Global Trickbot disruption operation shows promise

intel471.com/blog/global-trickbot-disruption-operation-shows-promise

The following is an update on the status of Trickbot at noon GMT, Oct. 20, 2020.

On Oct. 19, 2020, Emotet was used to distribute Trickbot. This is the most recent Trickbot sample Intel 471 has observed. The following is a list of control servers included as part of this Trickbot sample's configuration:

Control Server IP Address	City	Country	Organization
131.153.22.145	Amsterdam	Netherlands	AS60558 PHOENIX NAP LLC.
185.99.2.123	Sarajevo	Bosnia and Herzegovina	AS200698 Globalhost d.o.o.
185.99.2.160	Sarajevo	Bosnia and Herzegovina	AS200698 Globalhost d.o.o.
194.5.249.216	Bucharest	Romania	AS64398 NXTSERVERS SRL
199.38.120.91	Georgetown	United States	AS35862 JCWIFI.COM
199.38.121.150	Freeport	United States	AS35862 JCWIFI.COM
199.38.123.58	Georgetown	United States	AS35862 JCWIFI.COM
208.86.161.113	Milledgeville	United States	AS35862 JCWIFI.COM
208.86.162.215	Coleta	United States	AS35862 JCWIFI.COM
208.86.162.241	Thomson	United States	AS35862 JCWIFI.COM
45.89.127.118	Berlin	Germany	AS30823 combahton GmbH
45.89.127.119	Berlin	Germany	AS30823 combahton GmbH
62.108.35.29	Solingen	Germany	AS30962 comtrance GmbH
62.108.35.36	Heidelberg	Germany	AS30962 comtrance GmbH

80.85.156.116	Ashgabat	Turkmenistan	AS44493 Chelyabinsk-Signal LLC
86.104.194.102	Bucharest	Romania	AS48874 HOSTMAZE INC SRL-D

On Oct. 19, 2020, when this latest Trickbot sample was distributed, none of the above listed control servers were able to respond to Trickbot bot requests, a state that continued at the time of this report. Intel 471 believes disruption operations against Trickbot are currently global in nature and have had success against Trickbot infrastructure. Regardless, there still is a small number of working controllers based in Brazil, Colombia, Indonesia and Kyrgyzstan that still are able to respond to Trickbot bot requests. This small number of working control servers was not listed in the most recent distributed Trickbot sample.