TrickBot gang shuts down botnet after months of inactivity

therecord.media/trickbot-gang-shuts-down-botnet-after-months-of-inactivity/

February 24, 2022

Image: Steve Johnson

The operators of the TrickBot malware botnet have shut down their server infrastructure today after months of inactivity, bringing to an end one of the most dangerous and persistent malware operations seen in recent years.

Prior to today's voluntary shutdown, the TrickBot gang hadn't set up new servers or tried to carry out email spam campaigns since mid-December 2021.

But today's shutdown comes as no surprise, Vitali Kremez, CEO of security firm AdvIntel, told The Record in a phone call earlier today.

It comes after the group's malware has become "highly detectable" by security products, which appears to have damaged the group's ability to infect and then sell access to Windows systems to its criminal clientele, security firms AdvIntel and Intel471 wrote in separate reports analyzing the malware's recent slump.

"Trickbot, after all, is relatively old malware that hasn't been updated in a major way. Detection rates are high, and the network traffic from bot communication is easily recognized," Intel471 said earlier today before Kremez confirmed that TrickBot had decided to call it quits.

> TrickBot is gone…It is official now as of Thursday, February 24, 2022
> See you soon … or not 😉 pic.twitter.com/zWCCpngUI7
>
> — Vitali Kremez (@VK_Intel) February 24, 2022

Kremez also cited recent recruitment from the Conti ransomware gang as a primary factor in TrickBot's recent demise.

After resurrecting and integrating the Emotet botnet into its "cybercrime cartel" towards the end of 2021, Kremez said that the Conti gang has now also recruited several top members of the TrickBot gang as well.

Under its new leadership, the old TrickBot malware codebase and infrastructure appears to have been abandoned, and Kremez said that the Conti gang is working with the former TrickBot devs to further develop and deploy BazaarBackdoor, one of TrickBot's former modules, as a replacement for TrickBot itself.

TrickBot goes out on its own terms

The TrickBot gang fading its old malware and morphing into a new operation cames after both US authorities and security firms have tried to forcibly take down its command and control server infrastructure in October 2020.

Despite losing roughly 94% of its servers, the botnet survived and returned with new servers days later and with new attacks after a few weeks.

But the failed takedown attempt didn't dissuade US authorities and they responded in 2021 by charging and detaining two of TrickBot's programmers, Alla Witte and Vladimir Dunaev.

However, the arrests didn't touch the group's leadership, which remained intact, and continued to operate the botnet throughout 2021 before entering their recent Conti collaboration and moving on to a new malware codebase.

In December 2021, just days before TrickBot ceased operations, Check Point reported seeing the malware on more than 140,000 systems throughout the year (2021).

In a Wired feature on TrickBot, security firm Hold Security said saw the TrickBot gang invested more than $20 million in its infrastructure last year, which shows the scale of its operation, which dwarfs many legitimate software firms today.

Tags

- AdvIntel
- BazaarBackdoor
- botnet
- Conti

- cybercrime
- Intel471
- malware
- Trickbot

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.