JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: AA21-076A

March 17, 2021

TrickBot Malware

SUMMARY

***Callout Box**: This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.*

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) have observed continued targeting through spearphishing campaigns using TrickBot malware in North America. A sophisticated group of cybercrime actors is luring victims, via phishing emails, with a traffic infringement phishing scheme to download TrickBot.

TrickBot—first identified in 2016—is a Trojan developed and operated by a sophisticated group of cybercrime actors. Originally designed as a banking Trojan to steal financial data, TrickBot has evolved into highly modular, multi-stage malware that provides its operators a full suite of tools to conduct a myriad of illegal cyber activities.

To secure against TrickBot, CISA and FBI recommend implementing the mitigation measures described in this Alert, which include blocking suspicious Internet Protocol addresses, using antivirus software, and providing social engineering and phishing training to employees.

TECHNICAL DETAILS

TrickBot is an advanced Trojan that malicious actors spread primarily by spearphishing campaigns using tailored emails that contain malicious attachments or links, which—if enabled—execute malware (*Phishing: Spearphishing Attachment* [T1566.001], *Phishing: Spearphishing Link* [T1566.002]). CISA and FBI are aware of recent attacks that use phishing emails, claiming to contain proof of a traffic violation, to steal sensitive information. The phishing emails contain links that redirect to a website hosted on a compromised server that prompts the victim to click on photo proof of their traffic violation. In clicking the photo, the victim unknowingly downloads a malicious JavaScript file that, when opened, automatically communicates with the malicious actor's command and control (C2) server to download TrickBot to the victim's system.

Attackers can use TrickBot to:

- Drop other malware, such as Ryuk and Conti ransomware, or
- Serve as an Emotet downloader.[1]

TrickBot uses person-in-the-browser attacks to steal information, such as login credentials (*Man in the Browser* [T1185]). Additionally, some of TrickBot's modules spread the malware laterally across a network by abusing the Server Message Block (SMB) Protocol. TrickBot operators have a toolset capable of spanning the entirety of the MITRE ATT&CK framework, from actively or passively gathering information that can be used to support targeting (*Reconnaissance* [TA0043]), to trying to manipulate, interrupt, or destroy systems and data (*Impact* [TA0040]).

TrickBot is capable of data exfiltration, cryptomining, and host enumeration (e.g., reconnaissance of Unified Extensible Firmware Interface or Basic Input/Output System [UEFI/BIOS] firmware).[2] For host enumeration, operators deliver TrickBot in modules containing a configuration file with specific tasks.

Figure 1 lays out TrickBot's use of enterprise techniques.

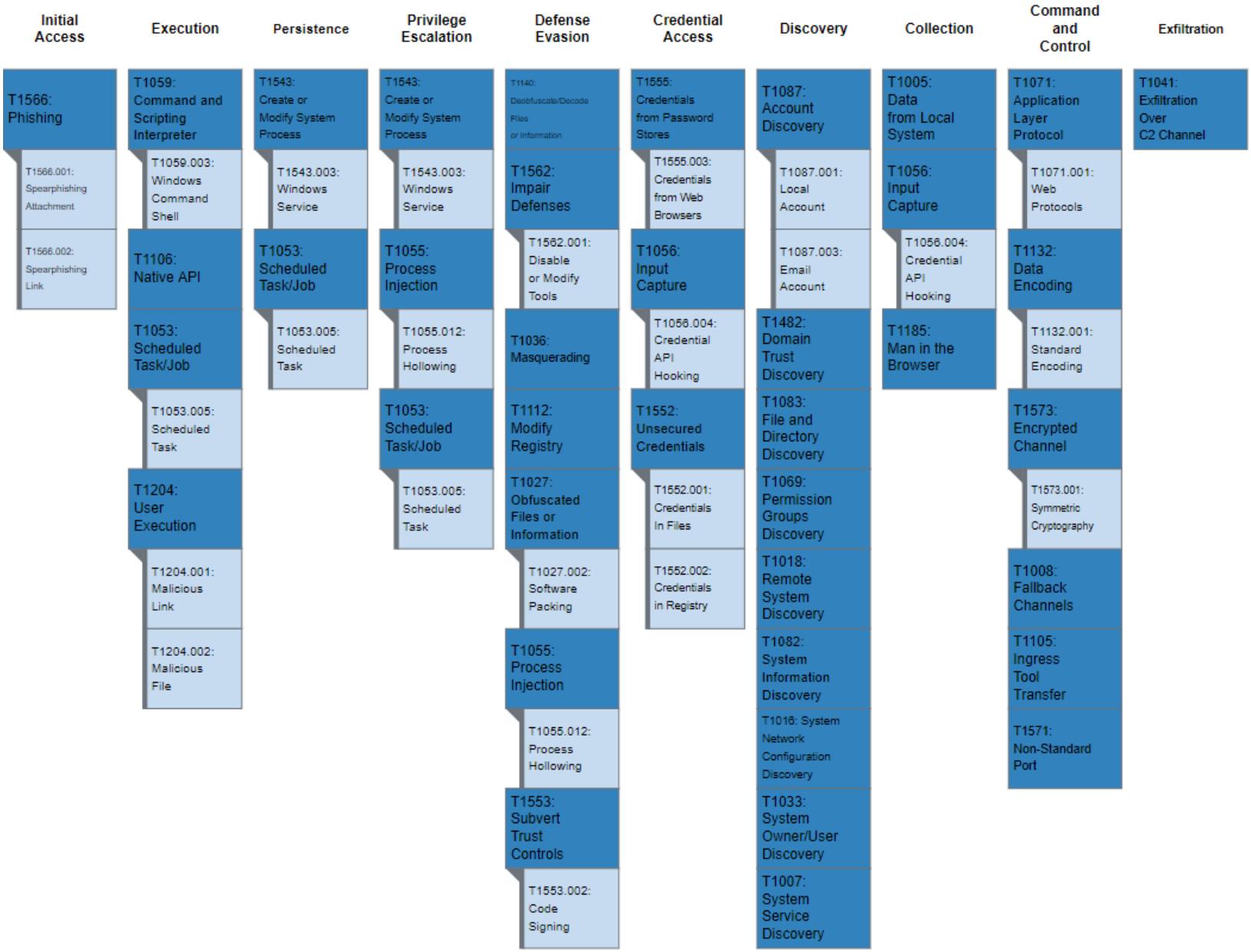

Figure 1: MITRE ATT&CK enterprise techniques used by TrickBot

MITRE ATT&CK TECHNIQUES

According to MITRE, *TrickBot* [S0266] uses the ATT&CK techniques listed in table 1.

Table 1: TrickBot ATT&CK techniques for enterprise

Technique Title	ID	Use
***Initial Access* [TA0001]**		
Phishing: Spearphishing Attachment	T1566.001	TrickBot has used an email with an Excel sheet containing a malicious macro to deploy the malware.
Phishing: Spearphishing Link	T1566.002	TrickBot has been delivered via malicious links in phishing emails.
***Execution* [TA0002]**		
Scheduled Task/Job: Scheduled Task	T1053.005	TrickBot creates a scheduled task on the system that provides persistence.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	TrickBot has used macros in Excel documents to download and deploy the malware on the user's machine.
Native API	T1106	TrickBot uses the Windows Application Programming Interface (API) call, CreateProcessW(), to manage execution flow.
User Execution: Malicious Link	T1204.001	TrickBot has sent spearphishing emails in an attempt to lure users to click on a malicious link.
User Execution: Malicious File	T1204.002	TrickBot has attempted to get users to launch malicious documents to deliver its payload.
***Persistence* [TA0003]**		
Scheduled Task/Job: Scheduled Task	T1053.005	TrickBot creates a scheduled task on the system that provides persistence.
Create or Modify System Process: Windows Service	T1543.003	TrickBot establishes persistence by creating an autostart service that allows it to run whenever the machine boots.
***Privilege Escalation* [TA0004]**		
Scheduled Task/Job: Scheduled Task	T1053.005	TrickBot creates a scheduled task on the system that provides persistence.

Process Injection: Process Hollowing	T1055.012	TrickBot injects into the svchost.exe process.
Create or Modify System Process: Windows Service	T1543.003	TrickBot establishes persistence by creating an autostart service that allows it to run whenever the machine boots.
***Defense Evasion* [TA0005]**		
Obfuscated Files or Information	T1027	TrickBot uses non-descriptive names to hide functionality and uses an AES CBC (256 bits) encryption algorithm for its loader and configuration files.
Obfuscated Files or Information: Software Packing	T1027.002	TrickBot leverages a custom packer to obfuscate its functionality.
Masquerading	T1036	The TrickBot downloader has used an icon to appear as a Microsoft Word document.
Process Injection: Process Hollowing	T1055.012	TrickBot injects into the svchost.exe process.
Modify Registry	T1112	TrickBot can modify registry entries.
Deobfuscate/Decode Files or Information	T1140	TrickBot decodes the configuration data and modules.
Subvert Trust Controls: Code Signing	T1553.002	TrickBot has come with a signed downloader component.
Impair Defenses: Disable or Modify Tools	T1562.001	TrickBot can disable Windows Defender.
***Credential Access* [TA0006]**		
Input Capture: Credential API Hooking	T1056.004	TrickBot has the ability to capture Remote Desktop Protocol credentials by capturing the CredEnumerateA API.
Unsecured Credentials: Credentials in Files	T1552.001	TrickBot can obtain passwords stored in files from several applications such as Outlook, Filezilla, OpenSSH, OpenVPN and WinSCP. Additionally, it searches for the .vnc.lnk affix to steal VNC credentials.
Unsecured Credentials: Credentials in Registry	T1552.002	TrickBot has retrieved PuTTY credentials by querying the

		Software\SimonTatham\Putty\Sessions registry key.
Credentials from Password Stores	T1555	TrickBot can steal passwords from the KeePass open-source password manager.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	TrickBot can obtain passwords stored in files from web browsers such as Chrome, Firefox, Internet Explorer, and Microsoft Edge, sometimes using esentutl.
***Discovery* [TA0007]**		
System Service Discovery	T1007	TrickBot collects a list of install programs and services on the system's machine.
System Network Configuration Discovery	T1016	TrickBot obtains the IP address, location, and other relevant network information from the victim's machine.
Remote System Discovery	T1018	TrickBot can enumerate computers and network devices.
System Owner/User Discovery	T1033	TrickBot can identify the user and groups the user belongs to on a compromised host.
Permission Groups Discovery	T1069	TrickBot can identify the groups the user on a compromised host belongs to.
System Information Discovery	T1082	TrickBot gathers the OS version, machine name, CPU type, amount of RAM available from the victim's machine.
File and Directory Discovery	T1083	TrickBot searches the system for all of the following file extensions: .avi, .mov, .mkv, .mpeg, .mpeg4, .mp4, .mp3, .wav, .ogg, .jpeg, .jpg, .png, .bmp, .gif, .tiff, .ico, .xlsx, and .zip. It can also obtain browsing history, cookies, and plug-in information.
Account Discovery: Local Account	T1087.001	TrickBot collects the users of the system.
Account Discovery: Email Account	T1087.003	TrickBot collects email addresses from Outlook.
Domain Trust Discovery	T1482	TrickBot can gather information about domain trusts by utilizing Nltest.

***Collection* [TA0009]**		
Data from Local System	T1005	TrickBot collects local files and information from the victim's local machine.
Input Capture: Credential API Hooking	T1056.004	TrickBot has the ability to capture Remote Desktop Protocol credentials by capturing the CredEnumerateA API.
Person in the Browser	T1185	TrickBot uses web injects and browser redirection to trick the user into providing their login credentials on a fake or modified webpage.
***Command and Control* [TA0011]**		
Fallback Channels	T1008	TrickBot can use secondary command and control (C2) servers for communication after establishing connectivity and relaying victim information to primary C2 servers.
Application Layer Protocol: Web Protocols	T1071.001	TrickBot uses HTTPS to communicate with its C2 servers, to get malware updates, modules that perform most of the malware logic and various configuration files.
Ingress Tool Transfer	T1105	TrickBot downloads several additional files and saves them to the victim's machine.
Data Encoding: Standard Encoding	T1132.001	TrickBot can Base64-encode C2 commands.
Non-Standard Port	T1571	Some TrickBot samples have used HTTP over ports 447 and 8082 for C2.
Encrypted Channel: Symmetric Cryptography	T1573.001	TrickBot uses a custom crypter leveraging Microsoft's CryptoAPI to encrypt C2 traffic.
***Exfiltration* [TA0010]**		
Exfiltration Over C2 Channel	T1041	TrickBot can send information about the compromised host to a hardcoded C2 server.

DETECTION

Signatures

CISA developed the following snort signature for use in detecting network activity associated with TrickBot activity.

```
alert tcp any [443,447] -> any any (msg:"TRICKBOT:SSL/TLS Server X.509 Cert Field
contains 'example.com' (Hex)"; sid:1; rev:1; flow:established,from_server;
ssl_state:server_hello; content:"|0b|example.com"; fast_pattern:only;
content:"Global Security"; content:"IT Department";
pcre:"/(?:\x09\x00\xc0\xb9\x3b\x93\x72\xa3\xf6\xd2|\x00\xe2\x08\xff\xfb\x7b\x53\x
76\x3d)/"; classtype:bad-unknown; metadata:service ssl,service and-ports;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT_ANCHOR:HTTP URI GET contains
'/anchor'"; sid:1; rev:1; flow:established,to_server; content:"/anchor";
http_uri; fast_pattern:only; content:"GET"; nocase; http_method;
pcre:"/^\/anchor_?.{3}\/[\w_-]+\.[A-F0-9]+\/?$/U"; classtype:bad-unknown;
priority:1; metadata:service http;)
```

```
alert tcp any $SSL_PORTS -> any any (msg:"TRICKBOT:SSL/TLS Server X.509 Cert
Field contains 'C=XX, L=Default City, O=Default Company Ltd'"; sid:1; rev:1;
flow:established,from_server; ssl_state:server_hello; content:"|31 0b 30 09 06 03
55 04 06 13 02|XX"; nocase; content:"|31 15 30 13 06 03 55 04 07 13 0c|Default
City"; nocase; content:"|31 1c 30 1a 06 03 55 04 0a 13 13|Default Company Ltd";
nocase; content:!"|31 0c 30 0a 06 03 55 04 03|"; classtype:bad-unknown;
reference:url,www.virustotal.com/gui/file/e9600404ecc42cf86d38deedef94068db39b7a0
fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP Client Header contains
'boundary=Arasfjasu7'"; sid:1; rev:1; flow:established,to_server;
content:"boundary=Arasfjasu7|0d 0a|"; http_header;
content:"name=|22|proclist|22|"; http_header; content:!"Referer";
content:!"Accept"; content:"POST"; http_method; classtype:bad-unknown;
metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP Client Header contains
'User-Agent|3a 20|WinHTTP loader/1.'"; sid:1; rev:1; flow:established,to_server;
content:"User-Agent|3a 20|WinHTTP loader/1."; http_header; fast_pattern:only;
content:".png|20|HTTP/1.";
pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}(?:\x3a\d{2,5})?$/mH";
```

```
content:!"Accept"; http_header; content:!"Referer|3a 20|"; http_header;
classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any $HTTP_PORTS -> any any (msg:"TRICKBOT:HTTP Server Header contains
'Server|3a 20|Cowboy'"; sid:1; rev:1; flow:established,from_server;
content:"200"; http_stat_code; content:"Server|3a 20|Cowboy|0d 0a|"; http_header;
fast_pattern; content:"content-length|3a 20|3|0d 0a|"; http_header; file_data;
content:"/1/"; depth:3; isdataat:!1,relative; classtype:bad-unknown;
metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP URI POST contains C2
Exfil"; sid:1; rev:1; flow:established,to_server; content:"Content-Type|3a
20|multipart/form-data|3b 20|boundary=------Boundary"; http_header; fast_pattern;
content:"User-Agent|3a 20|"; http_header; distance:0; content:"Content-Length|3a
20|"; http_header; distance:0; content:"POST"; http_method; pcre:"/^\/[a-
z]{3}\d{3}\/.+?\.[A-F0-9]{32}\/\d{1,3}\//U";
pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}$/mH"; content:!"Referer|3a|";
http_header; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP URI GET/POST contains '/56evcxv'
(Trickbot)"; sid:1; rev:1; flow:established,to_server; content:"/56evcxv";
http_uri; fast_pattern:only; classtype:bad-unknown; metadata:service http;)
```

```
alert icmp any any -> any any (msg:"TRICKBOT_ICMP_ANCHOR:ICMP traffic conatins
'hanc'"; sid:1; rev:1; itype:8; content:"hanc"; offset:4; fast_pattern;
classtype:bad-unknown;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains POST with
'host|3a 20|*.onion.link' and 'data=' (Trickbot/Princess Ransomeware)"; sid:1;
rev:1; flow:established,to_server; content:"POST"; nocase; http_method;
content:"host|3a 20|"; http_header; content:".onion.link"; nocase; http_header;
distance:0; within:47; fast_pattern; file_data; content:"data="; distance:0;
within:5; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains 'host|3a
20|tpsci.com' (trickbot)"; sid:1; rev:1; flow:established,to_server;
content:"host|3a 20|tpsci.com"; http_header; fast_pattern:only; classtype:bad-
unknown; metadata:service http;)
```

MITIGATIONS

CISA and FBI recommend that network defenders—in federal, state, local, tribal, territorial governments, and the private sector—consider applying the following best practices to strengthen the security posture of their organization's systems. System owners and administrators should review any configuration changes prior to implementation to avoid negative impacts.

- Provide social engineering and phishing training to employees.
- Consider drafting or updating a policy addressing suspicious emails that specifies users must report all suspicious emails to the security and/or IT departments.
- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Adhere to the principle of least privilege.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system.
- Segment and segregate networks and functions.
- Limit unnecessary lateral communications between network hoses, segments and devices.
- Consider using application allowlisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets. Ensure that such technology only allows authorized, digitally signed scripts to run on a system.
- Enforce multi-factor authentication.
- Enable a firewall on agency workstations configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Implement an Intrusion Detection System, if not already used, to detect C2 activity and other potentially malicious network activity
- Monitor web traffic. Restrict user access to suspicious or risky sites.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against network propagation modules used by TrickBot.
- Visit the MITRE ATT&CK Techniques pages (linked in table 1 above) for additional mitigation and detection strategies.
- See CISA's Alert on Technical Approaches to Uncovering and Remediating Malicious Activity for more information on addressing potential incidents and applying best practice incident response procedures.

For additional information on malware incident prevention and handling, see the National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

RESOURCES

- CISA Fact Sheet: TrickBot Malware
- MS-ISAC White Paper: Security Primer – TrickBot
- United Kingdom National Cyber Security Centre Advisory: Ryuk Ransomware Targeting Organisations Globally
- CISA and MS-ISAC Joint Alert AA20-280A: Emotet Malware
- MITRE ATT&CK for Enterprise

REFERENCES

[1] FireEye Blog – A Nasty Trick: From Credential Theft Malware to Business Disruption

[2] Eclypsium Blog – TrickBot Now Offers 'TrickBoot': Persist, Brick, Profit