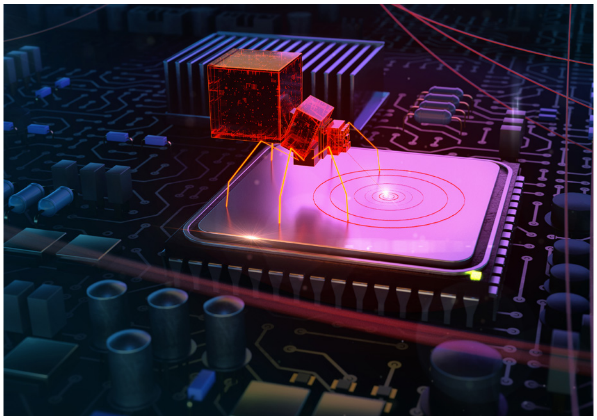
BLM-Themed Malspam Delivers Trickbot Banking Trojan

Author: Eric Patterson



Overview

On 25 June, Infoblox observed a Black Lives Matters (BLM)-themed malicious spam (malspam) campaign delivering Trickbot malware.[1,2,3] The previous Trickbot campaign we wrote about employed an email lure that spoofed an alert from the World Health Organization regarding the Coronavirus pandemic.[4]

Customer Impact

Considered a successor to the Dyre banking trojan, Trickbot was first discovered in 2016 and has since grown in popularity.[5,6,7] Trickbot infects victims, steals sensitive financial information and exfiltrates it to its command and control (C2) server. It can also move laterally within a network by brute-forcing Remote Desktop Protocol (RDP) credentials.

Threat actors favor Trickbot due to its modular nature, which facilitates customization and provides attackers the capability to drop additional malware such as Emotet on an infected system.

Campaign Analysis

The emails we observed in this campaign all portrayed themselves to be from official-sounding sources such as the “State Authority” or “Country Administration,” which do not actually exist.

The email subject lines varied, asking the recipient to vote on or express how they felt about the BLM movement. The message bodies followed this theme, asking recipients to anonymously leave their reviews on the subject matter. The bodies also indicated that some sort of claim was attached. The accompanying files were Microsoft Word documents that followed the naming scheme: *e-vote_form <4-5 digits>.doc*.

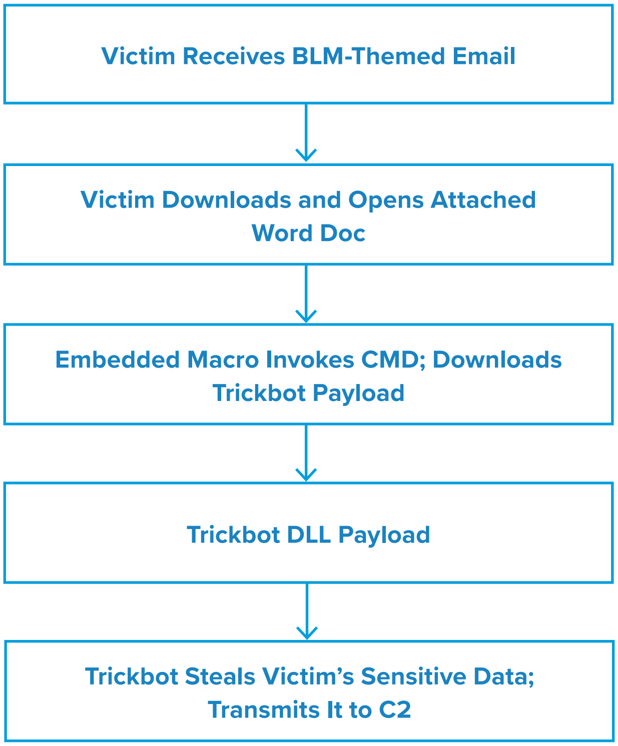
Attack Chain

When the user opens the attached file, they are prompted to enable editing and then enable content. Once this is done, an embedded macro will invoke *cmd.exe* to download the Trickbot dynamic-link library (DLL) payload.

After Trickbot successfully installs itself, it attempts to steal sensitive victim data, establish communications with its C2 infrastructure to transmit information, and potentially download additional malware onto the infected device.

Some researchers have noted an unexplained delay of up to two weeks from when they enabled content to when they received the Trickbot DLL on their system.

There were no indications that the Trickbot sample in this campaign went on to download additional malware or that it carried out further exploitation. Given the length of time taken to download the TrickBot payload, this may change in the coming weeks if the threat actor(s) have intentionally time-delayed additional malware payloads.



Victim Receives BLM-Themed Email

Victim Downloads and Opens Attached Word Doc

Embedded Macro Invokes CMD; Downloads Trickbot Payload

Trickbot DLL Payload

Trickbot Steals Victim's Sensitive Data; Transmits It to C2

Vulnerabilities & Mitigation

Trickbot is a prolific banking trojan that is capable of stealing user credentials, invoking additional software such as the Mimikatz password-stealing tool, and gaining machine persistence. Infoblox recommends the following methods for detecting, preventing, and mitigating Trickbot threats:

- Install and run advanced antivirus software that can detect, quarantine, and remove malware.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Develop traffic rules that can block outbound access to potentially malicious endpoints based on domains or unique URI parameters.
- Implement command prompt logging to detect any anomalous or malicious use.
- Install strong email security solutions to detect emails with suspicious content.

Endnotes

1. https://twitter.com/malware_traffic/status/1276193322999123972
2. https://twitter.com/abuse_ch/status/1275526243404972034
3. https://news.zepko.com/black-lives-matter-email-campaign-delivers-trickbot-malware/
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--66
5. https://blog.malwarebytes.com/detections/trojan-trickbot/
6. https://www.fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/
7. https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com