# Something strange is going on with Trickbot

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 15:27:50 UTC

It's been a turbulent 18 months for Trickbot.

The notorious modular malware has been in the spotlight, largely due to actions taken by both private companies and the U.S. government to thwart the attacks. Even as U.S. Cyber Command and Microsoft seized servers and the U.S. Department of Justice arrested several people alleged to be involved with the group that runs the malware, Trickbot stayed active throughout 2021 with various infection campaigns.

These sporadic periods of activity have not continued into 2022. From December 28, 2021 until February 17, 2022, Intel 471 researchers have not seen new Trickbot campaigns. While there have been lulls from time-to-time, this long of a break can be considered unusual. Our team assesses with high confidence that this break is partially due to a big shift from Trickbot's operators, including working with the operators of Emotet.

## Trickbot's recent behavior

Examination of individual malware campaigns, tracked by identifiers known as "gtags," further show there has been a lull in activity since mid-December 2021. These gtags are often listed as a three-letter term followed by a three-number sub-tag that further delineates individual campaigns. Intel 471 researchers tracking "lipXXX" campaigns show that the latest builds, categorized as "lip166," came on December 28, 2021. That was one of three malware campaigns that were active during the month. As a contrast, eight different "lipXXX" builds were discovered in November 2021.

We found a similar pattern in campaigns with a "topXXX" gtag. The last known build came from the "top166" gtag on December 28, 2021, which was one of three "topXXX" builds in December. Yet eight separate "topXXX" builds were discovered the prior month.

In addition to the unusual disappearance of new builds (gtags), we have also observed that the onboard malware configuration files (mcconf), which contain a list of controller addresses the bot can connect to, have gone untouched for long periods of time. The most recent mcconf version numbers are 100021 (Dec 9) and 2000036 (Oct 25). These were once updated frequently, but are receiving fewer and fewer updates. It should be mentioned that Trickbot can receive controller address list updates on-the-fly, so the lack of updates could mean that there isn't anyone cleaning up Trickbot controllers nor is there any pressure to update the on-board controller list.

The scarcity of campaigns only tells part of the story. While the campaigns themselves have been quiet, command and control infrastructure tied to Trickbot continues to operate normally, serving additional plugins, web injects and additional configurations to bots in the botnet. This activity shows that while there haven't been any new campaigns, there is evidence of some effort to maintain Trickbot's command and control infrastructure, even if that effort is essentially an automated one.

Looking at this holistically, this is unusual behavior, but it's part of a trend that Intel 471 and other researchers have been observing for several months. The amount of Trickbot campaigns observed by researchers has continuously decreased over time. However, the amount of ransomware deployments of ransomware families linked with Trickbot, such as Conti, has continued. What can we deduce from this behavior?

### Trickbot's new teammates

Our team assesses with high confidence that Trickbot operators are working closely with the operators of Emotet. There is clear evidence of this relationship, for example, the resurrection of Emotet began with Trickbot. On November 14, 2021, we observed Trickbot pushing a command to its bots to download and execute Emotet samples. This marked the beginning of the return of Emotet.

Even before this event, Trickbot and Emotet operators had a relationship. Emotet was often used to drop Trickbot samples until the Emotet takedown. These Trickbot samples often had the gtag "morXXX." The relationship worked both ways: Intel 471 has observed commands from Trickbot controllers to download and execute Emotet, long before the Emotet's 2021 return.

Intel 471 cannot confirm, but it's likely that the Trickbot operators have phased Trickbot malware out of their operations in favor of other platforms, such as Emotet. 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.

Another crucial piece of the puzzle is the Bazar malware family, which has development ties to the Trickbot group. Multiple threat actors leverage this stealthy backdoor to gain an initial foothold into high-value targets and execute follow-up payloads, such as Cobalt Strike and IcedID aka Bokbot. We have also seen Bazar controllers pushing commands to download and execute Trickbot (mid-2021) and Emotet (November 2021). These events connect Bazar to Trickbot operators, as well as to the revival of Emotet.

Bazar, Bokbot and Emotet likely aren't the only tools leveraged by the threat actor group ditching Trickbot. Our monitoring registered instances of Trickbot pushing Qbot installs to bots of the Trickbot botnet shortly after the Emotet return from November 2021. This observation is yet another indicator that the Trickbot bots are being migrated to other malware platforms.

| Date | Bot Transfer | Payload URL | Notes |
|---|---|---|---|
| Feb 7, 2020 | Trickbot -> Emotet | http://66[.]85.173[.]43/59Emotic1.jpg | only morXXX bots received this command |
| Apr 1, 2020 | Trickbot -> Emotet | none, payload direct from C2 | only morXXX bots received this command |

| | | | |
|---|---|---|---|
| Sep 16, 2020 | Trickbot -> Emotet | http://104[.]193.252[.]221/FortiPlan1.gif | only morXXX bots received this command |
| Nov 14, 2021 | Trickbot -> Emotet | http://141[.]94.176[.]124/Loader_90563_1.dll | First stage of Emotet's resurrection campaign (bots with all gtags received the command) |
| Nov 24, 2021 | Bazar -> Bokbot | none, payload direct from C2 | Bokbot project ID BA205ACA |
| Nov 26, 2021 | Bazar -> Emotet | none, payload direct from C2 | |
| Dec 9, 2021 | Trickbot -> Qbot | http://46[.]30.41[.]173/stager2.dll | Qbot botnet ng_domain |

### Avoiding the spotlight

Despite the takedowns by U.S. Cyber Command in October 2020, Trickbot remained active into 2021. However, with the arrests of two alleged Trickbot developers and an in-depth Wired article that details alleged internal conversations from the group's leadership, Trickbot is under more scrutiny than ever before.

Perhaps a combination of unwanted attention to Trickbot and the availability of newer, improved malware platforms has convinced the operators of Trickbot to abandon it. We suspect that the malware control infrastructure (C2) is being maintained because there is still some monetization value in the remaining bots.

Intel 471 will continue to track Trickbot and will report on any further observations in the future.

---

Source: https://intel471.com/blog/trickbot-2022-emotet-bazar-loader