## **OUTBREAK ALERTS**



### Highly targeted router vulnerabilities

Router Malware Attack

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

Camera vulnerability. April 12, 2022: FortiGuard Labs posted a blog about Enemybot Malware and how it targets various router

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

vulnerabilities such as Netgear, D-Link etc.

through IoT and web application vulnerabilities.

Dec 27, 2022: FortiGuard Labs released an Outbreak Alert about Zerobot Malware which spreads primarily

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

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

attempts for our customers.

CVE number as of now. https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-code-execution-and-denialof-service-vulnerabilities-of-cpe

products if still in use. FortiGuard labs has already released multiple IPS and AV protections to block such attack

attackers and we see IPS detections of upto 5000+ devices.

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

devices and checks for device posture as they access corporate applications and data.

**Latest Developments** 

**FortiSASE** 

**FortiMail** 

DB 90.09110

**FortiCASB** 

DB 90.09110

**FortiCWP** 

DB 90.09110

AV

DB 90.09110 DB 90.09110 DB 90.09110 DB 90.09110

**FortiWeb** 

**FortiClient** 

**Detects and blocks malware related to Router Malware Attack** 



**FortiEDR** 

DB 90.09110 DB 90.09110 DB 90.09110

**FortiNDR** 



**FortiGate** 

DB 19.251 DB 19.251 DB 19.251 DB 19.251 DB 19.251

**FortiADC** 



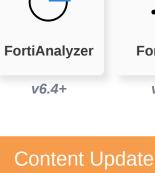


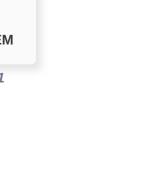
## DB 1.00085

**Outbreak Detection** 

DETECT

alert and generate reports:





**RESPOND** 

**Automated Response** 

**FortiXDR** 

Response

Develop containment techniques to mitigate impacts of security events:

**FortiSIEM** 

v6.6+



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

**RECOVER** 

FortiRecon:

**Assisted Response Services** 

Services that can automatically respond to this outbreak.



**IDENTIFY** 



Security FortiRecon: Rating **EASM** 



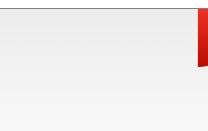


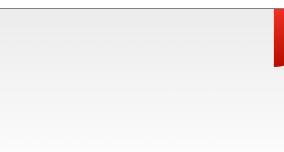
### **ZeroBot Outbreak Alert Hikvision Outbreak Alert** https://www.fortiguard.com/outbreak-alert/hikvision-command-injection

**BotenaGo Threat Signal** https://www.fortiguard.com/threat-signal-report/4389/botenago-malware-targets-multiple-iot-devices

Learn more about FortiGuard Outbreak Alerts







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 FortiGuard Labs also observed CVE-2023-26801, a vulnerability affecting LB-LINK devices targeted by the 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,

Reconnaissance Weaponization **Delivery** 

**FortiGate** 





**FortiSASE** 

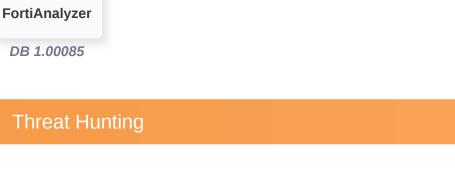
**FortiSandbox** 





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

**FortiProxy** 



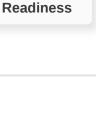




Security readiness and awareness training for SOC teams, InfoSec and general employees.









https://www.fortiguard.com/outbreak-alert/zerobot-attack