Trickbot disrupted

microsoft.com/security/blog/2020/10/12/trickbot-disrupted/

October 12, 2020

As announced today, Microsoft took action against the Trickbot botnet, disrupting one of the world's most persistent malware operations. Microsoft worked with telecommunications providers around the world to disrupt key Trickbot infrastructure. As a result, operators will no longer be able to use this infrastructure to distribute the Trickbot malware or activate deployed payloads like ransomware.

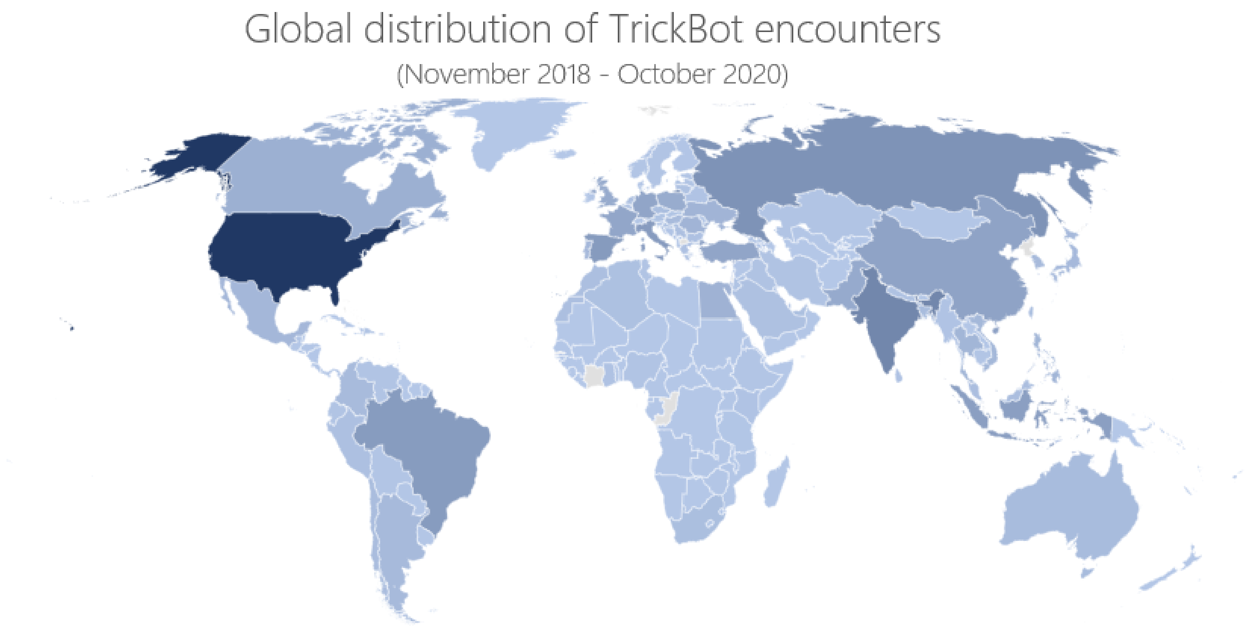
Microsoft actively tracks the threat landscape, monitoring threat actors, their campaigns, specific tactics, and evolution of malware. We share this intelligence with the community and use our research to continuously improve our products. Below, we will detail the evolution of the Trickbot malware, associated tactics, recent campaigns, and dive into the anatomy of a particular attack we observed.

Trickbot was first spotted in 2016 as a banking trojan that was created as a successor to Dyre and designed to steal banking credentials. Over the years, Trickbot's operators were able to build a massive botnet, and the malware evolved into a modular malware available for malware-as-a-service. The Trickbot infrastructure was made available to cybercriminals who used the botnet as an entry point for human-operated campaigns, including attacks that steal credentials, exfiltrate data, and deploy additional payloads, most notably Ryuk ransomware, in target networks.

Trickbot was typically delivered via email campaigns that used current events or financial lures to entice users to open malicious file attachments or click links to websites hosting the malicious files. Trickbot campaigns usually used Excel or Word documents with malicious macro codes, but other types of attachments have been used. The campaigns were observed in a wide range of verticals and geolocation, with operators frequently reusing previously compromised email accounts from earlier campaigns to distribute emails without narrowing targets.

In addition to phishing emails, Trickbot was also deployed through lateral movement via Server Message Block (SMB) or as a second-stage payload of other malware like Emotet. Once Trickbot was launched, operators utilized it to install reconnaissance tools like PowerShell Empire, Metasploit, and Cobalt Strike. They used these tools to steal credentials and network configuration information, move laterally to high-value assets, or deliver additional malicious payloads.

Threat data from Microsoft 365 Defender, which correlates signals from endpoints, email and data, identities, and cloud apps to deliver comprehensive protection against threats, shows that Trickbot showed up in both large and small enterprises across the globe, helped no doubt by its modular nature and widespread misconception of it being a “commodity” banking trojan.


Global distribution of TrickBot encounters
(November 2018 - October 2020)

Anatomy of a Trickbot campaign

Trickbot is one of the most prolific malware operations in the world, churning out multiple campaigns in any given period. In one specific campaign, the Trickbot operators used several disparate compromised email accounts to send out hundreds of malicious emails to both enterprise and consumer accounts. Recipients were from a variety of industry verticals and geolocations and do not appear to have been specifically targeted. This campaign used a shipping and logistics theme, and had the following subject lines:

- Shipment receipt
- Delivery finished
- Urgent receipt comment
- Essential receipt reminder
- Required declaration

The emails contained a malicious Excel attachment that, when opened, prompted the user to enable macros. If enabled, the macro wrote a malicious JScript Encoded (JSE) file to the disk, which is then executed via WScript. The JSE script connected to the affected organization’s domain controller and performed several LDAP queries to gather information about Active Directory, including the schema and user lists. The script then exfiltrated the information to attacker-controlled infrastructure. The script used the jscript.encode command to encode both server-side and client-side files in order to obfuscate content and evade detection.

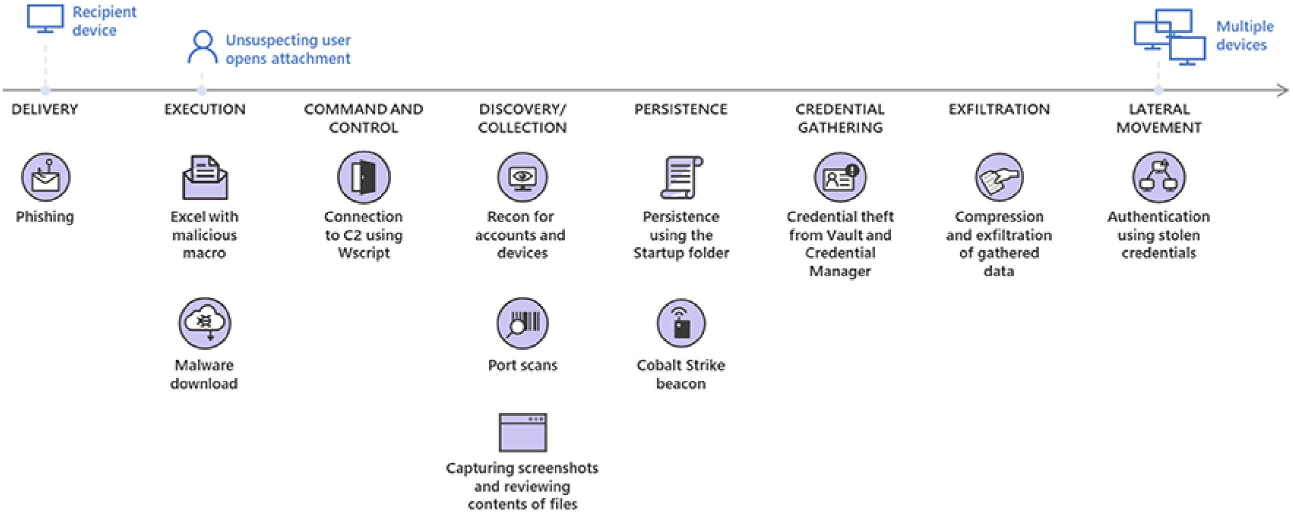
Next, the JSE file performed several reconnaissance queries to obtain information about the device’s network adapter, antivirus products, domain role, and email. Once the exfiltration was completed, a dropped .bat file established a connection with two separate C2 servers: an IP address and a domain hosted on a separate IP address. Trickbot used both these C2 servers to evade network filtering configurations. The .bat file performed reconnaissance commands to find domain administrators on the network. It then dropped and launched the Greenshot screenshot tool and Cobalt Strike beacon on the device.

At this point, the operators had gained control of the affected device, only 8.5 hours after the user opened the malicious email attachment. The operators then started to copy the freeware tool ADFind.exe, which they used for discovery as well as for gathering domain configuration and organization information. They then archived data found during this discovery to a .7z file for later exfiltration.

The attackers ran several commands to obtain information about the domain controller and gather Kerberos tickets, conducted port scanning on SMB port 445, NetBIOS 139, and queried LDAP for multiple server devices. Using the information gathered, attackers pinged several potentially high-value devices. From there, they viewed the contents of specific text and log files, likely gleaned from their reconnaissance. Upon finding a device with an open port 445, they used runas /netonly (logon type 9, which is intentionally used to confuse analysis of logon events) for authentication and interactively executed commands on the device.

Once authenticated, the attackers viewed existing RDP files from prior unrelated sessions for RDP settings and credentials. From there, they dropped a Trickbot executable and stole credentials from the Windows Vault and Credentials Manager, allowing the attackers to evade many well-known security mechanisms that monitor processes accessing Local Security Authority Subsystem Service (LSASS) memory to dump the credentials. They used a .bat file to view multiple shares, ping additional servers, and read several text files. Finally, the attackers exfiltrated all gathered data.

The attackers persisted in the network via a copy of the malicious .jse file in the Startup folder. Using this .jse file, they have the capability to return to this network later and attempt to log on to other, more valuable devices and steal additional information or drop additional payloads. This highlights the importance of comprehensive response to “commodity malware” like Trickbot: the original banking trojan infection may be triaged and remediated, but without a full understanding of Trickbot as an entry vector to human adversaries, the real threat remains in the network.


Recipient device
Unsuspecting user opens attachment
Multiple devices
DELIVERY
EXECUTION
COMMAND AND CONTROL
DISCOVERY/ COLLECTION
PERSISTENCE
CREDENTIAL GATHERING
EXFILTRATION
LATERAL MOVEMENT
Phishing
Excel with malicious macro
Connection to C2 using Wscript
Recon for accounts and devices
Persistence using the Startup folder
Credential theft from Vault and Credential Manager
Compression and exfiltration of gathered data
Authentication using stolen credentials
Malware download
Port scans
Cobalt Strike beacon
Capturing screenshots and reviewing contents of files

Modular, multi-stage malware

Trickbot is a multi-stage malware typically composed of a wrapper, a loader, and a main malware module. The wrapper, which uses multiple templates that constantly change, is designed to evade detection by producing unique samples, even if the main malware code remains the same.

When the wrapper process runs, it runs the loader fully in its memory. The loader has a highly modular design. It decrypts each function at runtime before running it, and then encrypts it back. Likewise, all human-readable strings are decrypted and all APIs are resolved at runtime. In some scenarios, Trickbot uses UAC bypasses to elevate the privileges of its processes. On 64-bit systems, Trickbot uses the “Heaven’s Gate” technique to switch 32-bit code to 64-bit, and has an additional stage where a 64-bit loader injects the main module into the suspended process.

The loader runs the main malware module directly in memory. After creating scheduled tasks for persistence, the main malware module decrypts a configuration file, which contains the information it needs for its next steps:

- Establish HTTPS communication with command and control (C2) server
- Download modules from the C2 server
- Monitor the status of the downloaded modules
- Synchronize communication between the main module and the downloaded modules

The modules are likewise run in memory via injection into the suspended process. Over the years, Trickbot has used a wide range of modules for various malicious activities. These include the following:

Modules	Purpose

pwgrab	Gathers credentials, autofill data, history and so on from browsers
networkDll	Gathers network and system information
importDll	Gathers browser data
injectDll	Main banker module; uses static and dynamic web browser injection and data theft
tabDll	Propagates Trickbot via EternalRomance Exploit
	Propagates Trickbot via SMB EternalBlue Exploit
shareDll	Propagates Trickbot via Windows network shares
vncDll, BCTestDll	Remote control/Virtual Network Computing module; provides backdoor for further module downloads
rdpscanDll	Launches brute force attacks against selected Windows systems running Remote Desktop Protocol (RDP) connection exposed to the Internet
Systeminfo	Gathers system information
mailsearcher	Searches all files on disk and compares their extensions to a predefined list to harvest emails addresses
outlookDll	Gather Outlook credentials
psfin	Gathers point of sale (POS) software credentials
squlDll	Gathers email addresses stored in SQL servers
aDll	Runs various commands on a Windows domain controller to steal Active Directory credentials

Trickbot sends information like domain names and IP ranges of compromised networks back to operators, who then select some of these networks for additional exploitation and reconnaissance activities. On selected networks, Trickbot operators installed additional tools like Cobalt Strike, and switch to a hands-on-keyboard attacks. Once the operators gain foothold on a network, they used tools like Mimikatz and LaZagne to steal additional credentials and tools like BloodHound and ADFind to perform reconnaissance actions. Apart from using the stolen credentials and collected data to further the attack, operators also exfiltrated data. They then leave multiple persistence points on the network to enable the eventual delivery of other payloads like Ryuk ransomware.

While much has been made of the Trickbot’s supposed antivirus evasion capabilities, it’s a simple PowerShell command being run to turn off Microsoft Defender Antivirus, but it can perform this action only if the user has administrative rights.

Recent prominent Trickbot campaigns

In June 2020, we tracked multiple Trickbot campaigns. As is typical with Trickbot, some of the email campaigns took advantage of current events as lures to entice users to click on malicious attachments. These lures include Black Lives Matter and COVID-19. Earlier in the year, we reported that Trickbot was the most prolific malware operation using COVID-19-themed lures. Many other simultaneous campaigns used more generic lures, such as shipping and logistics, invoicing and payments, customer complaints, and various financial lures.

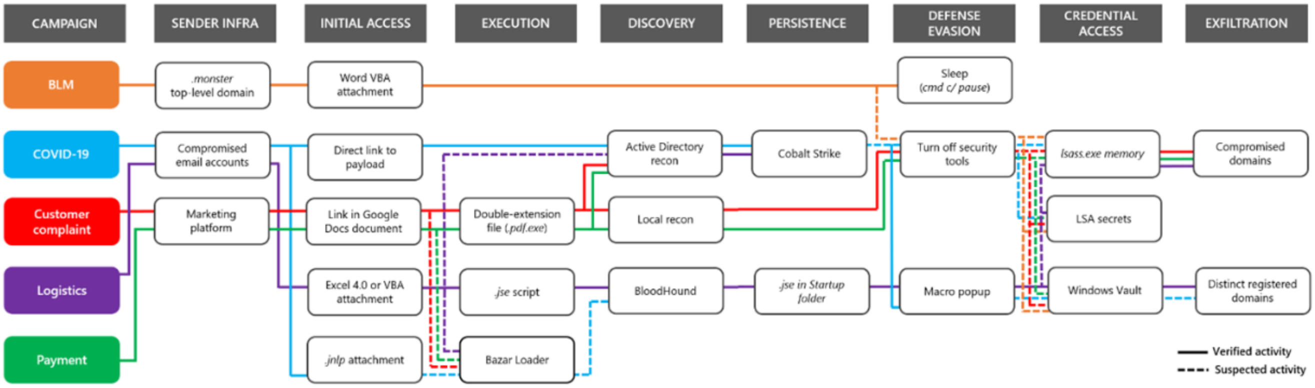
The email body was often simple but maintained consistency with the lure used in the subject line. The emails used a wide range of attachment types, including:

- Word macro attachments
- Excel VBA macro attachments
- Excel 4.0 macro attachments
- Java Network Launch Protocol (.jnlp) attachments

Some campaigns do away with the attachments and instead use malicious links to websites that host malicious files.

The sender infrastructure for all these emails varied as well. In most campaigns, operators used compromised legitimate email accounts and compromised marketing platforms to distribute the malicious emails. However, in one instance, the operators registered several domains using less popular top-level domains (TLDs) such as “.monster” and “.us” to create their own mail server and send malicious emails from attacker-defined email addresses. At least one of these campaigns used attacker-owned email sender infrastructure that was later used to deliver Dridex malware in a separate campaign. The Dridex malware is known to be associated with the CHIMBORAZO (also known as TA505) crime group. Additionally, CHIMBORAZO ran simultaneous campaigns that delivered Trickbot.

The following graphic illustrates the various campaigns, tactics, and techniques used by the operators. The complexity of these simultaneous campaigns and techniques indicates that this is a coordinated and professional effort conducted by a sophisticated activity group.



Extended detection and response for the full range of threats

The action against Trickbot is one of the ways in which Microsoft provide real-world protection against threats. This action will result in protection for a wide range of organizations, including financial services institutions, government, healthcare, and other verticals from malware and human-operated campaigns delivered via the Trickbot infrastructure.

In the recently released Microsoft Digital Defense Report, we called out that cybercriminals of all skill sets take advantage of the perception that commodity threats are less impactful to businesses. Trickbot is proof that this assumption is obsolete, and organizations need to treat and address Trickbot and other malware infections as the broadly damaging threats that they are.

To help protect customers from the full range of threats, from common malware to highly modular, multi-stage threats like Trickbot, as well as nation-state level attacks, Microsoft 365 Defender delivers coordinated protection for identities, endpoints, cloud apps, email and documents. Microsoft Defender for Office 365 detects malicious attachments and links in email campaigns. Microsoft Defender for Endpoint detects and blocks the Trickbot malware and all related components, as well as malicious activities on endpoints. Microsoft Defender for Identity identifies and detects suspicious user activities and compromised identities.

This breadth of cross-domain visibility allows Microsoft 365 Defender to correlate signals and comprehensively detect and resolve attack chains. Security operations teams can then use the rich set of tools in Microsoft 365 Defender to further hunt for threats and gain insights for hardening networks from compromise.

Microsoft 365 Defender Threat Intelligence Team

Microsoft 365 Defender Research Team

Digital Crimes Unit (DCU)

Detection and Response Team (DART)

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft 365 Defender tech community.

Read all Microsoft security intelligence blog posts.

Follow us on Twitter **@MsftSecIntel**.