Trickbot, Phishing, Ransomware & Elections

By Adam Caudill

Published: 2020-10-19 · Archived: 2026-04-02 11:51:19 UTC

The last few weeks have been rough for the operators of the Trickbot botnet, a malware-as-a-service operation, who are facing coordinated attacks from both the US Cyber Command and Microsoft, with the aid of a number of partners. Trickbot's operators went from successful, with over a million infections, to becoming the target of the US military and major corporations — and Reuters is reporting that indictments resulting from an FBI investigation will be unsealed soon.

This story that has a bit of everything: international intrigue, attacks on healthcare providers, phishing at a vast scale (using topics such as COVID-19 and Black Lives Matter as lures), the Internet of Things, counter-hacking, ransomware, stolen government secrets, novel legal techniques, and even a potential election impact. There is enough here for a techno-thriller.

While Trickbot has taken some hard punches, it's probably not done. Its command and control (C2) servers are spread across the world, some far from the reach of the court order that Microsoft is using to take many of them down. There are also signs that the people behind Trickbot are fighting back, bringing new servers up as others go down. Disrupting a botnet is one thing, but killing it is another.

Like many botnets, Trickbot has a history of being used for a variety of things, sending phishing emails to spread further, capturing credentials from victims' browsers, and distributing ransomware (Ryuk, in this case) — encrypting files and demanding payment for their return. As is often the case, the full harm caused by a botnet like this is hard to quantify, but with over a million infections, it's safe to say the harm has been substantial. And remember that one of the victims was a major healthcare provider. While the impact on the provider's level of clear isn't clear today, one must wonder if health outcomes were affected.

A Novel Legal Approach

Microsoft has leveraged the courts to take down other botnets, though this time it used a new legal maneuver: copyright violation. To secure the order to take down the IP addresses used by the Trickbot C2 servers, Microsoft pointed out that all programs that run on Windows require the use of the Windows SDK (for example, the header files for the Windows API), and the SDK's license includes a provision that prohibits its use "in malicious, deceptive, or unlawful programs." In addition, Microsoft claimed trademark infringement and other violations of law, as it has done in previous cases.

In essence, the argument is that any program that targets Windows that is malicious, deceptive, or illegal violates the license associated with the SDK, and thus is a violation of Microsoft's copyright. This has provided Microsoft (and the makers of other operating systems) a new method to fight the creators of malware.

It's a Phish … Again

Often, the route to infection starts with an email, something catchy or important in the subject line, and an attachment or a link to a file. If the file is opened, the victim is tricked into activating a malicious macro, and then

the system is compromised. Security tools are disabled, data is stolen from a variety of sources, and attacks against other systems are launched.

Phishing — from mass emails sent indiscriminately to spear-phishing that's highly targeted and customized — is a threat that year after year continues to be among the largest threats to both business and end users. This omnipresent threat is one that everyone should be aware of and take steps to protect themselves from. Here are several ways to do this:

- Email systems should be set up to scan for and block known threats.
- User's systems should be configured to disable dangerous features, such as macros in Office documents (unless absolutely needed).
- Email attachments should be treated as suspicious by default; users should never assume that any attachment is trustworthy unless they are expecting it and it's coming from a trusted sender. Assume it's malicious unless there's a good reason to believe otherwise.
- Just because it looks like it's from someone recognizable doesn't mean it is; anything that looks odd or suspicious should be confirmed out-of-band before clicking links or opening attachments.

It's always better to err on the side of caution when dealing with email, especially when anything seems off.

Ransomware Attacks & Election Security

In the United States, there are more than 10,000 separate election jurisdictions, using some combination of city, county, and state technical resources. Each of these represents a target for organized ransomware operations, targets that offer increasing value as the election approaches.

As vulnerable targets are found, operators may wait until the time is best, when it’s most lucrative to strike. As we approach an election that may bring both record turnouts and controversy, any delays or disruptions are sure to draw nationwide attention and raise questions about the integrity of the outcome. This means that anything that is even loosely related to elections is a prime target, and officials would be desperate to recover as quickly as possible.

Understanding this tactic of ransomware operators makes it easy to see why it’s important to act sooner rather than later.

The Future of Trickbot

Trickbot itself may or may not survive this effort to end its attacks, but the techniques will and the code behind it may — and once it's gone, there will be a replacement. Criminals are making a significant amount of money with these operations, and there will always be another one ready to replace the one that gets shut down.

While this disruption is a real victory, vigilance is still required.

About the Author

Security Architect, 1Password

Adam Caudill is a security architect at 1Password, and has 20 years of experience in research, security and software development. Adam's main areas of focus include application security, secure communications and cryptography. He is also an active blogger, speaker and trainer, open source contributor, and advocate for user privacy and protection.
