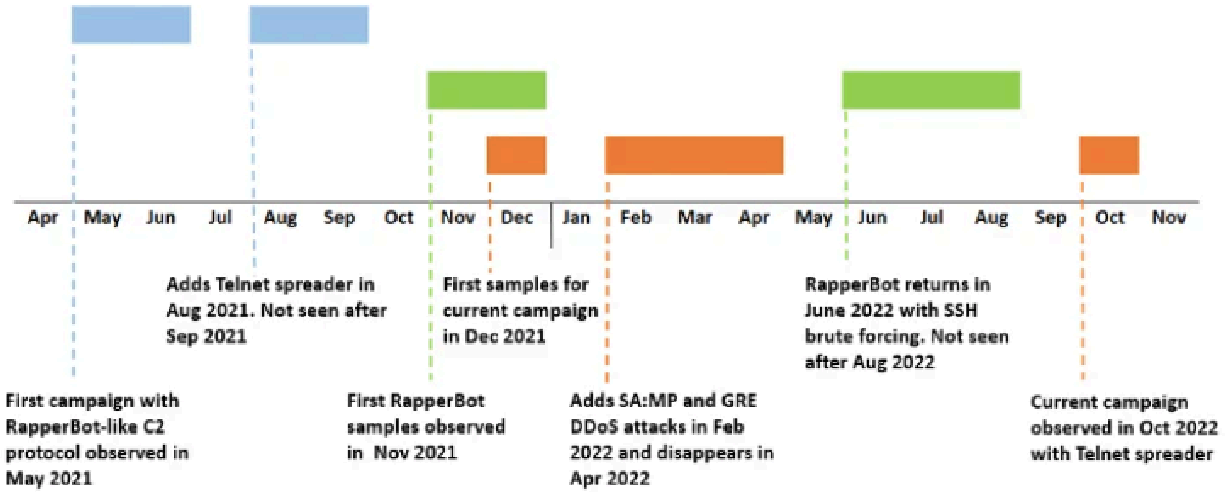
The Fall of RapperBot: A Landmark Blow to the DDoS Industry

Infosources™

August 22, 2025

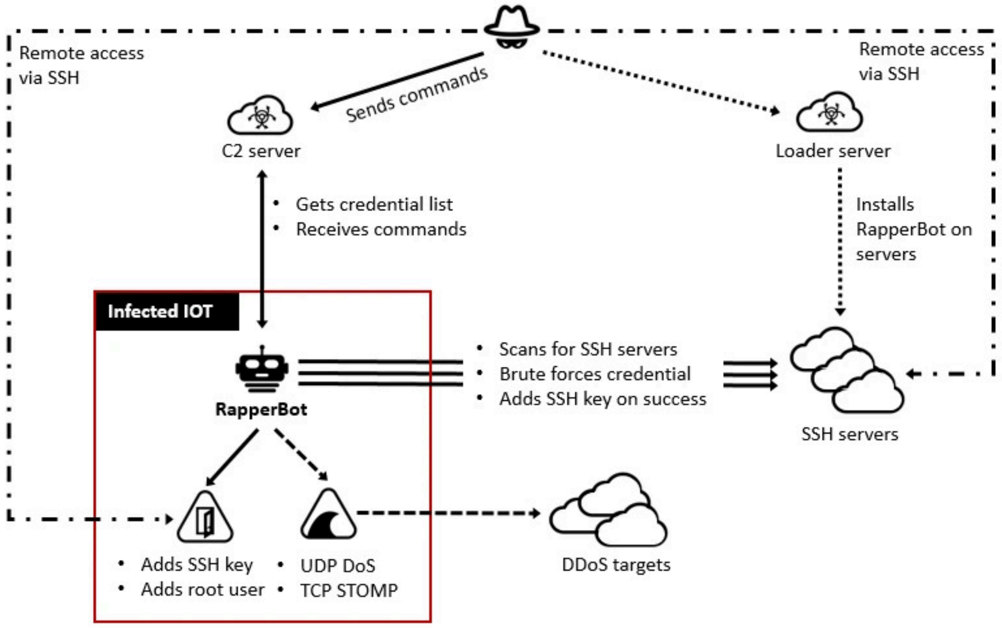
The dismantling of the RapperBot botnet represents a rare moment of disruption in the sprawling DDoS-for-hire economy. Built on the notorious Mirai malware, RapperBot was one of the most powerful and accessible botnets ever deployed, capable of overwhelming targets with terabit-scale attacks. Its takedown, the result of Operation PowerOFF and the unmasking of its operator Ethan Foltz, highlights both the scale of today's criminal infrastructure and the challenges of eradicating it. While law enforcement celebrates this victory, the persistence of Mirai variants and stressor services like DigitalStress suggest that the ecosystem enabling such botnets remains far from defeated.

The dismantling of the **RapperBot** network marks the end of one of the most dangerous DDoS infrastructures of the past decade. Emerging in 2021, RapperBot quickly distinguished itself by weaponizing a familiar lineage: much of its code was borrowed from **Mirai**, the infamous malware that in 2016 transformed unsecured IoT devices into a global army of attack nodes. Mirai's descendants have since multiplied into countless variants, but RapperBot stood out by combining accessibility with raw power. Marketed under names like *Eleven Eleven Botnet* or *CowBot*, it was not an underground curiosity but a subscription-based service—essentially **DDoS-as-a-Service**. Any criminal, regardless of technical skill, could rent its firepower and flood targets with terabit-scale assaults.

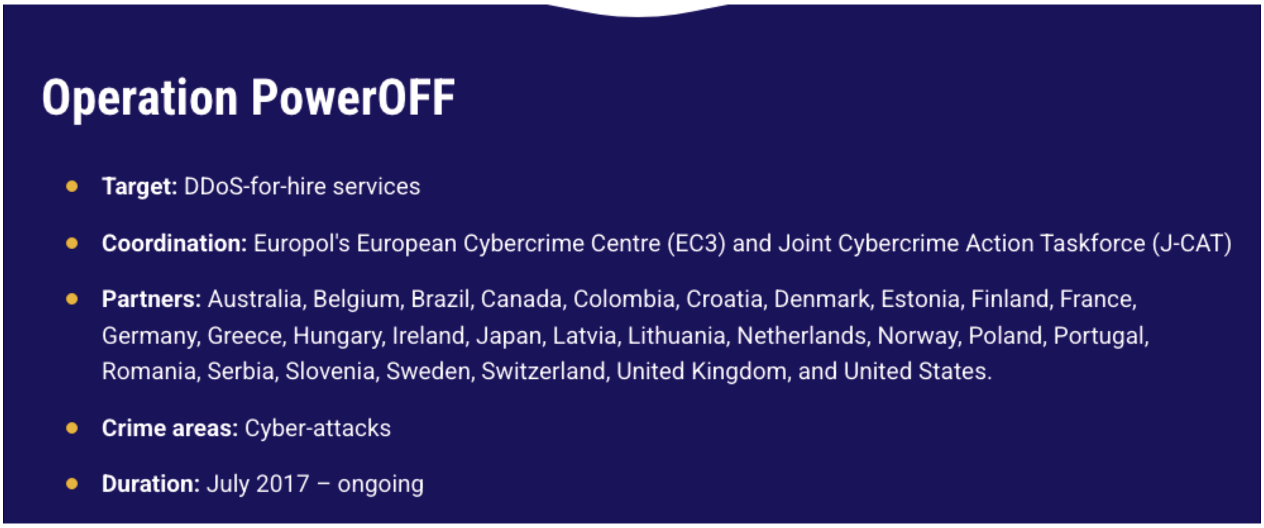

Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Adds Telnet spreader in Aug 2021. Not seen after Sep 2021
First samples for current campaign in Dec 2021
RapperBot returns in June 2022 with SSH brute forcing. Not seen after Aug 2022
First campaign with RapperBot-like C2 protocol observed in May 2021
First RapperBot samples observed in Nov 2021
Adds SA:MP and GRE DDoS attacks in Feb 2022 and disappears in Apr 2022
Current campaign observed in Oct 2022 with Telnet spreader

Timeline of RapperBot campaigns

The scale was staggering. Between 65,000 and 95,000 compromised devices—routers, DVRs, and other poorly secured endpoints—were enslaved. Attacks regularly peaked between 2 and 6 terabits per second, a capacity capable of crippling governments, corporations, and infrastructure. Over four years, more than **18,000 entities across 80 countries** felt its impact, including U.S. government systems. With more than **370,000 cyberattacks** attributed to it since April 2025 alone, RapperBot evolved into both a weapon and an extortion tool, with attackers demanding payment to cease bombardments. For victims, even a brief 30-second wave could translate into thousands of dollars in damages.

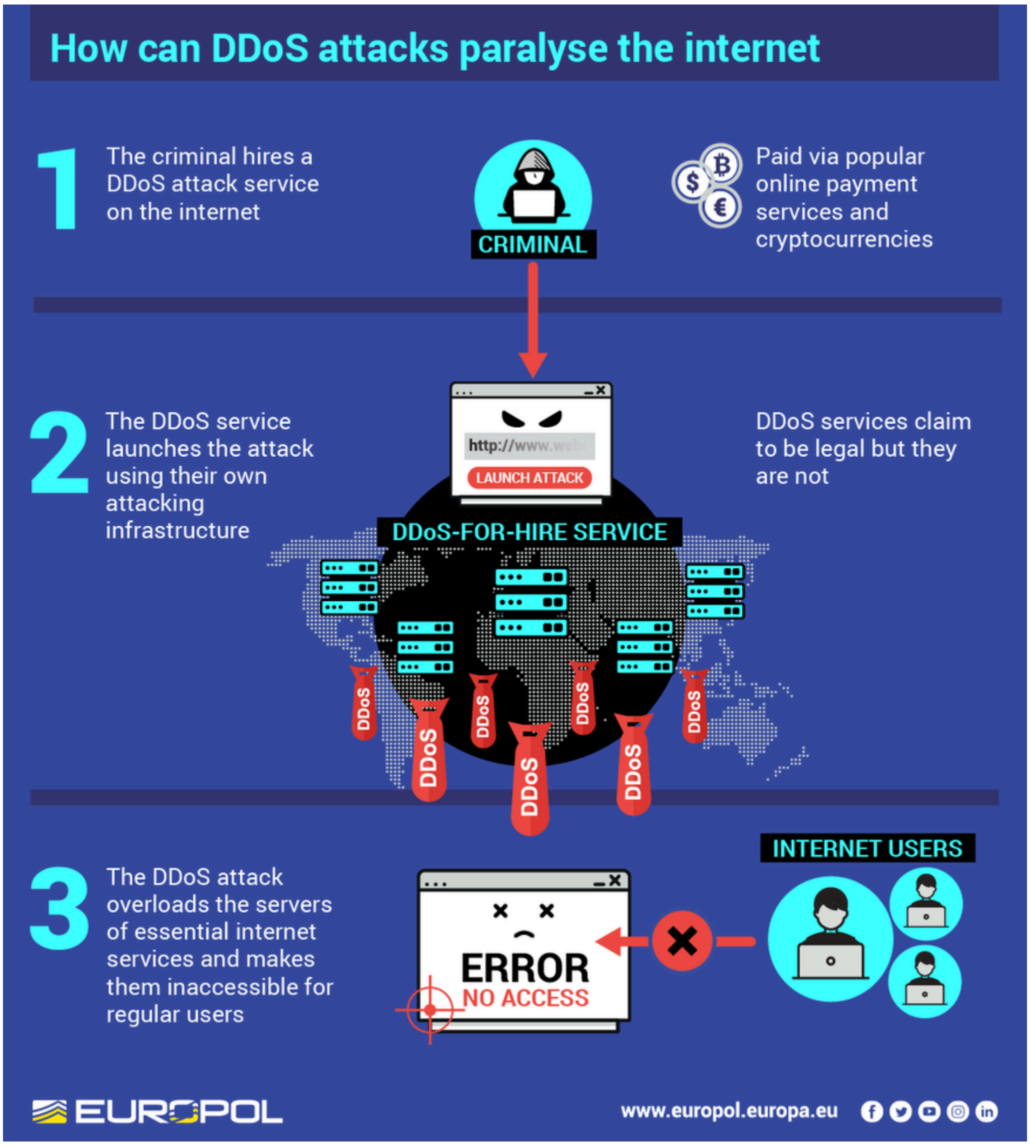


The person behind the operation, **Ethan Foltz**, a 22-year-old from Oregon, was identified and charged after investigators traced the infrastructure back to him. His arrest reflects not only the persistence of U.S. law enforcement but also the long arc of **Operation PowerOFF**, an international crackdown launched in 2018 against DDoS services. PowerOFF previously took down over two dozen stressor/booter platforms, including **DigitalStress** in 2024, a notorious marketplace offering on-demand attack services. RapperBot, however, was a different beast—its efficiency, scale, and longevity made it one of the most “sophisticated” botnets ever recorded.



Operation PowerOFF

- **Target:** DDoS-for-hire services
- **Coordination:** Europol's European Cybercrime Centre (EC3) and Joint Cybercrime Action Taskforce (J-CAT)
- **Partners:** Australia, Belgium, Brazil, Canada, Colombia, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Japan, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, United Kingdom, and United States.
- **Crime areas:** Cyber-attacks
- **Duration:** July 2017 – ongoing



How can DDoS attacks paralyse the internet

1 The criminal hires a DDoS attack service on the internet

Paid via popular online payment services and cryptocurrencies

2 The DDoS service launches the attack using their own attacking infrastructure

DDoS services claim to be legal but they are not

3 The DDoS attack overloads the servers of essential internet services and makes them inaccessible for regular users

This takedown sends a strong signal, but it also underscores a recurring challenge: botnets are hydra-headed. Mirai's code remains freely available, ensuring that the dismantling of one variant is never the end but only a temporary disruption. The collapse of RapperBot will certainly destabilize part of the DDoS-as-a-Service economy, yet the criminal ecosystem remains adaptive. With inexpensive IoT devices still flooding the market and weak security defaults persisting, new iterations are almost inevitable.

In this light, the fall of RapperBot is not just a victory for law enforcement but also a warning: the infrastructures of cybercrime, once built, are hard to erase. Each generation of botnets builds on the last, refining techniques and commoditizing their use. For governments and defenders, the question remains not if but when the next RapperBot will rise.