

Zerobot Attack

Go-based malware exploiting multiple vulnerabilities

<https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>
 CVEs: CVE-2017-17105, CVE-2019-10655, CVE-2020-25223, CVE-2021-42013, CVE-2022-31137, CVE-2022-33891

Zerobot is a Go-based botnet that spreads primarily through IoT and web application vulnerabilities. According to Fortinet research analysis the most recent distribution of Zerobot includes additional capabilities such as a new DDoS attack capabilities and exploiting Apache vulnerabilities.

Background In November 2022, FortiGuard Labs observed a unique botnet written in the Go language known as Zerobot which contains several modules, including self-replication, attacks for different protocols, and self-propagation. For more information on Zerobot Malware, see the link to Fortinet blog below. Please note, ZeroBot Malware does not relates to ZeroBot Chatbot or ZeroBot AI

Announced December 06, 2022: Fortinet posted a security blog research about Zerobot at <https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>

Latest Developments December 12, 2022: Microsoft uncovers new Zerobot 1.1 capabilities and posted a blog at <https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities>



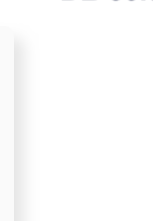




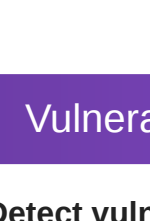

PROTECT

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

Reconnaissance
 Weaponization
 Delivery

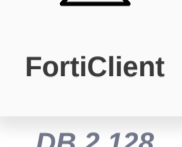
AV

Detect and block payloads related to Zerobot Malware

 FortiGate DB 90.08346	 FortiWeb DB 90.08346	 FortiClient DB 90.08346	 FortiSASE DB 90.08346	 FortiMail DB 90.08346	 FortiCASB DB 90.08346	 FortiCWP DB 90.08346
 FortiADC DB 90.08346	 FortiProxy DB 90.08346					

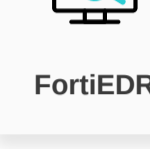
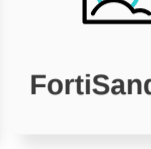
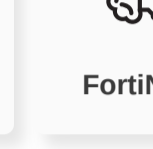
Vulnerability

Detect vulnerable devices related to Zerobot attack


FortiClient
DB 2.128

AV (Pre-filter)

Detect and block payloads related to Zerobot Malware

 FortiEDR DB 90.08346	 FortiSandbox DB 90.08346	 FortiNDR DB 90.08346
--	--	--

Behavior Detection

Behavior Detection Engine detects "ELF/Zerobot.A!tr" as High Risk


FortiSandbox
v4.0+

Exploitation

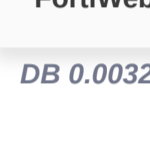
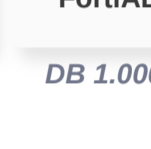
IPS

Detect and block Zerobot related attack attempts

 FortiGate DB 22.464	 FortiSASE DB 22.464	 FortiNDR DB 22.464	 FortiADC DB 22.464	 FortiProxy DB 22.464
---	---	--	--	--

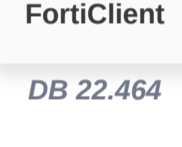
Web App Security

Detect and block Zerobot related attack attempts

 FortiWeb DB 0.00327	 FortiADC DB 1.00038
---	---

Application Firewall

Detect and block Zerobot related attack attempts


FortiClient
DB 22.464

Installation

Web Filter


Blocks known IOCs related to Zerobot Attack


FortiGate
DB 26.62875

C2

Botnet C&C

Blocks traffic to known Zerobot C2 servers

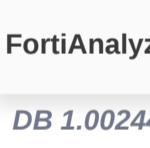
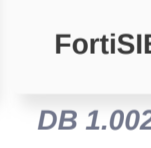

FortiGate
DB 3.00156

Action

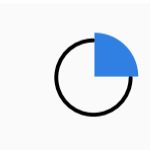
DETECT

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

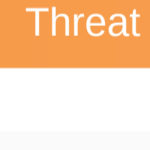

IOC

 FortiAnalyzer DB 1.002442	 FortiSIEM DB 1.002442	 FortiSOCaaS DB 1.002442
---	---	---

Outbreak Detection


FortiAnalyzer
DB 1.00082

Threat Hunting

 FortiAnalyzer v6.4+	 FortiSIEM v6.6+
---	---

Content Update

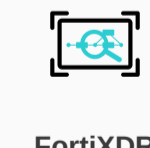

FortiSIEM
DB 309

RESPOND

Develop containment techniques to mitigate impacts of security events:

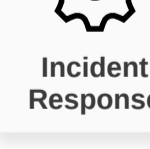
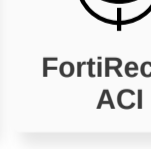
Automated Response

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:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.




Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

 Security Rating	 FortiRecon: EASM
--	---

Additional Resources

- Fortinet Blog <https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities>
- Micorsoft Blog <https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/>
- The Hacker News <https://thehackernews.com/2022/12/zerobot-botnet-emerges-as-growing.html>
- Security Week <https://www.securityweek.com/zerobot-iot-botnet-adds-more-exploits-ddos-capabilities>
- Bleeping Computer <https://www.bleepingcomputer.com/news/security/zerobot-malware-now-spreads-by-exploiting-apache-vulnerabilities/>
- Threat Signal <https://www.fortiguard.com/threat-signal-report/4926>

Learn more about [FortiGuard Outbreak Alerts](#)