

# Threat Report: TrickBot Banking Trojan

April 8, 2021



## Table of Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>EXECUTIVE SUMMARY</b> .....                 | <b>3</b>  |
| <b>2</b> | <b>Detection – Anatomy of TrickBot</b> .....   | <b>5</b>  |
| 2.1      | Phishing Malspam – T1566 .....                 | 5         |
| 2.2      | Execution - T1204.....                         | 5         |
| 2.3      | Persistence - TA0003.....                      | 7         |
| 2.4      | Defense Evasion - TA0030.....                  | 7         |
| 2.5      | Credentia gathering - TA0006 .....             | 7         |
| 2.6      | Discovery / Collection – TA0007.....           | 8         |
| 2.7      | Command and control - TA0011.....              | 8         |
| <b>3</b> | <b>Monitoring and Mitigation</b> .....         | <b>9</b>  |
| 3.1      | Recommended Monitoring for Detection .....     | 9         |
| 3.2      | Prevention Methods.....                        | 9         |
| 3.3      | Detection controls .....                       | 10        |
| 3.4      | Organizational Best Practices .....            | 10        |
| <b>4</b> | <b>TrickBot Indicators of Compromise</b> ..... | <b>11</b> |
| <b>5</b> | <b>References</b> .....                        | <b>14</b> |

# 1 EXECUTIVE SUMMARY

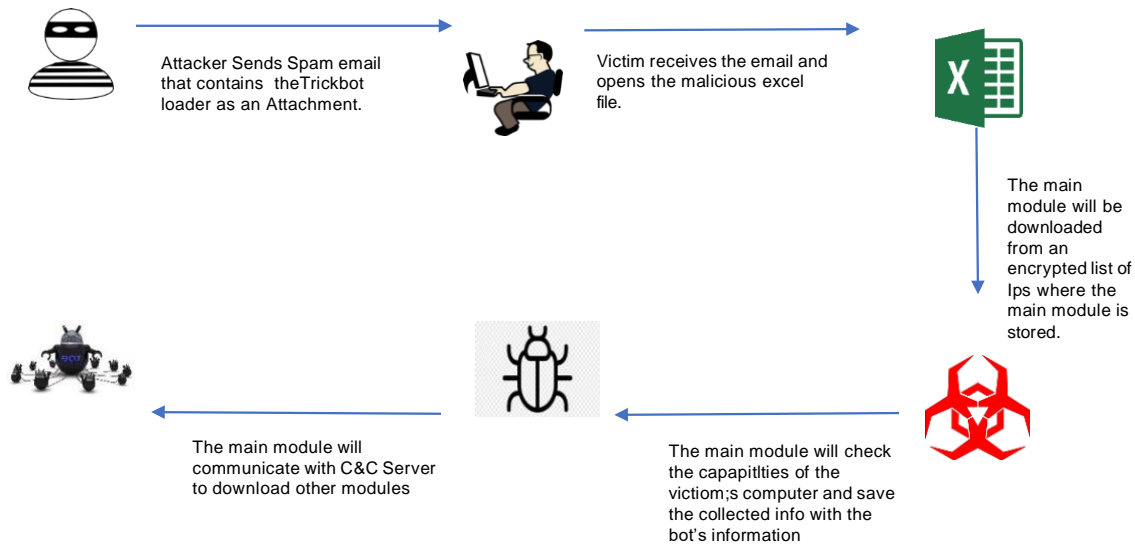
TrickBot is one of the most dangerous banking trojans due to the sophisticated techniques it employs and is mostly operated by threat actors TA505 and Wizard Spider. It was first uncovered in September 2016 and has a global reach, infecting more than a million computing devices and stealing millions of dollars from banking institutions and health care providers. Security researchers believe that it was developed by the same criminal group behind Dyre Ransomware, which suddenly stopped in late 2015, because its source code appears to be a rewritten version of Dyre.

Over the past few years, TrickBot has evolved and currently offers a full list of tools that provide a myriad of malicious activities, such as credential harvesting, data exfiltration, crypto mining, and the ability to deploy other malware such as Ryuk ransomware. This allows TrickBot to be flexible, customizable, and easily made available for cybercriminals to use in a Malware-as-a-Service model.

The preferred method used by threat actors to distribute TrickBot is the spear phishing email. These emails contain a financial lure to trick victims into opening malicious attachments and/or clicking on links that host malicious files. Malicious files are delivered in different formats, such as zipped scripts (WSF, VBS) and Microsoft Office documents (Word, Excel). Similar to other cybercriminals, TrickBot threat actors have taken advantage of current world trends with phishing campaigns leveraging different topics like COVID-19 and Black Lives Matter, enticing victims to click on malicious documents or links.

TrickBot is modular malware so it can perform many malicious activities. Its first module is the loader which contains an encrypted list of IP addresses from where it can download its main module. As shown by Figure 1, once downloaded, it starts collecting the infected machine's information and initiates a communication channel with a preconfigured list of C2 servers. It may also attempt to exploit different vulnerabilities to move laterally inside victims' networks and install itself on other computers. The Cysiv threat research team has analyzed different variants of the TrickBot banking trojan to help overcome these challenges and help ensure our clients are well-protected.

Figure 1 – TrickBot Infection Method



### Protection Provided by Cysiv:

Cysiv SOC-as-a-Service provides protection from a broad range of threats:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Human-led threat hunting helps to identify suspicious activity and digital footprints that are indicative of an intrusion.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.

## 2 DETECTION – ANATOMY OF TRICKBOT

Use the information provided in this section to study the key artifacts and behaviors of TrickBot so you can scan your system, determine if it is vulnerable, perform in-depth digital forensics, and help mitigate the impact.

### 2.1 Phishing Malspam – T1566

Most attackers tend to use phishing malspam as the most effective way of delivering TrickBot. An email is spammed to a list of addresses with a compelling subject line – the attention surrounding the COVID pandemic has recently been leveraged to entice users to open the malicious email, which typically contains a malicious MS Office file or a malicious link.

Figure 2 – Sample of Received TrickBot Malspam Email

From: Shallet.caldeira@motilaloswal.com  
 To:  
 Date: 08 Mar. 2021, 11:31:06  
 Policy: Inbound Default/Anti-Virus  
 Message type: Virus  
 Header: [Show headers](#)  
 Attachment: [Outstand Reminder.qz](#) [best.qif](#)  
 Subject: Outstanding Reminder

Dear Sir. Kindly find attached the Outstanding Please click attached file and Open it for Outstanding Reminder. For Motilaloswal ENTERPRISES Proprietor/Authorized Signatory

### 2.2 Execution - T1204

Once the user clicks on the malicious attachments and enables editing, a PowerShell script downloads the main module of TrickBot, the main module is executed and TrickBot then begins downloading the additional modules it needs for its programmed use case.

| Module     | Usage                                     |
|------------|---|
| importDll  | Stealing Browser Data.                    |
| cookiesDll | Stealing Cookies from infected machines.  |
| pwgrab     | Stealing credentials from browsers.       |
| networkDll | Gathering Network and System Information. |

|              |  |
|--------------|--|
| injectDll    | Main Banking Module, for injecting malicious content in browser to steal banking websites credentials. |
| tabDll       | to be spread through SMB usign many windows vulnerabilities.   |
| shareDll     | For lateral Movement and Enumeration through LDAP and SMB.   |
| vncDll       | For remote Control.  |
| rdpscanDll   | For running Brute-Force attack against RDP for spicific servers.                                       |
| mailsearcher | Search all files on desk to harvest email address.   |
| outlookDll   | Stealing OutLook Credentials.  |
| psfin        | Stealing POS software credenitals.   |

Figure – 3 Detection of Downloading TrickBot main module

```

GET /directory/lurdx.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: mamax.tk
Connection: Keep-Alive

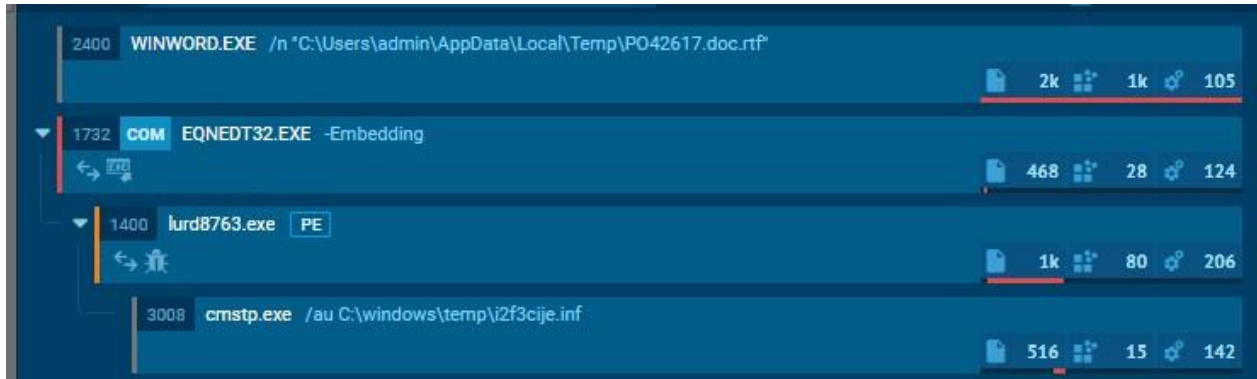
HTTP/1.1 200 OK
Date: Fri, 12 Mar 2021 16:01:27 GMT
Server: Apache/2.4.46 (CentOS)
Upgrade: h2
Connection: Upgrade, close
Last-Modified: Tue, 09 Mar 2021 12:35:30 GMT
ETag: "4c260-5bd19c92aeced"
Accept-Ranges: bytes
Content-Length: 311904
Content-Type: application/octet-stream

MZ.....@.....
!..L.!This program cannot be run in DOS mode.

$.PE.L.....".....@.
.....<.....@.
\..O.....`.....
......H.....text.....
..`rsrc.....@..@.reloc.....@..B

```

Figure – 4 Main Module is being downloaded from the Loader



## 2.3 Persistence - TA0003

TrickBot adds an entry to the “run keys” in the registry or startup, so the program is referenced to be executed when a user is logged in. Attackers use these system configurations to execute malware to maintain persistence even if the user reboots the machine.

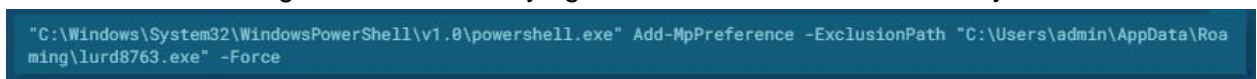
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

## 2.4 Defense Evasion - TA0030

TrickBot tries to be installed as a Scheduled Task and uses familiar names such as “Sysnsef” to remain hidden from detection. Also, it may be installed as a service that points to a copy in the system device root. Some TrickBot modules try to disable running AntiVirus tools to evade detection. This can be achieved by killing the security software process or event logging process and deleting registry keys.

Figure – 5 TrickBot trying to Create File in Admin Directory



## 2.5 Credential gathering - TA0006

TrickBot tries to search local file systems and remote file shares for files containing passwords. These files may store the credentials and/or shared credentials of users, or configuration files containing passwords for a service or system.

## 2.6 Discovery / Collection – TA0007

TrickBot uses many modules, such as “networkdll” and “psfin”, to collect local system and Network information like Domain Controllers and Kerberos, and also conducts port scanning of SMB ports, Netbios, and LDAP.

## 2.7 Command and control - TA0011

Attackers use many existing, legitimate external web services as a means for relaying commands to a compromised system. TrickBot has a predefined list of C&C servers to exfiltrate data through, so it encrypts all collected data and exfiltrates it using the HTTP protocol.



## 3 MONITORING AND MITIGATION

This section details mitigation information for TrickBot around prevention, detection and organizational best practices.

### 3.1 Recommended Monitoring for Detection

The following monitoring practices are recommended in relation to TrickBot.

- Monitor internal/external emails.
  - Monitor Web requests that first seen, newly registered and DGA domains.
  - Monitor received emails from first seen and newly registered domains.
  - Monitor for suspicious authentication activity on published services, from unexpected GeoLocations.
  - Monitor windows backup deletion.
  - Monitor for network share reconnaissance activities.
  - Monitor outgoing communications to suspicious or newly registered domains.
  - Monitor outside traffic size.
- Stay updated with the latest IOCs related to TrickBot.

### 3.2 Prevention Methods

**Patching of End User Productivity Tools** – By regularly patching end-user productivity tools like MS-Office, Adobe Acrobat Reader, organizations can minimize the exposure to weaponized attachments that include malicious code exploits and unpatched vulnerabilities.

**Disabling Macros** – A macro is a series of commands that a user can use to automate a repeated task. Attackers can use macros as an attack vector, including using macro language such as VBScript as a means of propagation, so whenever possible macros should be disabled.

**User Awareness** – Users are the prime targets of phishing campaigns and hence any effective prevention must involve training users on how to spot phishing emails and messages when they receive them and how to report them through the appropriate channels to the relevant incident response teams.

**Stay up to Date** – Most threat actors use known and exploitable vulnerabilities to attack organizations. Once a new vulnerability is discovered and disclosed or even sold on the dark web, a hacker will try to use it before organizations update their servers. So make sure to regularly maintain and update software and patch security vulnerabilities on all endpoints and software.

**Encrypt Sensitive Data** – Sensitive or classified data that you don't want anyone to access should be encrypted with a strong key and stored in a safe place so that in the event of a data breach the data will be unreadable to the attackers.

### 3.3 Detection controls

**Email Security** – Email security is a set of measures used to secure an organization's email service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts. Because of its ubiquity and inherent vulnerabilities, email is a popular vector for cyber-attacks, which can include malware, spam, and phishing. Well-configured and updated email security may detect phishing mails that contain malicious attachments and/or malicious URLs or domains, and even block them.

**Anti-Malware** – Anti-malware is software built to detect and destroy threats like viruses, malware, ransomware, spyware and others. It is mandatory for every organization to add this security layer in case of any malware attack that can affect its internal network. In many cases, phishing emails contain malicious attachments and when a victim clicks/downloads the attachment it will spread the malware to their machine. A properly configured and updated Antivirus program may detect or even prevent the malware from executing.

**Threat Hunting For IOCs** – Threat hunting is the proactive search for attack symptoms on your network, and IOCs (Indicators of Compromise) containing IPs, hashes, URLs and domains.

### 3.4 Organizational Best Practices

**Quickly Changing Passwords** – Organizations must develop detailed incident response procedures that involve the resetting of passwords of users who have received spear phishing emails or might have clicked on the links they contain. The effective implementation of this incident response procedure requires educating the users on how to report phishing emails and having the means to identify other users who might have received the malicious email and interacted with it in any way.

**Incident Response Plans** – An incident response defines the procedure for cleanup/recovery when for a discovered cybersecurity breach. It is recommended that every organization have a plan and a team dedicated to managing the incident and minimizing the damage and cost of recovery.

## 4 TRICKBOT INDICATORS OF COMPROMISE

| Indicator  | Type    |
|--|---------|
| AD41DF394F597F7F20D20A47F5DDF9514BDA74B3789AFC22105C3209F1AE77A6 | SHA-256 |
| 415E04EB340F1B092288CBCC71295A2C95E864FC1BBFCD55D6E3F5AA67099B1A | SHA-256 |
| 94AFDE50189796D71A329F77C8058E6748E473543140CF12EB5919898CC38172 | SHA-256 |
| 7BD6F034A4C3DC1E3DC2516F6962502AA8E243A3DA541FD73E886F287792E970 | SHA-256 |
| 9C129DA79A8FB3658FD590DFE50E99C541955CA4ED085D809C39F43D36A00575 | SHA-256 |
| 3D90F14C88DDACD592856E9E0D657D95E7BBC4BF41A0805CEA58FB725BB0D61D | SHA-256 |
| 13EF6FBD0FE8204DBE8831CAD802CCD300B8696A1815B830C7820E02E2E538EA | SHA-256 |
| E56A7E5D3AB9675555E2897FC3FAA2DD9265008A4967A7D54030AB8184D2D38F | SHA-256 |
| 18624CAE215E58079E8A9B236056A3A98EFEBF35CE799CB84CBAAF67B0972E0D | SHA-256 |
| 653C5BAB1504F9A6B9F3C865D50AE8993E307CDF6B2B58761CF7EE7AC5D62B7D | SHA-256 |
| 121118A0F5E0E8C933EFD28C9901E54E42792619A8A3A6D11E1F0025A7324BC2 | SHA-256 |
| DD20506B3C65472D58CCC0A018CB67C65FAB6718023FD4B16E148E64E69E5740 | SHA-256 |
| 3253BC9300DD0AA24997846B532C6966A3545DAE830EB6B7D54657AA3F739DB7 | SHA-256 |
| 05903B62D309D5B4C04C7C6865B1711CD9E4E6370D4DBF419B1611FF17C7A112 | SHA-256 |
| E407F2ABF8E890E536D1699AEFC58CE3B3094D26CA47DDBC72C1608F80F4F194 | SHA-256 |
| 6F1B1F3EF3598DF52054935D75EE1BF2E2BBB43643BC40693562859F17B5D405 | SHA-256 |
| 8E803B4F0640AACF8D6ADEAFA9AF182083711D09C6024B4DD91036933F1EF7A6 | SHA-256 |
| 6DB1BA2FA5CC9E8906E388FC2CF54283801771D36575D4F862320C16FA6577D7 | SHA-256 |
| 79A40AC47EA2B57727437A7A9365E860CC1FA1C7C96900F5A2A90133959C4694 | SHA-256 |
| 2AFE8912F1B7AFA3A4348EF4E027F7A46F4A2ADE824196265EA1AC952E172B3  | SHA-256 |
| 88bef4abd4db5e07764358ca39fe5bbf257603dbf3f0e4eeec2e8c127cfa7bfd | SHA-256 |
| 36b83f1df7c918efcde6ec5a895b4b53ec0307b1b8603a5ba3a3ab63ab7c2265 | SHA-256 |
| 36.91.45.10  | IP v4   |
| 123.231.149.122  | IP v4   |
| 85.204.116.188   | IP v4   |
| 27.110.228.186   | IP v4   |
| 180.250.197.188  | IP v4   |

|                           |        |
|---------------------------|--------|
| 66.181.167.72             | IP v4  |
| 181.113.20.186            | IP v4  |
| 103.94.122.254            | IP v4  |
| 181.115.168.69            | IP v4  |
| 186.42.186.202            | IP v4  |
| 52.37.89.225              | IP v4  |
| 95.171.16.42              | IP v4  |
| 107.181.175.122           | IP v4  |
| 186.159.1.217             | IP v4  |
| 31.214.138.207            | IP v4  |
| 181.113.17.230            | IP v4  |
| 47.7.211.242              | IP v4  |
| 170.238.117.187           | IP v4  |
| 103.102.220.50            | IP v4  |
| 45.234.248.66             | IP v4  |
| 23.95.97.59               | IP v4  |
| 51.254.25.115             | IP v4  |
| 193.183.98.66             | IP v4  |
| 91.217.137.37             | IP v4  |
| 87.98.175.85              | IP v4  |
| wearedevs.com             | Domain |
| caplinked.com             | Domain |
| majul.com                 | Domain |
| isns.net                  | Domain |
| fiberglassflyrodders.info | Domain |
| zolatee.com               | Domain |
| zullari.com               | Domain |
| youwantwork.com           | Domain |
| krupskaya.com             | Domain |
| m-onetrading-jp.com       | Domain |

|  |        |
|--|--------|
| thuocnam.tk  | Domain |
| msgsndr.com  | Domain |
| smtp.aiotecs.com   | Domain |
| measurements-api.wonderpush.com  | Domain |
| rockfeed.net   | Domain |
| www.sciencetechniz.com   | Domain |
| mediafire.fun  | Domain |
| afarmersway.com  | Domain |
| apexcpafirm.com  | Domain |
| tierwelt-live.de   | Domain |
| ipecho.net   | Domain |
| api.ipify.org  | Domain |
| checkip.amazonaws.com  | Domain |
| ip.anysrc.net  | Domain |
| wtfismyip.com  | Domain |
| ipinfo.io  | Domain |
| icanhazip.com  | Domain |
| myexternalip.com   | Domain |
| ident.me   | Domain |
| kostunivo.com  | Domain |
| chishir.com  | Domain |
| mangoclone.com   | Domain |
| onixcellent.com  | Domain |
| hxxps://ride.picky.co.ke/asset/app-assets/fonts/feather/fonts/156.dll  | URL    |
| hxxps://ride.picky.co.ke/asset/app-assets/fonts/feather/fonts/151.dll  | URL    |
| hxxps://ride.picky.co.ke/asset/app-assets/fonts/feather/fonts/147.dll  | URL    |
| hxxps://ride.picky.co.ke/asset/app-assets/fonts/feather/fonts/a156.dll | URL    |
| hxxps://spetsesyachtcharter.gr/share/148.dll                           | URL    |
| hxxps://spetsesyachtcharter.gr/share/mon92_cr.dll                      | URL    |
| hxxps://spetsesyachtcharter.gr/share/mon92.dll                         | URL    |

|   |     |
|---|-----|
| hxxps://newtrendeg.com/owncloud/apps/files_sharing/appinfo/Migrations/152.dll | URL |
| hxxps://newtrendeg.com/owncloud/apps/files_sharing/appinfo/Migrations/155.dll | URL |
| hxxps://mcrsal-rossais.com/font-awesome/css/155.dll                           | URL |
| hxxps://94.140.115.91.447/  | URL |
| hxxps://45.230.8.34.449/  | URL |
| hxxps://43.245.216.190.449/   | URL |
| hxxps://49.156.41.74.449/   | URL |
| hxxps://195.123.241.22.447/   | URL |
| hxxps://91.200.103.217.447/   | URL |
| hxxps://144.172.64.26.443/  | URL |
| hxxps://91.200.103.193.443/   | URL |
| hxxps://94.140.115.229.447/   | URL |
| hxxps://156.96.62.82.447/   | URL |
| hxxp://myexternalip.com/raw   | URL |
| hxxp://api.ipify.org  | URL |
| hxxp://icanhazip.com  | URL |
| hxxp://bot.whatismyipaddress.com  | URL |
| hxxp://ip.anysrc.net/plain/clientip   | URL |

## 5 REFERENCES

- <https://attack.mitre.org/software/S0266/>
- <https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/>
- <https://success.trendmicro.com/solution/1122411-trickbot-s-newly-released-modules-makes-it-even-trickier>
- <https://www.fortinet.com/blog/threat-research/deep-analysis-of-trickbot-new-module-pwgrab>

---

### Cysiv LLC

225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062

[www.cysiv.com](http://www.cysiv.com)

[sales@cysiv.com](mailto:sales@cysiv.com)