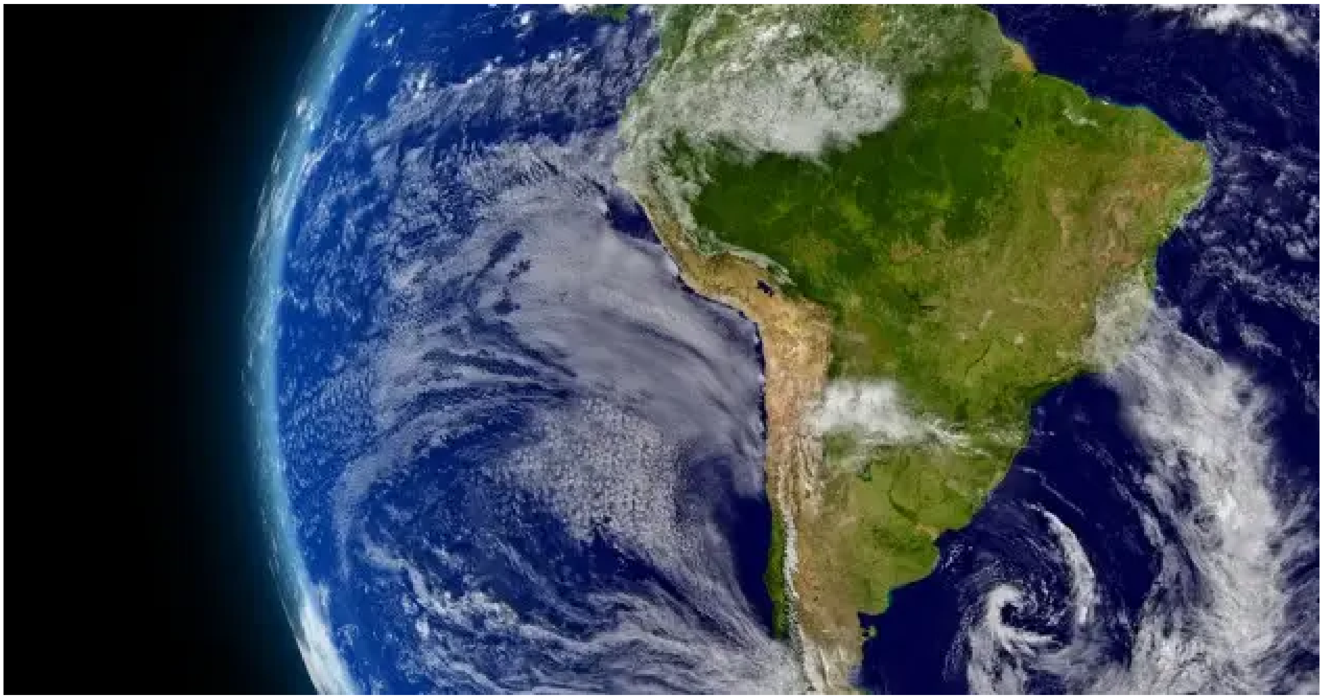
TrickBot Takes to Latin America, Continues to Expand Its Global Reach

securityintelligence.com/trickbot-takes-to-latin-america-continues-to-expand-its-global-reach/

October 11, 2017



Banking & Finance October 11, 2017
By Limor Kessem 4 min read

The TrickBot Trojan, a banking malware believed to be operated by an organized cybercrime group, has been the most active financial Trojan in the wild all summer. For some perspective, while other malware operators were much less active in the summer months, TrickBot was three times more active than Dridex in terms of campaigns and code updates in Q3 and Q4 to date, according to IBM X-Force Research. It continues to expand its reach, this time setting foot in Latin America, with bank targets in Argentina, Chile, Colombia and Peru.

At this time, the number of targets in Latin America is still small, but this strategy is typical for TrickBot's operators, who test the waters before moving ahead to set up redirection attacks and add more banks to their target lists.

Recent configuration files analyzed by IBM X-Force Research show that TrickBot's operators are still using redirection attacks for many of their targets. The ratio in recent campaigns, where TrickBot targeted banks in no less than 40 countries, was 60 percent webinjection attacks to 40 percent redirection attacks. Those are already active in all four countries in Latin America where TrickBot targets major banks. In the current cybercrime arena, according to X-Force research, the only other gangs to use redirection attacks are the operators of the Dridex and GootKit Trojans.

Watch the on-demand webinar: The Evolution of TrickBot Into the Next Global Banking Threat

Signed, Sealed, Delivered by Necurs

TrickBot is delivered to potential victims via email and pushed by the Necurs botnet. The connection with the Necurs gang has been ongoing since mid-2017, which has led to TrickBot being delivered as various file types to conceal its payloads. Most recently, the malware switched to using an eFax ploy to trick users into opening malicious VBS extensions that harbor its payload.

An X-Force analysis of the amount of spam emitted by the Necurs botnet during August and September showed that this cybercrime operation sent over 40 million emails carrying .7z archive file attachments per week in intermittent TrickBot and Locky ransomware campaigns.

This is not the only method by which TrickBot was delivered in Q3. The group has been experimenting with other ideas, such as setting up fake websites and serving the malware from there. In early August, TrickBot was spotted using the same infection zones as the Emotet Trojan, which has been linked with the QakBot banking Trojan, which recently propagated throughout corporate networks and caused massive Active Directory lockouts.

Evolving to Get More

Delivery methods are not the only things TrickBot changes often; it has also been evolving its code over the past year. Q3 was especially active for TrickBot, which added modules to its existing hidden desktop and data theft capabilities.

In July, TrickBot's developers added support for the EternalBlue exploit, a tool borrowed from attacks such as WannaCry and NotPetya that allows it to spread through enterprise networks, along with a new worm feature it adopted to fetch its payloads from malicious remote servers. TrickBot targets mostly business banking services, according to X-Force Research, so this addition is not a surprise.

By August, TrickBot already had new modules designed to steal Outlook email and browsing data. These modules do not feature the same code sophistication the core malware and modules present and were likely written by other developers. This could suggest that the TrickBot team recently took on new, less experienced members.

In early September, TrickBot's operators added cryptocurrency targets to their configuration files, aiming to steal user credentials for platforms such as the American-based Coinbase and the Luxembourg-based Blockchain. Both exchange different types of cryptocurrency coins. This addition enabled TrickBot's operators to take over victims' wallets and empty them or use them as part of a network of wallets to move other coins and wipe their illegitimate traces.

Global Reach

TrickBot has managed to spread to a large number of countries and language zones in relatively little time. The malware operates redirection attacks in over 20 countries and targets banks in over 40 countries spanning Asia, Europe, North America, South America, Australia, New Zealand and the Nordics.

Figure 1: A timeline of Trickbot's global spread (Source: IBM X-Force)

In terms of the top geographies on TrickBot's radar, the focus changes in different configurations, which are attributed to infection cycles destined for each country or region. In recent attacks in which a large number of countries appears on the same list, X-Force data showed the following distribution:

Figure 2: TrickBot's current configuration and geodistribution of targets (Source: IBM X-Force)

Unlike most Trojans, which mainly target the larger parts of Europe such as the U.K., Germany and France, TrickBot also targets banks in smaller unlikely countries, some of which were previously part of the Soviet bloc. Some examples include Bulgaria, Lithuania, Latvia, Slovenia and Slovakia. These countries, where the economy is not as strong and people are less likely to have high residual incomes, are much less likely to be used as run-of-the-mill targets and are more often exploited as cash-out routes for the TrickBot gang.

TrickBot is currently the sixth most prevalent financial malware family in the global financial cybercrime arena, as show in Figure 3.

Figure 3: Most prevalent financial malware families, October 2017 YTD (Source: IBM Trusteer)

Keeping Up With TrickBot

The TrickBot Trojan is an evolving malware project that appears to have funding and alliances in the cybercrime arena. According to X-Force Research, its targets are mostly business banking, wealth management and private banking services, which simply means that the malware's operators are after corporate money and hefty illicit profits.

This gang is believed to be organized, international and unlikely to disappear anytime soon. X-Force Research expects to see TrickBot continue to target banks, organizations and consumers in Q4 2017. To keep up to date about this malware, follow our ongoing X-Force Exchange Collection on TrickBot.

Read the white paper to learn how digital banking is transforming fraud detection

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...

IBM **Security**