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

Currently, there are at least 21 malware families targeting Linux Servers\(^2\)

Linux malware accounts for more than 36% of all new malware detections\(^1\)

Fewer vulnerabilities but far fewer protections (largely open source)\(^3\)
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\(^4,6\)

2. Lack of telemetry
   Few security packages for businesses, many of which do not share telemetry, making Linux-wide insights unavailable\(^5\)

3. Linux defenses are siloed
   Malware squeezes between gaps and defenses\(^4\)
### Linux malware is rapidly evolving

99% of Linux malware targets businesses for criminal aims.

<table>
<thead>
<tr>
<th>Malware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloudsnooper</strong></td>
<td>Allows exfiltration, command and control communication, and more. Traced to successful AWS attack in early 2020.</td>
</tr>
<tr>
<td><strong>QNAPCrypt</strong></td>
<td>Linux ransomware that targets network-attached storage.</td>
</tr>
<tr>
<td><strong>GonnaCry</strong></td>
<td>Ransomware that has evolved along the same path as WannaCry and Petya.</td>
</tr>
<tr>
<td><strong>HiddenWasp</strong></td>
<td>Allows remote control of infected systems. Consists of a trojan, a user-mode rootkit, and an initial deployment script.</td>
</tr>
<tr>
<td><strong>FBOT</strong></td>
<td>Variant of the infamous Mirai botnet that targets Linux IoT devices.</td>
</tr>
</tbody>
</table>
Introducing security built for Linux

Malwarebytes Endpoint Protection for Servers on Linux

Keep 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

Sources


