Trickbot down, but is it out?

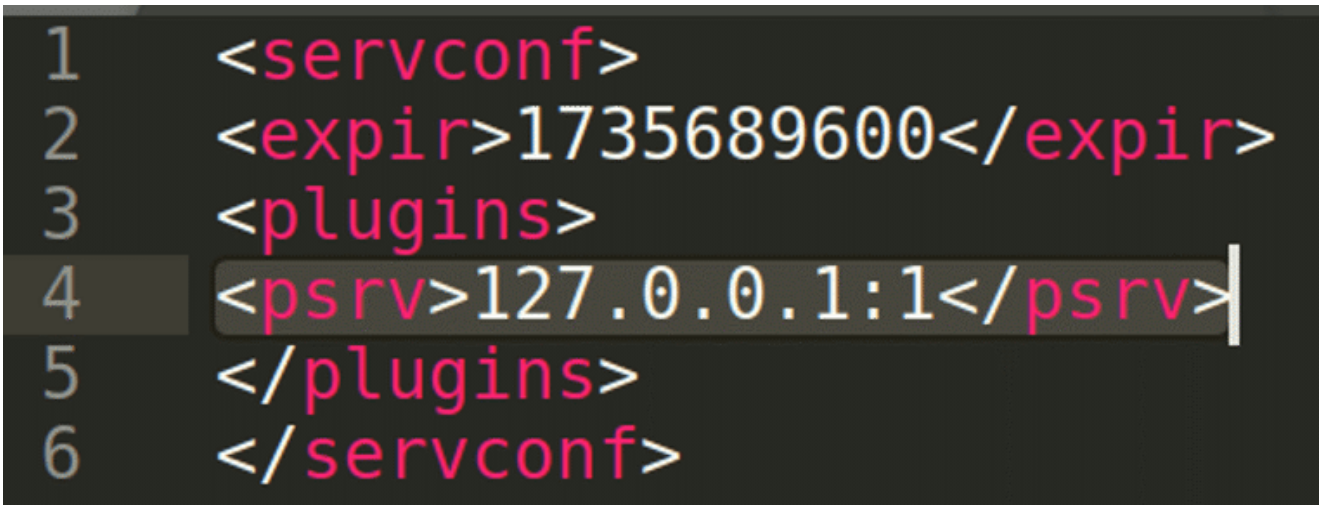
intel471.com/blog/trickbot-update-november-2020-bazar-loader-microsoft

Summary

Since the separate and independent actions taken against Trickbot, we have observed successful disruption of its command and control infrastructure. However, the actors linked to Trickbot have not ceased their criminal activities. These actors have continued engaging in ransomware activity, using BazarLoader instead of Trickbot. We are unable to assess the long-term impact of the Trickbot disruption activity or whether Trickbot will continue to be used by cybercrime groups. This analysis covers the period from Sept. 22, 2020 until Nov. 6, 2020.

The battle begins: Sept. 22 - Oct. 12, 2020

The first blow Intel 471 observed was believed to be struck by the U.S. Cyber Command [1] on Sept. 22, 2020. Utilizing their access to Trickbot command and control servers, Cyber Command operators are believed to have modified several Trickbot configuration files that were sent by their C&C infrastructure to Trickbot-infected systems. Their actions were believed to be intended to render the bots unable to communicate with Trickbot's control servers. Responding to this disruption, Trickbot operators stabilized their operation within 24 hours, restoring working configuration files on their command and control servers. Cyber Command struck again, poisoning the Trickbot configuration files for a second time. This time the botnet operators needed more time to restore their servers. The impact of this action was a loss of an unknown number of bots from their botnet. However, the actors linked to Trickbot are efficient at identifying high-value targets from within their pool of already compromised systems and using second-stage tools such as Cobalt Strike to maintain persistent access to these networks. As a result, the actors maintained access to systems where they already were engaged in follow-on intrusion activity.



The image reflects the poisoned Trickbot plug-in server configuration.

Microsoft joins the fray: Oct. 12, 2020

It was unclear exactly when Microsoft began their own action against Trickbot, but they announced their action publicly on Oct. 12, 2020 [2]. Unsealed indictments contained a list of IP addresses that Intel 471 identified as belonging to Trickbot or Bazar control server infrastructure [3]. In that indictment, Microsoft appealed to the court to order U.S. hosting companies responsible for hosting Trickbot controller infrastructure to shut down the infrastructure and "transfer any content and software hosted at the IP addresses" to Microsoft. However, we believe Microsoft also successfully impacted Trickbot's infrastructure that was outside the jurisdiction of U.S. courts.

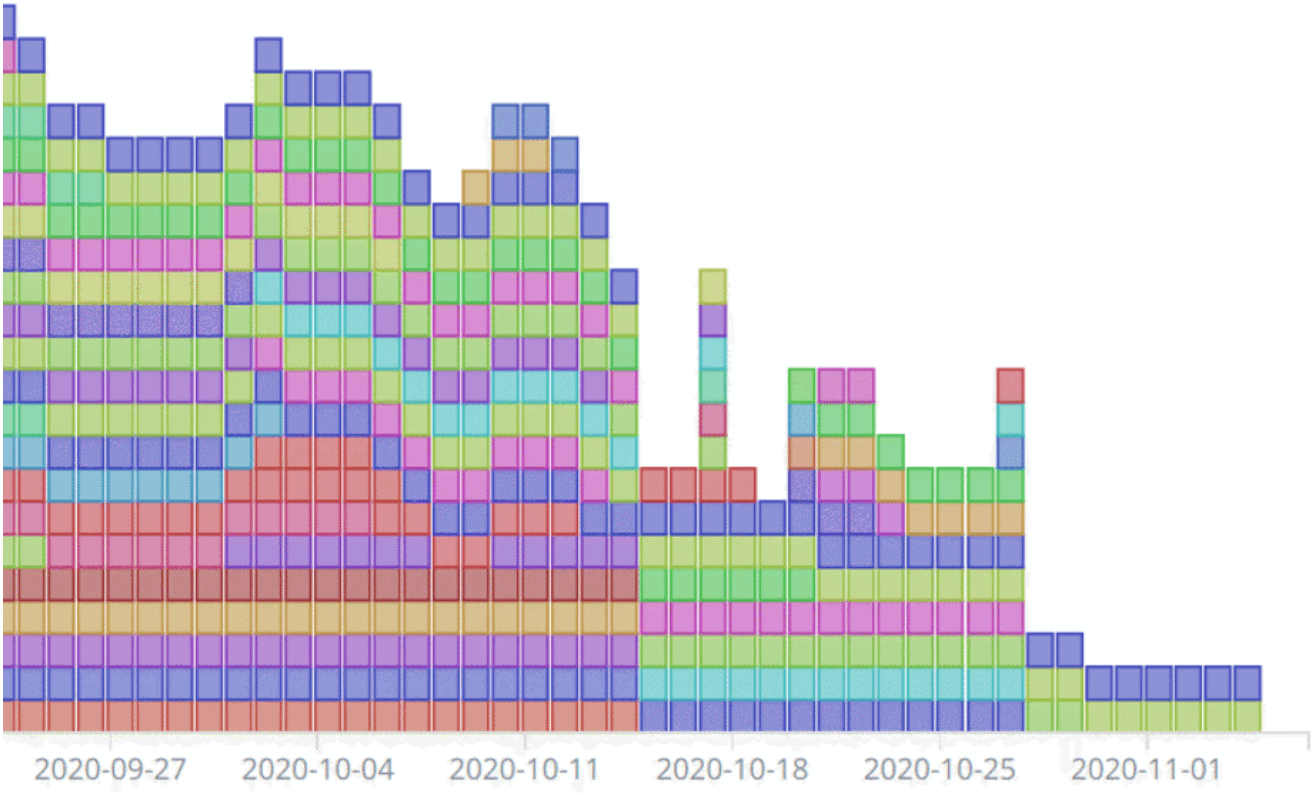
War of attrition: Oct. 13 - Nov. 1, 2020

From Oct. 13, 2020, to Nov. 1, 2020, we began to see the impact of Microsoft's takedown actions against Trickbot's infrastructure. During this period, we observed that a significant amount of Trickbot's infrastructure was rendered inoperable while the Trickbot operators were setting up new infrastructure in response. This allowed Trickbot to maintain an active and working command and control infrastructure, which was degraded significantly compared to the previous month prior to any action. During this time, Trickbot operators also initiated new infection campaigns via the Emotet malware-as-a-service (MaaS) (see: screenshot below) and other mass-spam sources to rebuild their botnet.

Trickbot was distributed by the Emotet service Oct. 19, 2020.

Current state of affairs: Oct. 28 - Nov. 6, 2020

Between Oct. 28, 2020 and Nov. 6, 2020, we have not seen any new Trickbot infection campaigns in our monitoring nor in open source reporting. We observed the number of active and working Trickbot control servers being reduced over time and we were unable to identify any working Trickbot control servers as of Nov. 6.



The number of active Trickbot control servers diminished in October 2020.

BazarLoader instead of Trickbot?

Reports from security researchers [4][5] and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) indicate a recent resurgence of ransomware incidents involving the Ryuk ransomware. This strain of ransomware was frequently linked to Trickbot by security researchers [6]. In these recent Ryuk attacks, incident responders have reported that instead of seeing Trickbot in the initial stages of an incident, they saw a different malware known as BazarLoader aka KEGTAP. BazarLoader is linked to the Trickbot operators in many ways, including shared infrastructure and code similarities. This indicates the actors linked to Trickbot continue to launch targeted ransomware attacks successfully despite the disruption of the Trickbot infrastructure. It was unclear whether the Trickbot operators will return to using Trickbot or will completely move to using BazarLoader as a replacement.

Regardless of the switch from Trickbot to BazarLoader, we are encouraged by the overall impact of disruption activity against Trickbot's infrastructure. At the very least, this disruption activity caused the actors behind Trickbot to spend time and effort setting up new

infrastructure instead of impacting and ransoming victims.

Update - Nov. 10, 2020

This blog post covers the period Sep 22, 2020 to Nov 6, 2020. On Nov 9, 2020, we did see a new version of Trickbot that was distributed via a spam campaign (gtag tar2).