New action to combat ransomware ahead of U.S. elections

blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

October 12, 2020

Today we took action to disrupt a botnet called Trickbot, one of the world's most infamous botnets and prolific distributors of ransomware.

As the United States government and independent experts have warned, ransomware is one of the largest threats to the upcoming elections. Adversaries can use ransomware to infect a computer system used to maintain voter rolls or report on election-night results, seizing those systems at a prescribed hour optimized to sow chaos and distrust.

We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world. We have now cut off key infrastructure so those operating Trickbot will no longer be able to initiate new infections or activate ransomware already dropped into computer systems.

In addition to protecting election infrastructure from ransomware attacks, today’s action will protect a wide range of organizations including financial services institutions, government agencies, healthcare facilities, businesses and universities from the various malware infections Trickbot enabled.

The Trickbot botnet

Trickbot has infected over a million computing devices around the world since late 2016. While the exact identity of the operators is unknown, research suggests they serve both nation-states and criminal networks for a variety of objectives.

In the course of Microsoft’s investigation into Trickbot, we analyzed approximately 61,000 samples of Trickbot malware. What makes it so dangerous is that it has modular capabilities that constantly evolve, infecting victims for the operators’ purposes through a “malware-as-a-service” model. Its operators could provide their customers access to infected machines and offer them a delivery mechanism for many forms of malware, including ransomware. Beyond infecting end user computers, Trickbot has also infected a number of “Internet of Things” devices, such as routers, which has extended Trickbot’s reach into households and organizations.

In addition to maintaining modular capabilities for a variety of end purposes, the operators have proven adept at changing techniques based on developments in society. Trickbot’s spam and spear phishing campaigns used to distribute malware have included topics such as Black Lives Matter and COVID-19, enticing people to click on malicious documents or links. Based on the data we see through Microsoft Office 365 Advanced Threat Detection, Trickbot has been the most prolific malware operation using COVID-19 themed lures.

Disruption components and new legal strategy

We took today’s action after the United States District Court for the Eastern District of Virginia granted our request for a court order to halt Trickbot’s operations.

During the investigation that underpinned our case, we were able to identify operational details including the infrastructure Trickbot used to communicate with and control victim computers, the way infected computers talk with each other, and Trickbot’s mechanisms to evade detection and attempts to disrupt its operation. As we observed the infected computers connect to and receive instructions from command and control servers, we were able to identify the precise IP addresses of those servers. With this evidence, the court granted approval for Microsoft and our partners to disable the IP addresses, render the content stored on the command and control servers inaccessible, suspend all services to the botnet operators, and block any effort by the Trickbot operators to purchase or lease additional servers.

To execute this action, Microsoft formed an international group of industry and telecommunications providers. Our Digital Crimes Unit (DCU) led investigation efforts including detection, analysis, telemetry, and reverse engineering, with additional data and insights to strengthen our legal case from a global network of partners including FS-ISAC, ESET, Lumen's Black Lotus Labs, NTT and Symantec, a division of Broadcom, in addition to our Microsoft Defender team. Further action to remediate victims will be supported by internet service providers (ISPs) and computer emergency readiness teams (CERTs) around the world.

This action also represents a new legal approach that our DCU is using for the first time. Our case includes copyright claims against Trickbot's malicious use of our software code. This approach is an important development in our efforts to stop the spread of malware, allowing us to take civil action to protect customers in the large number of countries around the world that have these laws in place.

We fully anticipate Trickbot's operators will make efforts to revive their operations, and we will work with our partners to monitor their activities and take additional legal and technical steps to stop them.

Impact to additional sectors

In addition to its threat to elections, Trickbot is known for using malware to reach online banking websites and steal funds from people and financial institutions. Financial institutions ranging from global banks and payments processors to regional credit unions have been targeted by Trickbot. For this reason, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has been a critical partner and a co-plaintiff in our legal action.

When someone using a Trickbot-infected computer attempts to log onto a financial institutions website, Trickbot executes a series of activities to secretly hijack the user's web browser, capture the person's online financial login credentials and other personal information, and send that information to the criminal operators. People are unaware of Trickbot's activity as the operators have designed it to hide itself. After Trickbot captures login credentials and personal information, operators use that information to access people's bank accounts. People experience a normal login process and are typically unaware of the underlying surveillance and theft.

Trickbot is also known to deliver the Ryuk crypto-ransomware that has been used in attacks against a wide range of public and private institutions. Ransomware can have devastating effects. Most recently, it crippled the IT network of a German hospital resulting in the death of a woman seeking emergency treatment. Ryuk is a sophisticated crypto-ransomware because it identifies and encrypts network files and disables Windows System Restore to prevent people from being able to recover from the attack without external backups. Ryuk has been attacking organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises and large universities. For example, Ryuk has been attributed to attacks targeting a contractor for the Department of Defense, the North Carolina city of Durham, an IT provider for 110 nursing homes, and a number of hospitals during the COVID-19 pandemic.

Election security and guarding against malware

As we shared last month in the Microsoft Digital Defense Report, ransomware is on the rise. For organizations involved in the elections wanting protection from ransomware and other threats, we offer the threat notification service AccountGuard at no cost which now protects more than two million email accounts around the world. We've completed more than 1,500 AccountGuard nation-state attack notifications to AccountGuard enrollees to date. We also offer Microsoft 365 for Campaigns, an easy-to-set-up version of Microsoft 365 that comes with intelligent and secure default settings at an affordable price. Finally, Election Security Advisors provide proactive resiliency services and reactive incident response for campaigns and election officials, also at an affordable price.

Our Digital Crimes Unit will also continue to engage in operations to protect organizations involved in the democratic process and our entire customer base. Since 2010, Microsoft, through the Digital Crimes Unit, has collaborated with law enforcement and other partners on 23 malware and nation-state domain disruptions, resulting in over 500 million devices rescued from cybercriminals. With this civil action, we have leveraged a new legal strategy that allows us to enforce copyright law to prevent Microsoft infrastructure, in this case our software code, from being used to commit crime. As copyright law is more common than computer crime law, this new approach helps us pursue bad actors in more jurisdictions around the world.

To make sure your computer is free of malware, visit support.microsoft.com/botnets.

Tags: cybersecurity, Defending Democracy Program, ElectionGuard, ransomware, trickbot