F#RTINET. **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

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

FortiGuard Labs continue to observe widespread activity of Androxgh0st Malware in the wild exploiting multiple vulnerabilities, specifically targeting-

Background

and deploy web shell to maintain persistent access to systems

AndroxGh0st has numerous malicious functions to abuse SMTP, scan and exploit exposed credentials and APIs,

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.

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

operating systems, software, and firmware up to date.

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.

FortiGate devices a day on average.

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

PROTECT

Reconnaissance

Weaponization

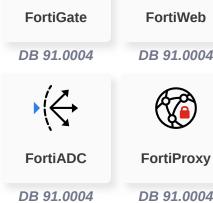
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity

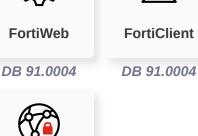
Delivery

events:

Detects and blocks known Androxgh0st Malware related files

AV







FortiADC

DB 22.488

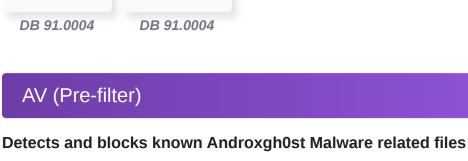
FortiProxy

DB 22.488









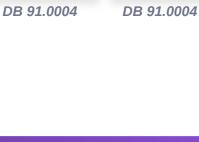
FortiEDR

DB 91.0004

Exploitation

IPS





FortiNDR

FortiNDR

DB 22.488

FortiGate

DB 22.488

Web App Security

Detects and blocks Androxgh0st Malware Attack

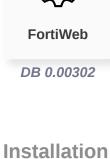
FortiADC

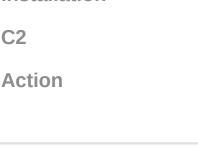
DB 1.00038

FortiSASE

DB 22.488

Detects and blocks Androxgh0st Malware Attack





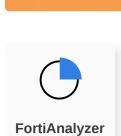
DETECT

alert and generate reports:

Outbreak Detection

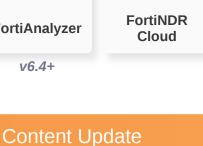
FortiNDR FortiAnalyzer Cloud DB 2.00035

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



v6.4+

Threat Hunting





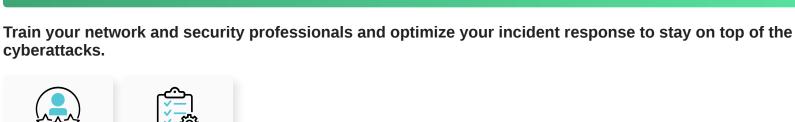


Develop containment techniques to mitigate impacts of security events: **Automated Response**

FortiXDR

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





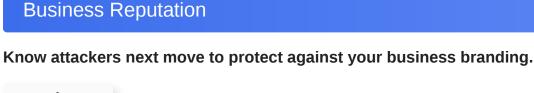
and other forms of cyberattacks.

End-User Training

IDENTIFY

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

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download





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

Security Week

The Record

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

Learn more about FortiGuard Outbreak Alerts





Playbook

FortiSIEM





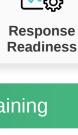
FortiRecon: Incident Response

Assisted Response Services

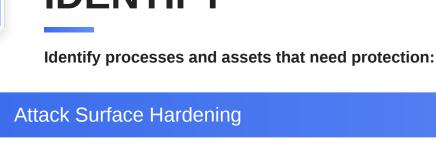
RECOVER Improve security posture and processes by implementing security awareness and training, in preparation for

Services that can automatically respond to this outbreak.









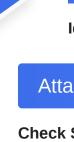
Security **Awareness & Training**















Security Rating

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

F