Who is Trickbot? - CYJAX

By Joe Wrieden

Published: 2022-07-15 · Archived: 2026-04-05 17:47:00 UTC

Since the start of the Russia-Ukraine conflict, Russian based cybercrime groups have been placed into a difficult position. With many groups being comprised of a variety of different nationalities, the various members need to make decisions on allegiance. Leading the charge was the Conti ransomware group who decided on 25 February 2022 to make a post detailing their full support for the Russian government, shown in **Figure 1**, communicating their willingness to fight against those who oppose them. This post came only one day after the invasion of Ukraine on 24 February 2022. It is possible that Conti were required to post this, resulting in the fast reaction time to the invasion, due to the Russian governmental ties the group holds.

Figure 1

This post caused shockwaves in both the intelligence community and within Conti itself. Many members of the group were unhappy with this decision, either not wishing to be seen supporting the Russian government or being from the victim country Ukraine. This inevitably led to Conti retracting their statement only two days later, now saying they only wish to target the “Western warmongers” and “[do] not ally with any governments and [...] condemn the ongoing war”.

Figure 2

However, this reversal was not enough for most members, resulting in them becoming one of the most targeted ransomware groups by Ukrainian supporting organisations and other threat actors. It did not take long for this unrest to lead to action when on 27 February 2022, a Twitter account *@ContiLeaks* began posting links to the logs of internal communications by the group. Within hours threat intelligence researchers around the world were beginning to conduct analysis into the dump, containing over 60,000 messages. This leak caused significant unrest within the group, with the *@ContiLeaks* account itself tweeting: “We know everything about you Conti, go to panic, you can’t even trust your gf, we against you!”.

On 4 March 2022, whilst mass attention was focused on *@ContiLeaks*, another account *@trickleaks* was created, posting the tweet: “We have evidence of the FSB’s cooperation with members of the Trickbot criminal group (Wizard Spider, Maze, Conti, Diavol, Ruyk)”. After this damning message, tweets began to appear containing links to internal communications from members of the Trickbot group. At time of writing, the *@trickleaks* account has approximately 1,700 followers. This is about five times less followers than the *@ContiLeaks* account. These

leaks, which I will refer to as the Trickbot Leaks, were posted increasingly quickly as 35 believed member's messages were uploaded over a two-month period. This led to a total of over 1000 communication extracts.

Each file consists of a direct communication or a group chat involving the user, which range in size. Some files contain nearly 10,000 messages. In total, there are approximately 250,000 messages which contain over 2,500 IP addresses, around 500 potential crypto wallet addresses, and thousands of domains and email addresses. This leak was like nothing seen before and gave cyber threat intelligence researchers unprecedented access to the Trickbot organisation. To put this leak into perspective, it was over four times the size of the Conti leaks which was seen by some researchers as one of the most useful information dumps of the past few years. Alongside these messages, PDF files were leaked which contained large amounts of information reportedly about individual members. This included full names, addresses and identification numbers. These "Doxing PDF" files have given us the ability to analyse the people behind the usernames, examining how and why they are working for the criminal organisation.

Within this report we will analyse and discuss the full extent of the content of these leaks, from the infrastructure and tooling the criminal organisation uses to the inner workings of how the group operates.

Link to PDF

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.
