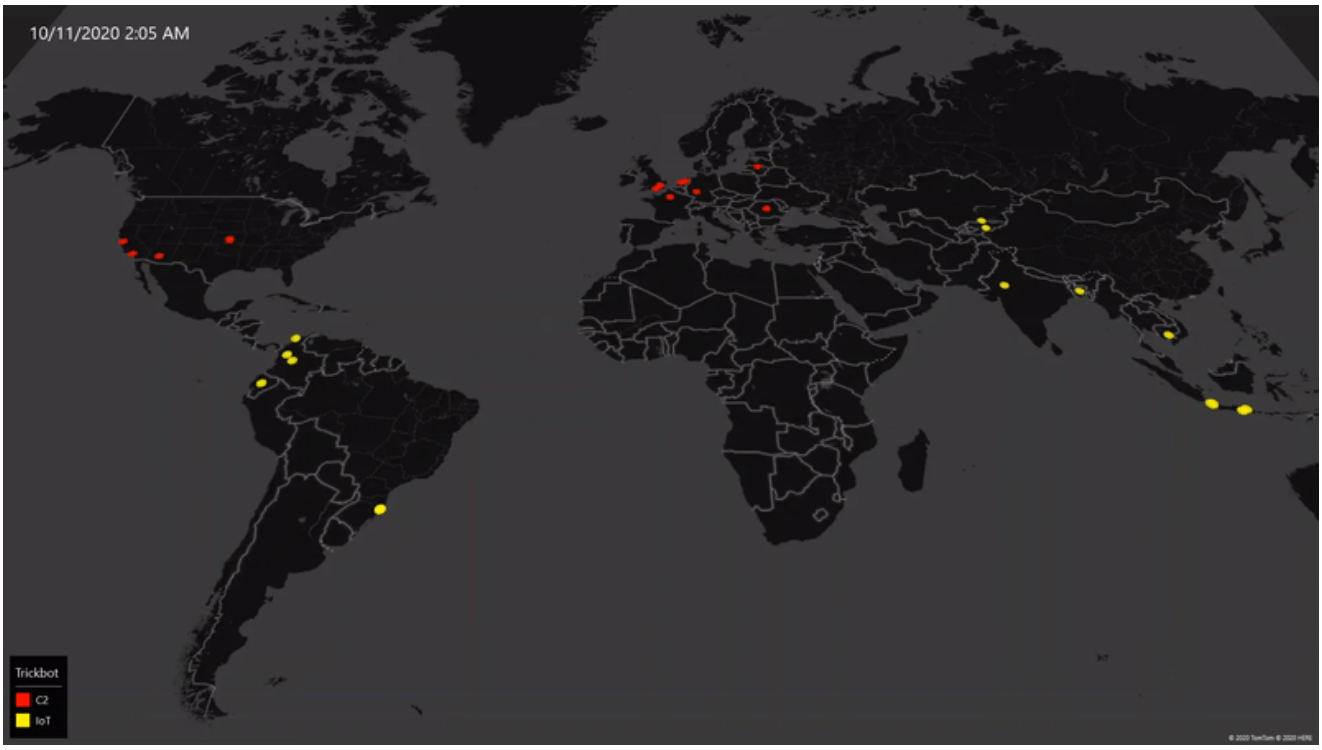
An update on disruption of Trickbot

blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/

October 20, 2020



Last week, we announced a disruption targeting the botnet Trickbot. Trickbot is a network of servers and infected devices run by criminals responsible for a wide range of nefarious activity including the distribution of ransomware which can lock up computer systems. Our disruption is intended to disable Trickbot's infrastructure and make it difficult for its operators to enable ransomware attacks, which have been identified as one of the biggest threats to the upcoming U.S. elections. We've had many requests for updates on the operation, so I'd like to share more on how it's going.

As of October 18, we've worked with partners around the world to eliminate 94% of Trickbot's critical operational infrastructure including both the command-and-control servers in use at the time our action began and new infrastructure Trickbot has attempted to bring online.

Here's how the numbers break down. We initially identified 69 servers around the world that were core to Trickbot's operations, and we disabled 62 of them. The seven remaining servers are not traditional command-and-control servers but rather internet of things (IoT) devices Trickbot infected and was using as part of its server infrastructure; these are in the process of being disabled. As expected, the criminals operating Trickbot scrambled to replace the infrastructure we initially disabled. We tracked this activity closely and identified 59 new servers they attempted to add to their infrastructure. We've now disabled all but one

of these new servers. In sum, from the time we began our operation until October 18, we have taken down 120 of the 128 servers we identified as Trickbot infrastructure around the world.

To be clear, these numbers will change regularly as we expect action we've already taken will continue to impact the remaining infrastructure and as we and others continue to take new action between now and the election. This is challenging work, and there is not always a straight line to success. At the same time, we're pleased with our progress and for several reasons I'm optimistic about the outcomes we can achieve.

First, Microsoft and our partners are trying to take a persistent and layered approach to addressing Trickbot's operations around the world. This is necessary due to the unique architecture of the Trickbot botnet, and the creativity and persistence of the criminals operating it. Since the initial court order we obtained, we've gone back to court and secured subsequent orders to take down the newly activated infrastructure. We will continue to do this between now and election day on November 3. Additionally, our partners and the hosting providers we work with – who have been crucial to our progress – have been sharing information that has uncovered more command-and-control servers. As we continue to cut off these new servers, our partners are also working to clean and remediate the compromised IoT devices, especially routers, that the Trickbot operators are using as non-traditional command-and-control infrastructure. These compromised routers pose a unique challenge for the internet service providers (ISPs) as they must simultaneously work to remediate devices while keeping legitimate traffic uninterrupted, and this delicate work is underway. Finally, we're working with ISPs and others to also clean devices in people's homes and businesses that might be infected.

Second, this work has always been about disrupting Trickbot's operations during peak election activity – doing what we can to take action at a critical time – and we're encouraged by what we're seeing. Anytime a botnet's server infrastructure is eliminated, the attempt to rebuild is not as simple as setting up new servers. New servers need to be provisioned to begin talking with the botnet's infected devices and issuing commands, all of which takes time. We have identified new Trickbot servers, located their respective hosting provider, determined the proper legal methodology to take action, and completely disabled those servers in less than three hours. Our global coordination has allowed a provider to take quick action as soon as we notify them – in one case, in less than six minutes. What we're seeing suggests Trickbot's main focus has become setting up new infrastructure, rather than initiating fresh attacks, and it has had to turn elsewhere for operational help.

In fact, we and others have detected the Trickbot operators attempting to use a competing criminal syndicate to drop what were previously Trickbot payloads. This is one of many signs that suggests to us that, faced with its critical infrastructure under repeated attack, Trickbot operators are scrambling to find other ways to stay active. While an arrangement with other actors will not enable Trickbot to equal its homegrown capabilities, it's also a reminder that there are many threats to keeping cyberspace secure and it's important for people –

especially those involved in the security of our electoral processes – to stay vigilant. It's also why we offer those involved in the election tools such as AccountGuard, Microsoft 365 for Campaigns and Election Security Advisors.

Third, we have the right team and the right groundwork in place to continue having impact in the coming weeks. Our Digital Crimes Unit has spent years studying, documenting and categorizing Trickbot's infrastructure, identifying which command-and-controls are traditional servers and which are actually IoT devices. We believe we understand the right details about Trickbot's infrastructure to focus our attention on the specific command-and-control servers that allow for the greatest degree of disruption. Even more importantly, our network of global partners is monitoring Trickbot's activities and sharing information around the clock. And we have members of our Digital Crimes Unit around the world in direct contact with local ISPs and telecommunications companies.

We fully expect that Trickbot's operators will continue looking for ways to stay operational, and we and our partners will continue to monitor them and take action. We encourage others in the security community who believe in protecting the elections to join the effort and share their intelligence directly with hosting providers and ISPs that can take Trickbot's infrastructure offline. As this work continues, it will be important to focus on the collective impact to Trickbot's capabilities between now and the election, rather than to focus on potentially misleading simplified snapshots from any single moment in time.

Tags: cyberattacks, cybersecurity, Defending Democracy Program, ElectionGuard, Microsoft 365 for Campaigns, Microsoft AccountGuard, ransomware, trickbot