Attacks Aimed at Disrupting the Trickbot Botnet

krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/

Over the past 10 days, someone has been launching a series of coordinated attacks designed to disrupt **Trickbot**, an enormous collection of more than two million malware-infected Windows PCs that are constantly being harvested for financial data and are often used as the entry point for deploying ransomware within compromised organizations.

On Sept. 22, someone pushed out a new configuration file to Windows computers currently infected with Trickbot. The crooks running the Trickbot botnet typically use these config files to pass new instructions to their fleet of infected PCs, such as the Internet address where hacked systems should download new updates to the malware.

A text snippet from one of the bogus Trickbot configuration updates. Source: Intel 471

But the new configuration file pushed on Sept. 22 told all systems infected with Trickbot that their new malware control server had the address 127.0.0.1, which is a “localhost” address that is not reachable over the public Internet, according to an analysis by cyber intelligence firm Intel 471.

It’s not known how many Trickbot-infected systems received the phony update, but it seems clear this wasn’t just a mistake by Trickbot’s overlords. Intel 471 found that it happened yet again on Oct. 1, suggesting someone with access to the inner workings of the botnet was trying to disrupt its operations.

“Shortly after the bogus configs were pushed out, all Trickbot controllers stopped responding correctly to bot requests,” Intel 471 wrote in a note to its customers. “This possibly means central Trickbot controller infrastructure was disrupted. The close timing of both events suggested an intentional disruption of Trickbot botnet operations.”

Intel 471 CEO **Mark Arena** said it's anyone's guess at this point who is responsible.

"Obviously, someone is trying to attack Trickbot," Arena said. "It could be someone in the security research community, a government, a disgruntled insider, or a rival cybercrime group. We just don't know at this point."

Arena said it's unclear how successful these bogus configuration file updates will be given that the Trickbot authors built a fail-safe recovery system into their malware. Specifically, Trickbot has a backup control mechanism: A domain name registered on EmerDNS, a decentralized domain name system.

"This domain should still be in control of the Trickbot operators and could potentially be used to recover bots," Intel 471 wrote.

But whoever is screwing with the Trickbot purveyors appears to have adopted a multi-pronged approach: Around the same time as the second bogus configuration file update was pushed on Oct. 1, someone stuffed the control networks that the Trickbot operators use to keep track of data on infected systems with millions of new records.

Alex Holden is chief technology officer and founder of Hold Security, a Milwaukee-based cyber intelligence firm that helps recover stolen data. Holden said at the end of September Trickbot held passwords and financial data stolen from more than 2.7 million Windows PCs.

By October 1, Holden said, that number had magically grown to more than seven million.

"Someone is flooding the Trickbot system with fake data," Holden said. "Whoever is doing this is generating records that include machine names indicating these are infected systems in a broad range of organizations, including the Department of Defense, U.S. Bank, JP Morgan Chase, PNC and Citigroup, to name a few."

Holden said the flood of new, apparently bogus, records appears to be an attempt by someone to dilute the Trickbot database and confuse or stymie the Trickbot operators. But so far, Holden said, the impact has been mainly to annoy and aggravate the criminals in charge of Trickbot.

"Our monitoring found at least one statement from one of the ransomware groups that relies on Trickbot saying this pisses them off, and they're going to double the ransom they're asking for from a victim," Holden said. "We haven't been able to confirm whether they actually followed through with that, but these attacks are definitely interfering with their business."

Intel 471's Arena said this could be part of an ongoing campaign to dismantle or wrest control over the Trickbot botnet. Such an effort would hardly be unprecedented. In 2014, for example, U.S. and international law enforcement agencies teamed up with multiple security

firms and private researchers to commandeer the Gameover Zeus Botnet, a particularly aggressive and sophisticated malware strain that had enslaved up to 1 million Windows PCs globally.

Trickbot would be an attractive target for such a takeover effort because it is widely viewed as a platform used to find potential ransomware victims. Intel 471 describes Trickbot as "a malware-as-a-service platform that caters to a relatively small number of top-tier cybercriminals."

One of the top ransomware gangs in operation today — which deploys ransomware strains known variously as "**Ryuk**" and "**Conti**," is known to be closely associated with Trickbot infections. Both ransomware families have been used in some of the most damaging and costly malware incidents to date.

The latest Ryuk victim is **Universal Health Services** (UHS), a Fortune 500 hospital and healthcare services provider that operates more than 400 facilities in the U.S. and U.K.

On Sunday, Sept. 27, UHS shut down its computer systems at healthcare facilities across the United States in a bid to stop the spread of the malware. The disruption has reportedly caused the affected hospitals to redirect ambulances and relocate patients in need of surgery to other nearby hospitals.