FORTINET

OUTBREAK ALERTS

Router Malware Attack

Highly targeted router vulnerabilities

https://www.fortinet.com/blog/threat-research/2022-iot-threat-review

CVEs: CVE-2019-10891, CVE-2018-10562, CVE-2018-10561, CVE-2015-2051, CVE-2023-27076, CVE-2023-26802, CVE-2023-26801

FortiGuard Labs has observed various router vulnerabilities being exploited in the wild to distribute malware such as MooBot Malware, Lucifer Malware, BotenaGo Botnet, Zerobot Malware, Enemybot Malware.

Background

Dec 06, 2021: FortiGuard Labs posted a blog about MooBot Malware analyzing how Moobot targets Hikvision Camera vulnerability.

April 12, 2022: FortiGuard Labs posted a blog about Enemybot Malware and how it targets various router vulnerabilities such as Netgear, D-Link etc.

Jan 27, 2022: FortiGuard Labs released a Threat Signal on BotenaGo Malware which targets multiple IoT devices.

Dec 27, 2022: FortiGuard Labs released an Outbreak Alert about Zerobot Malware which spreads primarily through IoT and web application vulnerabilities.

Please go to Additional Resources section for links to blog posts, threat signal and outbreak alert mentioned above.

Announced

In Jan, 2023: FortiGuard Labs observed severe IPS detections (peak of up-to 50,000 unique IPS devices) and associated malware activity exploiting older router vulnerabilities. In particular, MooBot and Enemybot Malware targeting D-Link routers (CVE-2015-2051) and Lucifer Malware, BotenaGo Botnet and Zerobot Malware exploiting vulnerabilities on unpatched Dasan GPON home routers (CVE-2018-10562, CVE-2018-10561).

FortiGuard Labs recommends upgrading the vulnerable routers to latest firmware and discontinue using end-of-life products if still in use. FortiGuard labs has already released multiple IPS and AV protections to block such attack attempts for our customers.

Latest Developments

In June 2023: FortiGuard observed upto 18,000+ IPS devices that blocked attack attempts affecting some Zyxel CPE models. Zyxel has released firmware updates for RCE and DoS vulnerabilities which does not have assigned CVE number as of now.
https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-cpe

FortiGuard Labs also observed CVE-2023-26801, a vulnerability affecting LB-LINK devices targeted by the attackers and we see IPS detections of upto 5000+ devices.

With popularity of 'Work from Anywhere', company's employees can get compromised easily if they are using vulnerable home router devices. Fortinet Zero Trust Access solutions provide continuous verification of all users, devices and checks for device posture as they access corporate applications and data.
https://www.fortinet.com/solutions/enterprise-midsize-business/network-access/application-access

PROTECT

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

- Reconnaissance
- Weaponization
- Delivery

AV

Detects and blocks malware related to Router Malware Attack

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 90.09110	DB 90.09110	DB 90.09110	DB 90.09110	DB 90.09110	DB 90.09110	DB 90.09110

FortiADC
DB 90.09110

AV (Pre-filter)

Detects and blocks malware related to Router Malware Attack

FortiEDR	FortiSandbox	FortiNDR
DB 90.09110	DB 90.09110	DB 90.09110

- Exploitation

IPS

Detects and blocks attack attempts related to Router vulnerabilities (CVE-2019-10891, CVE-2018-10562, CVE-2018-10561, CVE-2015-2051)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 19.251	DB 19.251	DB 19.251	DB 19.251	DB 19.251

- 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
DB 1.00085

Threat Hunting

FortiAnalyzer	FortiSIEM
v6.4+	v6.6+

Content Update

FortiSIEM
DB 311

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

ZeroBot Outbreak Alert	https://www.fortiguard.com/outbreak-alert/zerobot-attack
Hikvision Outbreak Alert	https://www.fortiguard.com/outbreak-alert/hikvision-command-injection
BotenaGo Threat Signal	https://www.fortiguard.com/threat-signal-report/4389/botenago-malware-targets-multiple-iot-devices

Learn more about FortiGuard Outbreak Alerts