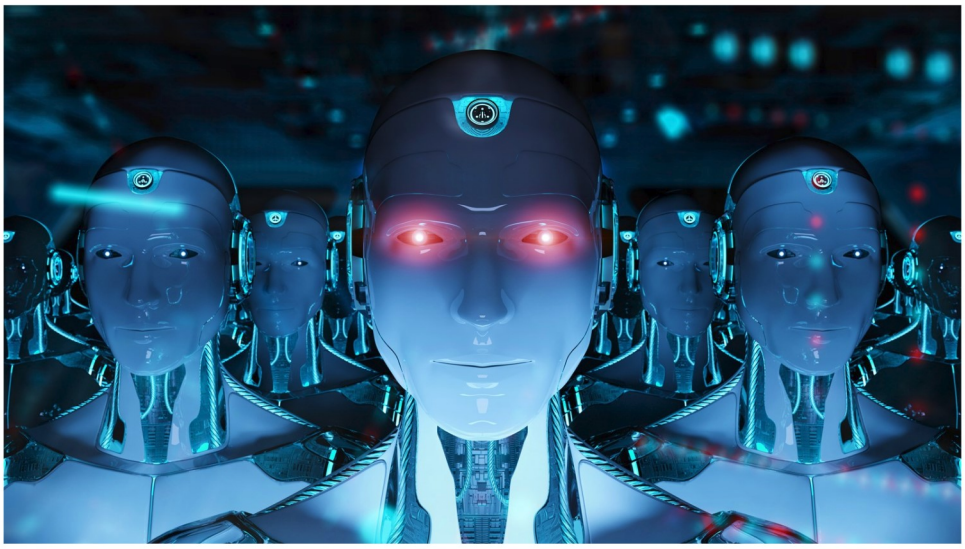
# Cybersecurity researchers take down DDoS botnet by accident

By
**Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)**

November 30, 2022 03:12 PM 1



While analyzing its capabilities, Akamai researchers have accidentally taken down a cryptomining botnet that was also used for distributed denial-of-service (DDoS) attacks.

As revealed in a report (https://www.akamai.com/blog/security-research/kmdsbot-the-attack-and-mine-malware) published earlier this month,

the KmsdBot malware behind this botnet was discovered by members of the Akamai Security Intelligence Response Team (SIRT) after it infected one of their honeypots.

KmsdBot targets Windows and Linux devices with a wide range of architectures, and it infects new systems via SSH connections that use weak or default login credentials.


Compromised devices are being used to mine for cryptocurrency and launch DDoS attacks, with some of the previous targets being gaming and technology companies, as well as luxury car manufacturers.

Unfortunately for its developers and luckily for the device owners, the botnet doesn't yet have persistence capabilities to evade detection.

However, this means the malware has to start all over if it's detected and removed or it malfunctions in any way and loses its connection to the command-and-control (C2) server.

## Tango Down

This is also what also led to the botnet's demise after the current versions of the KmsdBot malware was unintentionally deactivated by Akamai's researchers.

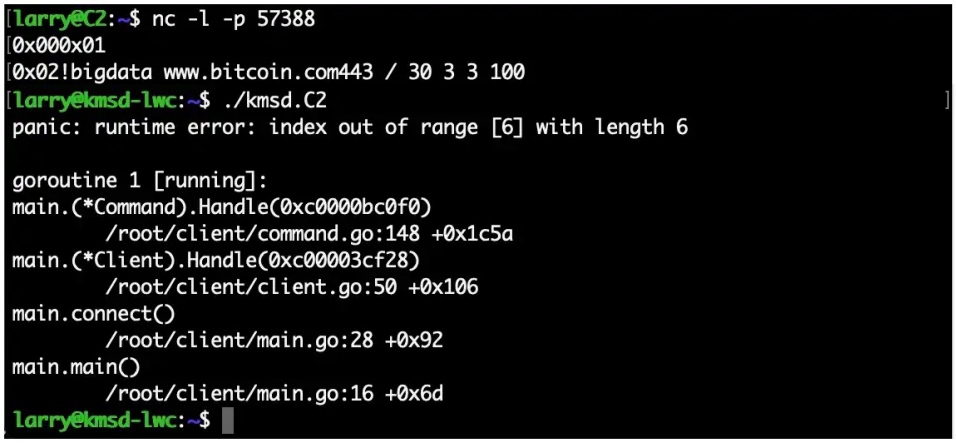
"In our controlled environment, we were able to send commands to the bot to test its functionality and attack signatures," Akamai vulnerability researcher Larry Cashdollar explained in a new report (https://www.akamai.com/blog/security-research/kmsdbot-part-two-crashing-a-botnet).

"As part of this analysis, a syntax error caused the bot to stop sending commands, effectively killing the botnet."

What helped take down KmsdBot was its lack of error-checking and "the

coding equivalent of a typo," which led to the malware crashing and stopping to send attack commands due to the wrong number of arguments to the C2 server.

Basically, as Cashdollar explained, the crash was caused by issuing an attack command where the space between the target website and the port was missing.




*KmsdBot botnet crash (Akamai)*

"This malformed command likely crashed all the botnet code that was running on infected machines and talking to the C2 — essentially, killing the botnet," Cashdollar added.

"Because the bot doesn't have any functionality for persistence on an infected machine, the only way to recover is to re-infect and rebuild the botnet from scratch."

Organizations that could be the target of botnets using similar spreading tactics are advised to secure their systems against attacks by:

- Not using weak credentials and changing default ones for servers or deployed apps
- Ensuring all deployed software is up-to-date
- Using public key authentication for SSH connections to avoid compromise via credential brute-forcing

## Related Articles:

New HeadCrab malware infects 1,200 Redis servers to mine Monero (https://www.bleepingcomputer.com/news/security/new-headcrab-malware-infects-1-200-redis-servers-to-mine-monero/)

New DDoS-as-a-Service platform used in recent attacks on hospitals (https://www.bleepingcomputer.com/news/security/new-ddos-as-a-service-platform-used-in-recent-attacks-on-hospitals/)

Russia's largest ISP says 2022 broke all DDoS attack records (https://www.bleepingcomputer.com/news/security/russia-s-largest-isp-says-2022-broke-all-ddos-attack-records/)

How Gcore uses regular expressions to block DDoS attacks (https://www.bleepingcomputer.com/news/security/how-gcore-uses-regular-expressions-to-block-ddos-attacks/)

DDoS and bot attacks in 2022: Business sectors at risk and how to defend (https://www.bleepingcomputer.com/news/security/ddos-and-bot-attacks-in-2022-business-sectors-at-risk-and-how-to-defend/)

BOTNET (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BOTNET/)

CRYPTOMINER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CRYPTOMINER/)

DDOS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DDOS/)

DISTRIBUTED DENIAL-OF-SERVICE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DISTRIBUTED-DENIAL-OF-SERVICE/)

(https://www.bleepingcomputer.com/author/sergiu-gatlan/)

**SERGIU GATLAN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/SERGIU-GATLAN/)**
**(MAILTO:SERGIU@BLEEPINGCOMPUTER.COM) (HTTPS://TWITTER.COM/SERGHEI)**

Sergiu Gatlan has covered cybersecurity, technology, and a few other topics for over a decade. Email or Twitter DMs for tips.

PREVIOUS ARTICLE

NEXT ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/TECHNOLOGY/CLOUDFLARE-RAISES-MONTHLY-PLAN-PRICES-FOR-THE-FIRST-TIME/)

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/NEW-WINDOWS-MALWARE-ALSO-STEALS-DATA-FROM-VICTIMS-MOBILE-PHONES/)

## Comments

Bournius Photo

**Bournius** (https://www.bleepingcomputer.com/forums/u/1268324/bournius/)

Active Member

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.bleepingcomputer.com/forums/&ved=2ahUKEwihr5uc4vv7AhV8TWwGHQEWCrsQFnoECAoQAQ&usg=AOvVaw1gSz2p8Rjjkv4FlQgXIYU4 (https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.bleepingcomputer.com/forums/&ved=2ahUKEwihr5uc4vv7AhV8TWwGHQEWCrsQFnoECAoQAQ&usg=AOvVaw1gSz2p8Rjjkv4FlQgXIYU4)

## Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

**You need to login in order to post a comment**

**Login**

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

## You may also like:

**POPULAR STORIES**


**New Nevada Ransomware targets Windows and VMware ESXi systems**

(https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/)

**Google Fi data breach let hackers carry out SIM swap attacks**

(https://www.bleepingcomputer.com/news/security/google-fi-data-breach-let-hackers-carry-out-sim-swap-attacks/)

**FOLLOW US:**

(https://www.bleepingcomputer.com/BleepingComputer)

**MAIN SECTIONS**

News (https://www.bleepingcomputer.com/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

**COMMUNITY**

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

**USEFUL RESOURCES**

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

**COMPANY**

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/)