FORTINET

OUTBREAK ALERTS

Androxgh0st Malware Attack

Actively stealing credentials in the wild

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a
CVEs: CVE-2021-41773, CVE-2018-15133, CVE-2017-9841

FortiGuard Labs continue to observe widespread activity of Androxgh0st Malware in the wild exploiting multiple vulnerabilities, specifically targeting the PHPUnit (CVE-2017-9841), Laravel Framework (CVE-2018-15133) and Apache Web Server (CVE-2021-41773) to spread and conduct information gathering attacks on the target networks.

Background

Androxgh0st malware is a python-based malware, which primarily targets user environment (.env) files. These files may contain credentials for various high-profile applications such as AWS, O365, SendGrid, and Twilio. Androxgh0st has numerous malicious functions to abuse SMTP, scan and exploit exposed credentials and APIs, and deploy web shell to maintain persistent access to systems

Announced

March 17, 2023: FortiGuard Labs released a Threat Signal
https://www.fortiguard.com/threat-signal-report/5066

January, 2024: FortiGuard Labs continue to block Androxgh0st malware activity on more than 40,000+ unique FortiGate devices a day on average.

Latest Developments

January 16, 2024: The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released the joint Cybersecurity Advisory (CSA) to share known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with threat actors deploying Androxgh0st malware.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

Fortinet customers remain protected by the IPS signatures for all related vulnerabilities (CVE-2021-41773, CVE-2017-9841, CVE-2018-15133) however, users are requested to review the related CVEs and make sure all operating systems, software, and firmware up to date.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

AV

Detects and blocks known Androxgh0st Malware related files

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 91.0004	*DB 91.0004*	*DB 91.0004*	*DB 91.0004*	*DB 91.0004*	*DB 91.0004*	*DB 91.0004*

FortiADC	FortiProxy
DB 91.0004	*DB 91.0004*

AV (Pre-filter)

Detects and blocks known Androxgh0st Malware related files

FortiEDR	FortiSandbox	FortiNDR
DB 91.0004	*DB 91.0004*	*DB 91.0004*

- **Exploitation**

IPS

Detects and blocks Androxgh0st Malware Attack

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 22.488	*DB 22.488*	*DB 22.488*	*DB 22.488*	*DB 22.488*

Web App Security

Detects and blocks Androxgh0st Malware Attack

FortiWeb	FortiADC
DB 0.00302	*DB 1.00038*

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer	FortiNDR Cloud
DB 2.00035	

Threat Hunting

FortiAnalyzer	FortiNDR Cloud
v6.4+	

Content Update

FortiSIEM
DB 603

Playbook

FortiSOAR
v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training	Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

CISA Advisory https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

The Record https://therecord.media/malware-hackers-creating-botnet-cisa-fbi

Security Week https://www.securityweek.com/us-gov-issues-warning-for-androxgh0st-malware-attacks/

Learn more about FortiGuard Outbreak Alerts

FORTINET