Top 15 Vulnerabilities Attackers Exploited Millions of Times to Hack Linux Systems

August 23, 2021 Ravie Lakshmanan

(https://thehackernews.com/images/-mNDlC0tKMKU/YSOiCQjKsfI/AAAAAAAADm0/8vxg1C4GwelrljnlPQrCj0yPLMYs18y_ACLcBGAsYHQ/s0/linux.jpg)

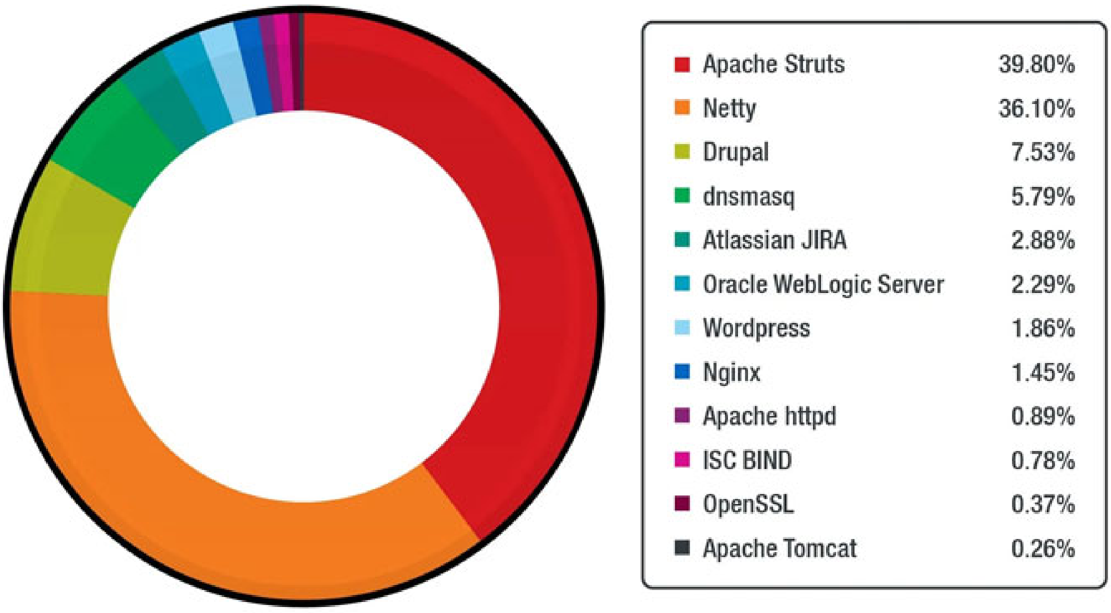
Close to 14 million Linux-based systems are directly exposed to the Internet, making them a lucrative target for an array of real-world attacks that could result in the deployment of malicious web shells, coin miners, ransomware, and other trojans.

That's according to an in-depth look at the Linux threat landscape published by U.S.-Japanese cybersecurity firm Trend Micro (https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-threat-report-2021-1h-linux-threats-in-the-cloud-and-security-recommendations) , detailing the top threats and vulnerabilities affecting the operating system in the first half of 2021, based on data amassed from honeypots, sensors, and anonymized telemetry.

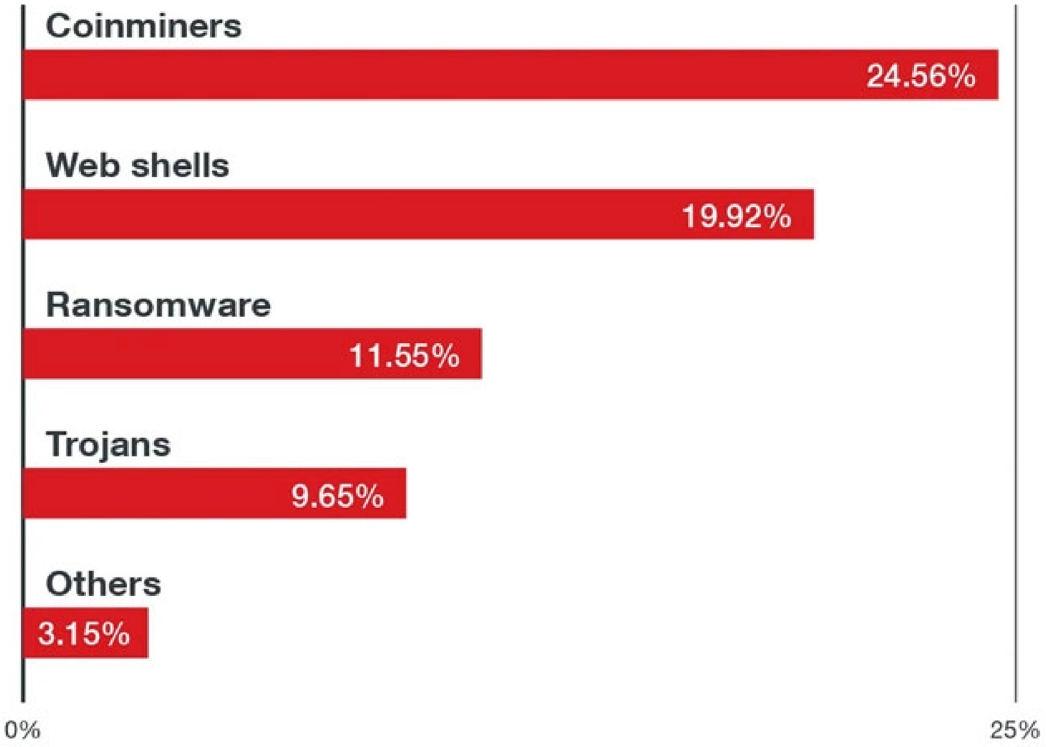
The company, which detected nearly 15 million malware events aimed at Linux-based cloud environments, found coin miners and ransomware to make up 54% of all malware, with web shells accounting for a 29% share.

In addition, by dissecting over 50 million events reported from 100,000 unique Linux hosts during the same time period, the researchers found 15 different security weaknesses that are known to be actively exploited in the wild or have a proof of concept (PoC) —

- **CVE-2017-5638** (https://nvd.nist.gov/vuln/detail/CVE-2017-5638) (CVSS score: 10.0) - Apache Struts 2 remote code execution (RCE) vulnerability
- **CVE-2017-9805** (https://nvd.nist.gov/vuln/detail/CVE-2017-9805) (CVSS score: 8.1) - Apache Struts 2 REST plugin XStream RCE vulnerability
- **CVE-2018-7600** (https://nvd.nist.gov/vuln/detail/CVE-2018-7600) (CVSS score: 9.8) - Drupal Core RCE vulnerability
- **CVE-2020-14750** (https://nvd.nist.gov/vuln/detail/CVE-2020-14750) (CVSS score: 9.8) - Oracle WebLogic Server RCE vulnerability
- **CVE-2020-25213** (https://nvd.nist.gov/vuln/detail/CVE-2020-25213) (CVSS score: 10.0) - WordPress File Manager (wp-file-manager) plugin RCE vulnerability
- **CVE-2020-17496** (https://nvd.nist.gov/vuln/detail/CVE-2020-17496) (CVSS score: 9.8) - vBulletin 'subwidgetConfig' unauthenticated RCE vulnerability
- **CVE-2020-11651** (https://nvd.nist.gov/vuln/detail/CVE-2020-11651) (CVSS score: 9.8) - SaltStack Salt authorization weakness vulnerability
- **CVE-2017-12611** (https://nvd.nist.gov/vuln/detail/CVE-2017-12611) (CVSS score: 9.8) - Apache Struts OGNL expression RCE vulnerability
- **CVE-2017-7657** (https://nvd.nist.gov/vuln/detail/CVE-2017-7657) (CVSS score: 9.8) - Eclipse Jetty chunk length parsing integer overflow vulnerability
- **CVE-2021-29441** (https://nvd.nist.gov/vuln/detail/CVE-2021-29441) (CVSS score: 9.8) - Alibaba Nacos AuthFilter authentication bypass vulnerability
- **CVE-2020-14179** (https://nvd.nist.gov/vuln/detail/CVE-2020-14179) (CVSS score: 5.3) - Atlassian Jira information disclosure vulnerability
- **CVE-2013-4547** (https://nvd.nist.gov/vuln/detail/CVE-2013-4547) (CVSS score: 8.0) - Nginx crafted URI string handling access restriction bypass vulnerability
- **CVE-2019-0230** (https://nvd.nist.gov/vuln/detail/CVE-2019-0230) (CVSS score: 9.8) - Apache Struts 2 RCE vulnerability
- **CVE-2018-11776** (https://nvd.nist.gov/vuln/detail/CVE-2018-11776) (CVSS score: 8.1) - Apache Struts OGNL expression RCE vulnerability
- **CVE-2020-7961** (https://nvd.nist.gov/vuln/detail/CVE-2020-7961) (CVSS score: 9.8) - Liferay Portal untrusted deserialization vulnerability



(https://thehackernews.com/images/-CcxYro041Ss/YSOhRgK85gI/AAAAAAAADmo/EddtTNpqRVsnxWJ2QLdym3CSkEJDwcSggCLcBGAsYHQ/s0/report-1.jpg)



(https://thehackernews.com/images/-p0iNN7yORLk/YSOhRABhMqI/AAAAAAAADmk/RQED6fXWrDkadRhDxqU0JzZOoWwJePPkQCLcBGAsYHQ/s0/report-.jpg

Even more troublingly, the 15 most commonly used Docker images on the official Docker Hub repository has been revealed to harbor hundreds of vulnerabilities spanning across python, node, wordpress, golang, nginx, postgres, influxdb, httpd, mysql, debian, memcached, redis, mongo, centos, and rabbitmq, underscoring the need to secure containers (https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment) from a wide range of potential threats at each stage of the development pipeline.

"Users and organizations should always apply security best practices, which include utilizing the security by design approach, deploying multilayered virtual patching or vulnerability shielding, employing the principle of least privilege, and adhering to the shared responsibility model," the researchers concluded.

Found this article interesting? Follow THN on Facebook (https://www.facebook.com/thehackernews) , Twitter (https://twitter.com/thehackersnews) and LinkedIn (https://www.linkedin.com/company/thehackernews/) to read more exclusive content we post.