

A Look Inside The TrickBot Botnet

blog.lumen.com/a-look-inside-the-trickbot-botnet/

October 12, 2020

BLACK LOTUS LABS [Black Lotus Labs](#) Posted On October 12, 2020

0

0

Shares



Bolstered by contributions from [Black Lotus Labs](#) and others, Microsoft and FS-ISAC recently took court action to disrupt a particularly insidious botnet called TrickBot – a significant source of ransomware and banking credential theft.

As the threat intelligence arm of [Lumen Technologies](#), Black Lotus Labs exists to defend a clean internet, and we collaborate with other threat intelligence and security companies to do just that. In the Microsoft TrickBot case, we provided intelligence and a legal declaration that was filed with the court in support of Microsoft's application for a temporary restraining order to halt TrickBot's operations

This type of industry collaboration is key to disrupting bad actors' activities and increasing their cost of doing business.

A (Brief) History of TrickBot

TrickBot (a.k.a. The Trick, Trickbot, or TrickLoader) is a dangerous and widespread botnet that has operated with relative impunity since it emerged in 2016. It is believed to have evolved from an earlier botnet known as [Dyre](#) or [Dyreza](#). From its onset, TrickBot had the ability to steal credentials when a user accessed banking websites from an infected machine; hence, it was initially categorized as a banking trojan.

The criminal gang behind TrickBot has regularly updated its malicious software, adding modules with new functionality to increase its effectiveness and potential to cause harm. They have incorporated tools such as Mimikatz and Cobalt Strike – often used by penetration testers and criminal attackers – to map victim networks, steal operating system credentials, and spread inside organizations. By 2018, the one-time banking trojan had clearly evolved to become a loader for other malware, including [Ryuk ransomware](#).

Botnets are often built with a single or small number of fixed controllers, referred to as command-and-control servers, or C2s. If TrickBot had a single server providing C2 capabilities, the groups monitoring TrickBot – including Black Lotus Labs – would have successfully neutered it by now. Instead, TrickBot has evolved to use a complex infrastructure that compromises third-party servers and uses them to host malware. It also infects consumer appliances such as DSL routers, and its criminal operators constantly rotate their IP addresses and infected hosts to make disruption of their crime as difficult as possible. To add to the complexity, different C2s may serve different purposes. For example, one group of servers (“core C2s”) might communicate directly with the bots, and another group (“plugin servers”) might serve up plugin modules after the initial infection.

An Earlier Disruption Attempt

Our collaboration with Microsoft was not the industry's first attempt to disrupt TrickBot. A few weeks prior to our collaborative effort, we learned that bots were receiving TrickBot configurations to replace the list of active C2 server IPs with reserved addresses (127.0.0.1, 0.0.0.0). These configurations prevented communication to the C2s, in effect blocking the infected bot from participating in the botnet. The unusual configurations were [revealed publicly](#) in early October, but the identity of the responsible parties remains a mystery.

While this disruption did remove some bots from the botnet, it did not prevent new infections from occurring because the botnet infrastructure remained intact. In fact, during the week of October 6, the TrickBot infections continued, with one of our partners even witnessing new TrickBot installations being delivered from another nefarious botnet – Emotet.

Black Lotus Labs vs. TrickBot

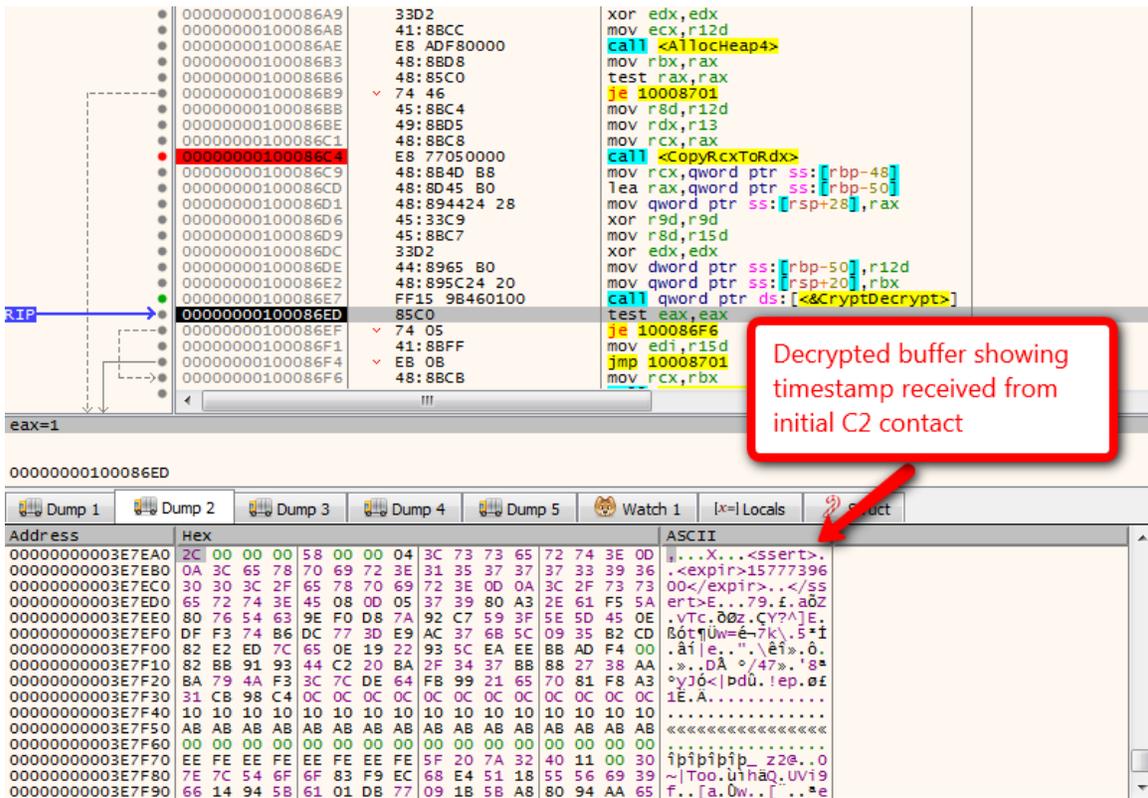
For several years, Black Lotus Labs has used the data from our global network visibility to target numerous malware families to better understand them, track their activity, and disrupt or mitigate their malicious activity. In 2019, we focused on TrickBot by reverse-engineering a TrickBot malware sample and writing a validator that allowed us to add detection of TrickBot C2s to our monitoring systems.

Reverse Engineering

With TrickBot, an infected host contacts the C2, which sends back commands to execute or software to download. The goal of reverse engineering is to understand these exact communication protocols and encryption techniques so we can validate C2s.

Because we don't have access to the original source code, a reverse engineer on the Black Lotus Labs team must dissect the contents of the binary executable itself. Developers of malware actively seek to make such analyses more difficult by encoding, packing, and even encrypting sections of the file. By hiding the presence of character strings that might reveal useful information such as C2 IP addresses, commands, and encryption keys. Our team's goal in reverse engineering is to understand more about how the malware operates in a network environment in order to detect and monitor it across our global network.

When TrickBot infects a machine, the malware generates a unique bot identifier (ID), and communications to the C2 include both the bot ID and a short group tag (referred to in the TrickBot configuration files as "gtag") which indicate the campaign leading to the infection. The gtag used in TrickBot campaigns typically has three or four letters and one to four digits, such as "tmt2" "ono76," "chil45" or "mor124." The TrickBot communication protocol itself implements one- to two-digit commands to update the bot software, download additional modules and their configurations, or even download a different malware entirely (such as ransomware). Communications from the C2 to the bot are encrypted (making it more difficult for network monitoring to discern the contents of the communications) and include a digital signature (protecting the integrity of messages).



Validating

After we finish reverse-engineering the TrickBot sample, our team writes a validator, which simulates bot communication to the C2s. This enables us to confirm that a suspected C2 server was responding in the manner unique to TrickBot. We regularly monitor C2s to track changes in the TrickBot infrastructure so we know when a C2 has gone offline. In addition to core C2s, we validate plugin servers, which together represent an important subset of the overall TrickBot infrastructure.

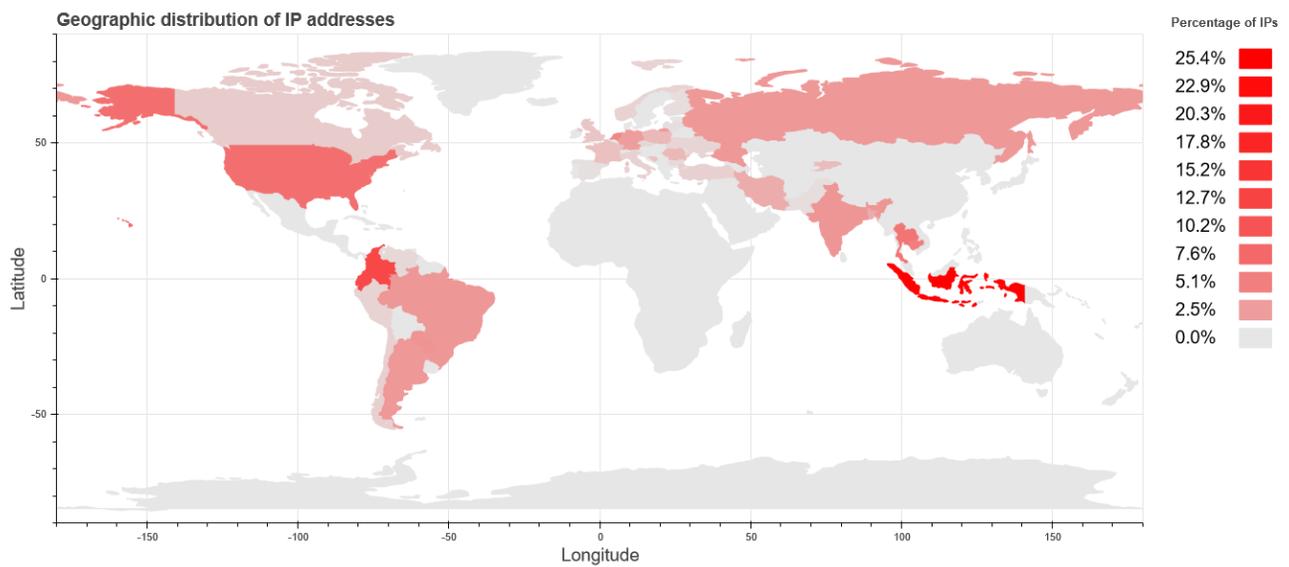
Leveraging our network visibility, we also identify infected bots by examining communication with confirmed C2s. We use machine learning algorithms that monitor our network data to identify other suspected C2s by training a classifier on network characteristics from C2 traffic. Additionally, we review third-party reports of suspicious behavior, and subsequently test those suspected C2s using our validator.

Once we confirm active C2s, we submit abuse notifications to the relevant ISPs and hosting providers to have the C2s taken down. In the past year, Black Lotus Labs has seen more than 500 IP addresses serving as active TrickBot C2s.

Based on our data, below are the top 15 countries where we saw hosting TrickBot C2s, weighted by the number of days a C2 was active:

Country Name C2s * Days Active

Indonesia	1,362
Colombia	652
Ecuador	637
United States	362
Thailand	330
Cambodia	285
Netherlands	232
Paraguay	174
India	165
Brazil	159
Russia	156
Argentina	154
Germany	135
Iran	86
Bangladesh	86



What's Next

Black Lotus Labs will continue to closely monitor to see what impact the collaboration with Microsoft has had on TrickBot's infrastructure and activities, and we hope to learn more for future disruption efforts. While our work might not remove the threat posed by TrickBot, it will raise the cost of doing business for the criminal gang behind the botnet because they will be forced to divert resources away from exploitation activities in order to rebuild the parts of their infrastructure that we disrupted. Meanwhile, we will continue our work to notify victims, null route traffic for malicious servers, disrupt botnets and other malicious activity, and share intel with partners in our efforts to make the internet a safer place for all.

Indicators of Compromise:

Sample hash:

4691a862842f286924357f074927b4e9f276c6073458e3dd4c66218cf4918ea1

C2 IPs:

5.152.210[.]188 27.147.173[.]227 36.91.45[.]10 45.138.158[.]33

5.182.210[.]224 36.66.218[.]117 36.91.87[.]227 45.148.10[.]174

5.182.211[.]124 36.89.182[.]225 36.94.33[.]102 45.66.10[.]22

5.182.211[.]138 36.89.243[.]241 45.127[.]222.8 45.89.125[.]148

45.89.127[.]27 181.129.134[.]18

51.77.112[.]252 181.143.186[.]42

51.83.196[.]234 182.253.113[.]67

51.89.215[.]186 185.14.30[.]247

62.108[.]35.9 185.142.99[.]94

80.210.32[.]67 185.172.129[.]100

83.220.171[.]175 185.234.72[.]114

85.204.116[.]117 185.234.72[.]35

89.249.65[.]53 185.236.202[.]249

91.200.100[.]71 185.25.51[.]139

91.200.103[.]236 185.99.2[.]106

92.38.135[.]61 185.99.2[.]115

92.62.65[.]163	186.159.8[.]218
93.189.42[.]225	190.136.178[.]52
96.9.73[.]73	190.145.83[.]98
96.9.77[.]142	190.152.182[.]150
96.9.77[.]56	190.214.28[.]74
103.111.83[.]246	190.99.97[.]42
103.12.161[.]194	192.3.246[.]216
103.196.211[.]120	194.5.249[.]214
103.221.254[.]102	194.5.249[.]215
103.36.48[.]103	194.87.236[.]171
103.76.169[.]213	195.123.238[.]83
104.161.32[.]108	195.123.239[.]193
104.161.32[.]118	195.123.240[.]18
107.155.137[.]15	195.123.240[.]93
110.93.15[.]98	195.123.241[.]224
112.109.19[.]178	195.123.241[.]229
117.252.214[.]138	195.161.62[.]25
121.100.19[.]18	200.116.159[.]183
121.101.185[.]130	200.116.232[.]186
122.50.6[.]122	200.171.101[.]169
129.232.133[.]39	200.29.119[.]71
131.161.253[.]190	201.231.85[.]50
139.60.163[.]45	212.22.70[.]59
156.96.46[.]27	220.247.174[.]12
158.181.155[.]153	
176.31.28[.]85	

177.190.69[.]162

179.127.88[.]41

180.211.170[.]214

181.112.157[.]42

181.129.104[.]139

Black Lotus LabsCybersecurityCybersecurity Attacks



Author

Black Lotus Labs

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.

Trending Now

You may also like



Services not available everywhere. ©2022 Lumen Technologies. All Rights Reserved.

Services not available everywhere. ©2022 Lumen Technologies. All Rights Reserved.