

# Malware is targeting Linux — and winning!

The perception in the industry is that Linux is “safe” from malware. However, it is in fact the opposite. Malware is targeting Linux business users – and predominantly for criminal aims.



# Linux security is now critical



Linux malware accounts for more than 36% of all new malware detections<sup>1</sup>

Currently, there are at least 21 malware families targeting Linux Servers<sup>2</sup>



Fewer vulnerabilities but far fewer protections (largely open source)<sup>3</sup>

# Barriers to Linux server security



1

## Market misperception that Linux is “safe”

Linux malware is evolving to be more lethal and more targeted against businesses<sup>4,6</sup>



2

## Lack of telemetry

Few security packages for businesses, many of which do not share telemetry, making Linux-wide insights unavailable<sup>5</sup>



3

## Linux defenses are siloed

Malware squeezes between gaps and defenses<sup>4</sup>

# Linux malware is rapidly evolving

99% of Linux malware targets businesses for criminal aims<sup>6</sup>

## Cloudsnooper

Allows exfiltration, command and control communication, and more<sup>4</sup>

Traced to successful AWS attack in early 2020<sup>4</sup>

## QNAPCrypt

Linux ransomware that targets network-attached storage<sup>4</sup>

## GonnaCry

Ransomware that has evolved along the same path as WannaCry and Petya<sup>4</sup>

## HiddenWasp

Allows remote control of infected systems<sup>4</sup>

Consists of a trojan, a user-mode rootkit, and an initial deployment script<sup>4</sup>

## FBOT

Variant of the infamous Mirai botnet that targets Linux IoT devices<sup>4</sup>

# Introducing security built for Linux

## Malwarebytes Endpoint Protection for Servers on Linux



Keeps Linux servers working with a full, integrated suite of malware detection, protection, and remediation capabilities.



Provides protection against exploits, ransomware, PUPs, and PUMs that impact Linux.



Leverages telemetry across business platforms—including Linux servers—and consumer devices.



Certified with Red Hat Enterprise Linux.

### LEARN MORE

Visit [www.malwarebytes.com/business](https://www.malwarebytes.com/business)

#### Sources

1. "Linux malware gaining favor among cybercriminals," SC Magazine, June 28, 2017, <https://www.scmagazine.com/home/security-news/malware/linux-malware-gaining-favor-among-cybercriminals/>.  
Source report is: Watchguard's Internet Security Report, Q1 2017, Watchguard <https://www.guardsite.com/51072/new-research-shows-cybersecurity-battleground-shifting-to-linux-and-web-servers>.
2. "ESET discovers 21 new Linux malware families," ZDNet, December 6, 2018, <https://www.zdnet.com/article/eset-discovers-21-new-linux-malware-families/>.
3. "Childhood's End: Attackers Increasingly Take Aim at Linux Systems," Linux Journal reprint, 2017, <https://static.helpsystems.com/powertech-x/pdfs/guides/pt-x-childhoods-end-geek-guide.pdf>.
4. "Linux Malware: The Truth About This Growing Threat," Linux Security, April 3, 2020, <https://linuxsecurity.com/features/features/linux-malware-the-truth-about-this-growing-threat?showall=1>.
5. "Up close and personal with Linux malware," We Live Security, February 21, 2020, <https://www.welivesecurity.com/2020/02/21/up-close-and-personal-with-linux-malware/>.
6. "Do you really need antivirus software for Linux desktops?," We Live Security, January 15, 2015, <https://www.welivesecurity.com/2015/01/13/really-need-antivirus-software-linux-desktops/>.



[malwarebytes.com/business](https://www.malwarebytes.com/business)



[corporate-sales@malwarebytes.com](mailto:corporate-sales@malwarebytes.com)



1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at [www.malwarebytes.com](https://www.malwarebytes.com).