 saw threat actors develop new Linux threats and also sharpen their existing ELF malware.

APTs

APTs targeting Linux environments are not new. We previously documented how APTs have targeted this operating system for a decade, mainly attributed to Russia, China and North Korea. In July, our researchers disclosed a previously undetected Linux version of WellMail, a malware the UK National Cyber Security Centre (NCSC) attributed to Russia's APT29.

From Windows to Linux

2020 also saw cybercrime groups targeting Linux. One of the most significant discoveries of the year was this Linux sample of TrickBot, which is commonly known for targeting Windows platforms.

IPStorm is another example. This Windows malware first identified in 2019 resurfaced in 2020 almost exclusively targeting Linux machines. The discovery of these Linux threats is further evidence that malware developers are moving to the cloud.

Updates to Existing Linux Malware

This year also saw updates made by threat actors who we already knew had Linux malware, such as Penquin (Turla) and QNAPCrypt. This proved that attackers are keeping their existing malware sharp and active in addition to developing new tools.

Golang

2020 was a bit like playing Whac-A-Mole. Threat actors, from APTs to botnet developers, turned to Golang as their programming language of choice to develop cross-platform malware that targeted both Windows and Linux. Just when you whacked one malware written in Golang, another one came rearing its ugly head.

Golang is incredibly efficient for developing malware that targets various operating systems. Since Golang files are compiled together with their runtime code, they are much heavier than native files. This makes it difficult for Antivirus engines to analyze them and allows Golang files to often bypass detection.

The good news is that you can detect cross-platform malware with the code reuse feature for Golang in Intezer Analyze. Here is an example of a Carbanak Linux sample, written in Golang, which at the time of its discovery was fully undetected in VirusTotal.

Top Linux Cloud Threats of 2020

The following timeline recaps the notable Linux malware discoveries of the year. It includes both newly discovered malware and previously reported tools that were updated in 2020.

Wrap-Up

You can call 2020 a lot of things. Maybe **The Year of the Gopher** is best fitting. It's important to be on the lookout for threats written in Golang because they are often multi-platform and can target different environments.

If 2021 is anything like the previous two years, we can expect more Windows threats to come out with Linux malware. ELF malware analysis is a skill that you will want to add to your arsenal, which is why we initiated this ELF Malware Analysis 101 series for you to practice hands-on. Of course you can always use Intezer Analyze to accelerate detection and classification of ELF malware.

Stay Protected Against Linux Threats

We also invite you to create a free Intezer Protect community edition account. Intezer Protect is a runtime Cloud Workload Protection Platform built specifically to protect cloud environments—including Linux servers, VMs, containers, k8s, CaaS and FaaS—against the aforementioned threats.

Hats off to the research community for the exceptional work they did this year **investigating the latest Linux threats.**

- NOTROBIN
- Cloud Snooper
- TSCookie, BlackTech
- PWNLNX, Winnti
- Kinsing
- Turla
- Kaiji
- ManusCrypt, Lazarus
- Doki
- AgeLocker
- WellMess & WellMail, APT29
- TrickBot
- Drovorub
- Carbanak
- TeamTNT
- FritzFrog
- Dalcs, Lazarus
- IPStorm
- RansomEXX
- PLEAD, BlackTech
- Stantinko
- PGMiner
- Prometei
