International Journal of Technology and Engineering Studies
volume 5 issue 3 pp. 95-105 doi: https://dx.doi.org/10.20469/ijtes.5.10004-3

Behavioral Analysis of Trickbot Banking Trojan with its New Tricks

Ruveyda Celik
Kayseri University, Kayseri, Turkey

Ali Gezer *
Kayseri University, Vocational College, Kayseri, Turkey

Abstract: This study aims to carry out a behavioral analysis of Trickbot and propose a machine learning technique for Trickbot detection. In the current study, an analysis is conducted to reveal Trickbot behavior while its code is injected into official banking websites. Trickbot is a banking trojan designed to steal users private information. Static and dynamic analyses using different tools were performed to identify TrickBot-associated streams and detect TrickBot infection. As a result of the analysis, it is found out that its authors use web injections to banking websites to steal and access login information. In addition, the analysis revealed that Trickbot targets many international banks in many countries via web injections. It is discovered that Trickbot uses different interfaces and files to replicate itself. The findings of this study could be used to deal with these attacks efficiently and prevent them in the future.

Keywords: *Trickbot, web injections, malware analyses, banking trojan*

Received: 2 April 2019; ***Accepted:*** 28 May 2019; ***Published:*** 21 June 2019

I. INTRODUCTION

Trickbot is a banking trojan that first appeared in late 2016. This malicious binary could be sent to users with an attahment into e-mail that they may think that it comes from their bank or a service which you had subscribed before. When the victim downloaded the attached file, it could infect the system and leak out credit card information and sensitive, data to the attackers [1, 2, 3, 4]. Then, all your credentials and credit card information might be stolen.

Trickbot is able to track the network traffic of various banks and seize users account names and passwords. In 2017, the Emotet trojan emerged and spread itself via e-mails [5]. In 2018 and 2019, Trickbot, which react again and attempt to infect their victims via fake mails. Trickbot will not only leak your data, It can also redirect ports on affected systems and set up virtual servers on devices on the same network [6, 7].

In this study, TrickBot's attack techniques after web injections had occured is analyzed. The data about Trickbot has been collected over the past few years. The current research also statically and dynamically analyzed the module files downloaded by Trickbot. To reveal the behavior of Trickbot trojan web-injections into banking websites, we run Trickbot samples on a virtual machine. The reason this study benefited from virtual machine is to prevent the virus from accessing our personal information, because we discovered that Trickbot's authors main motive is to steal credit card and banking information of users. As a result of our analysis, we learned that malware authors use web injections to steal and access login information.

In this analysis, it is found that Trickbot targets many international banks through web injections. In our article, we also discovered that Trickbot has updated itself and uses different ways to replicate itself.

This study analyzed the websites of three international banks targeted by Trickbot. The reason why we examine these banks that Trickbot targets is because Trickbot uses the three most important attack methods in these banks. We discovered that Trickbot may steal personal data and credit card information of people using Internet banking through web injections. In this article, the precautions to be taken to protect from the Trickbot attacks are also mentioned.

[*]Correspondence concerning this article should be addressed to Ali Gezer, Kayseri University, Vocational College, Kayseri, Turkey . E-mail: aligezer@uab.edu

II. RELATED WORKS

TrickBot is a well-known banking Trojan which is responsible for countless attacks in the world. TrickBot trojan has many similarities in structure to the Dyre trojan. It seems that there is a close link between these two trojans. Threat vectors in both viruses are constantly evolving, gaining new features as they defend themselves against new security measures implemented by PC security researchers. Dyre, also known as Dyreza, seems to have turned into a new banking Trojan with Trickbot.

Dyre Trojan horse is linked with extensive botnet families. In November 2015, Dyre attacked the computers of world-famous banks and took over financial institutions. The activities of this threat ended after its authors have been raided. It is believed that original developer of Dyre trojan contributed to the development of TrickBot. In 2017, Banking Trojan authors added a self-propagating component to their code, giving them the ability to spread malware. Obviously, the goal was to infect as many computers as possible and even the networks. In 2018, TrickBot reappeared with new talents. It is found that in May 2018, TrickBot collaborated with another banking Trojan, IcedID. One of the most important study about it was conducted by Ofir Ozer [8].

In January 2019, researchers discovered an active ransomware campaign targeted victim who were previously attacked by Emotet and TrickBot. There is evidence that cybercriminals first delivered Emotet through spam e-mails and various social engineering techniques. Then, an infected computer was used to distribute TrickBot, which stole sensitive information and helped attackers to find out if the victim was an appropriate industry target. Threat researcher Jason Reaves and his research teams [9] conducted similar studies. This research is based on a literature review showing the results of Trickbot analyzes.

One of the best resources for better understanding of Trickbot's behavioral analysis is the study of Gezer et al. [10]. In this study, behavioral analysis of Trickbot is explained, and a machine learning technique is proposed for Trickbot detection. A better understanding of Trickbot has been provided with static and dynamic analysis.

III. TRICKBOT BANKING TROJAN

TrickBot is one of the most dangerous crime codes and malware created by cybercrime gangs. Malware first appeared in August 2016. It is a modern and modular Trojan horse, which shows a striking resemblance to the behaviours Dyre trojan. With the codes embedded in the malware binary, the executable virus file could accomplish pulling extra usable modules from the command and control servers for a better control and access to the infected device. With modules that Trickbot has downloaded, it gains malicious functions that trick users for accessing their online banking credentials and personal data, and tricking people for disclosing their personal information via email to the adversaries. Over the years, TrickBot has continued to evolve. Trickbot developers are seeking to improve their research and development by making it difficult to investigate their privacy, bypassing basic security checks on user devices, and closing virus programs.

Although Trickbot has seen a large number of updates over the years, it has managed to overcome any virus programs and remediation solutions that try to prevent itself. Trickbot researchers have shown that TrickBot is replicated using spam emails and can be also distributed using fake Adobe Flash Player updates.

It seems that there is close link with the infrastructure of Dyre which is responsible for countless attacks in the world. The threats of these viruses are constantly evolving and gaining new features even when defending against new security measures implemented by PC security researchers.

TrickBot first appeared in October 2016, and first attacked to Australian banks. As of April 2017, there have been reports of attacks on leading and well-known banks in the UK, USA, Switzerland, Germany, Canada, New Zealand, France and Ireland. Other known names of this Trojan horse are TheTrick, Trickster, TrickLoader. One of the new versions of malware has been updated in the late 2017 to target cryptowallets that became popular after cryptoMY. The authors of Trickbot have added a component for the Trojan that makes the malware self-replicating. Obviously, Trickbot's goal was to infect as many computers as possible, and even to infiltrate all networks. In 2018, TrickBot reappeared with a wider range of capabilities and features.

From the beginning of 2019, the latest versions of TrickBot are available through seasonally themed spam emails as if they are coming from a major financial advisory or banking company. E-mails stand out as tax-related content, with users from major countries such as the United States, Germany, the UK, Spain and promising some tax assistance for people using online banking applications. However, once opened, it looks like a Microsoft Excel file attached to a email on the user's computer. After execution of th downloaded binary, the virus activates advanced proliferation modules [10, 11].

A. *How Does Trickbot Attack?*

After the virus infects itself into a machine, it creates many different attack vectors.

1) *Attack Vectors*

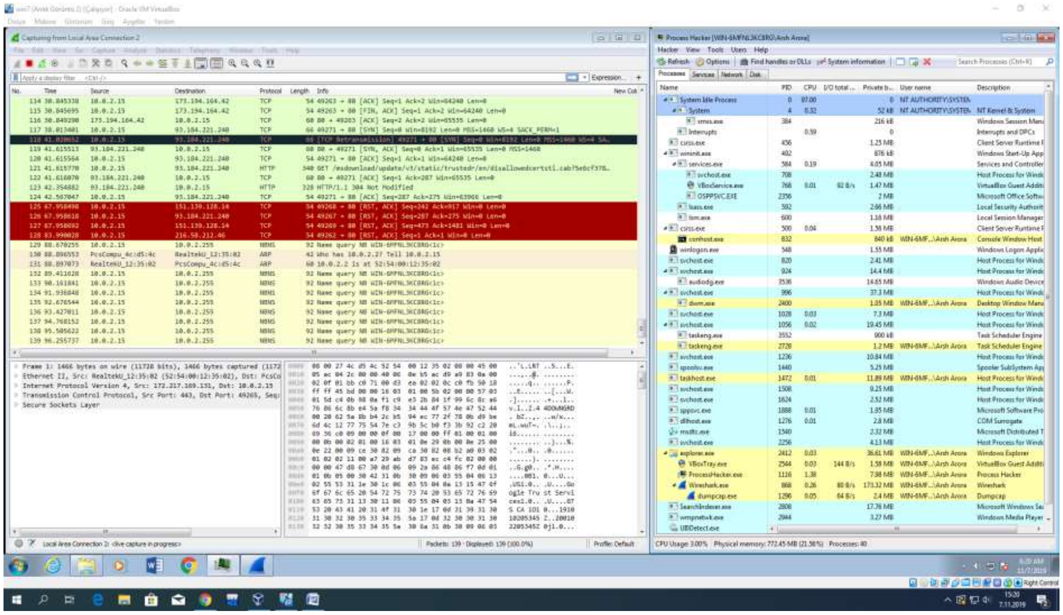
- SpearPhishing: Malware is usually distributed through infected phishing through additional infected files or malicious site URLs. The real hunting method is carried out through malicious e-mails, which are specifically targeted banks, firms or managers of different companies.
- Network Vulnerabilities: TrickBot spreads like a virus across all organization's networks using the Server Message Block (SMB) Protocol, which allows computers with Windows operating system to propagate information to other systems on the same network.
- Secondary payload: Trickbot is distributed by another powerful Trojan Malware, Emotet.

2) Attack Ways: After Trickbot's first appearance 3 years ago, TrickBot has gained many advanced capabilities. Trickbot installs itself with attack modules to replicate and download other malicious binaries.

- Persistence Module: TrickBot cannot be detected by the end user and gains the ability to hide itself by carefully creating a scheduled task.
- Explicit Routing and Server Side Injection: TrickBot exploits vulnerabilities, such as explicit redirects and server-side injections, to steal user's information when login information is entered from the user's banking website session. Using this, TrickBot can collect financial and personal bank information, and defraud its victims.
- Cookie Playback: Trickbot's cookie playback module gathers data from careless users such as login status, website preferences, personalized content, etc.
- Remote Application Playback: Trickbot adds a module to collect remote desktop application credentials which allows it to affect a range of applications.
- Viral Deployment: The new version of the TrickBot module uses infected computers to send spam e-mails that look like emails from trusted accounts. TrickBot has a database with more than 300 million email accounts [12].

B. *Dynamic Analysis of Trickbot*

We carried out dynamic analyses after infecting our systems with Trickbot binary. We analyzed Trickbot's behavior with dynamic analysis. We observed Trickbot's behavior via using different tools. We used Wireshark and Process Hacker as seen in Fig. 1 and Fig. 2. Fig. 1 is a screenshot of Wireshark and Process Hacker programs in a clean machine without any infection. Wireshark and Process Hacker image from an infected machine is given in Fig. 2. When the two images are carefully examined, Fig. 2 (infected virtual machine) also shows that the virus has created itself in a different name and image.


Capturing from Local Area Connection 2
Apply a display filter ... <Ctrl-/>
Expression...
Process Hacker [WIN-6MFNL3KC8RG\Arsh Arora]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

```
No.  Time       Source             Destination        Protocol Length Info
114 38.845338  10.0.2.15          173.194.164.42     TCP      54 49263 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0
115 38.845695  10.0.2.15          173.194.164.42     TCP      54 49263 → 80 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
116 38.849298  173.194.164.42     10.0.2.15          TCP      60 80 → 49263 [ACK] Seq=2 Ack=2 Win=65535 Len=0
117 38.013401  10.0.2.15          93.184.221.240     TCP      66 49271 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
118 41.020052  10.0.2.15          93.184.221.240     TCP      66 [TCP Retransmission] 49271 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA…
119 41.615513  93.184.221.240     10.0.2.15          TCP      60 80 → 49271 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
120 41.615564  10.0.2.15          93.184.221.240     TCP      54 49271 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
121 41.615770  10.0.2.15          93.184.221.240     HTTP     340 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5e6cf378…
122 41.616070  93.184.221.240     10.0.2.15          TCP      60 80 → 49271 [ACK] Seq=1 Ack=287 Win=65535 Len=0
123 42.354882  93.184.221.240     10.0.2.15          HTTP     328 HTTP/1.1 304 Not Modified
124 42.567047  10.0.2.15          93.184.221.240     TCP      54 49271 → 80 [ACK] Seq=287 Ack=275 Win=63966 Len=0
125 67.958000  10.0.2.15          151.139.128.14     TCP      54 49268 → 80 [RST, ACK] Seq=242 Ack=917 Win=0 Len=0
126 67.958618  10.0.2.15          93.184.221.240     TCP      54 49267 → 80 [RST, ACK] Seq=287 Ack=275 Win=0 Len=0
127 67.958692  10.0.2.15          151.139.128.14     TCP      54 49269 → 80 [RST, ACK] Seq=473 Ack=1481 Win=0 Len=0
128 83.990028  10.0.2.15          216.58.212.46      TCP      54 49262 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129 88.670255  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
130 88.896553  PcsCompu_4c:d5:4c  RealtekU_12:35:02  ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
131 88.897073  RealtekU_12:35:02  PcsCompu_4c:d5:4c  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
132 89.411628  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
133 90.161841  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
134 91.936848  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
135 92.676544  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
136 93.427011  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
137 94.768152  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
138 95.505622  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
139 96.255737  10.0.2.15          10.0.2.255         NBNS     92 Name query NB WIN-6MFNL3KC8RG<1c>
```

```
Frame 1: 1466 bytes on wire (11728 bits), 1466 bytes captured (1172
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCo
Internet Protocol Version 4, Src: 172.217.169.131, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 443, Dst Port: 49265, Seq:
Secure Sockets Layer
```

```
0000  08 00 27 4c d5 4c 52 54  00 12 35 02 08 00 45 00   ..'L.LRT ..5...E.
0010  05 ac 04 2c 00 00 40 06  0e b5 ac d9 a9 83 0a 00   ...,..@. ........
0020  02 0f 01 bb c0 71 00 d3  e6 02 02 0c c0 fb 50 18   .....q.. ......P.
0030  ff ff 45 bd 00 00 16 03  01 00 5b 02 00 00 57 03   ..E..... ..[...W.
0040  01 5d c4 0b 08 0a f1 c9  e5 2b 04 1f 99 6c 8c a6   .]...... .+...l..
0050  76 06 6c 8b e4 5a f8 34  34 44 4f 57 4e 47 52 44   v.l..Z.4 4DOWNGRD
0060  00 20 62 5a 8b b4 2c b5  94 ec 77 2f 78 0b d9 be   . bZ..,. ..w/x...
0070  6d 4c 12 77 75 54 7e c3  9b 5c b0 f3 3b 92 c2 20   mL.wuT~. .\..;..
0080  69 36 c0 09 00 00 0f 00  17 00 00 ff 01 00 01 00   i6...... ........
0090  00 0b 00 02 01 00 16 03  01 0e 29 0b 00 0e 25 00   ........ ..)...%.
00a0  0e 22 00 09 ce 30 82 09  ca 30 82 08 b2 a0 03 02   ."...0.. .0......
00b0  01 02 02 11 00 a7 29 ab  d7 03 ec c4 fc 02 00 00   ......). ........
00c0  00 00 47 d8 67 30 0d 06  09 2a 86 48 86 f7 0d 01   ..G.g0.. .*.H....
00d0  01 0b 05 00 30 42 31 0b  30 09 06 03 55 04 06 13   ....0B1. 0...U...
00e0  02 55 53 31 1e 30 1c 06  03 55 04 0a 13 15 47 6f   .US1.0.. .U....Go
00f0  6f 67 6c 65 20 54 72 75  73 74 20 53 65 72 76 69   ogle Tru st Servi
0100  63 65 73 31 13 30 11 06  03 55 04 03 13 0a 47 54   ces1.0.. .U....GT
0110  53 20 43 41 20 31 4f 31  30 1e 17 0d 31 39 31 30   S CA 1O1 0...1910
0120  31 30 32 30 35 33 34 35  5a 17 0d 32 30 30 31 30   10205345 Z..20010
0130  32 32 30 35 33 34 35 5a  30 6a 31 0b 30 09 06 03   2205345Z 0j1.0...
```

Packets: 139 · Displayed: 139 (100.0%) | Profile: Default

```
Name                  PID   CPU    I/O total ...  Private b...  User name                 Description
System Idle Process   0     97.00                 0             NT AUTHORITY\SYSTEM
  System              4     0.32                  52 kB         NT AUTHORITY\SYSTEM       NT Kernel & System
    smss.exe          384                         216 kB                                  Windows Session Mana
  Interrupts                0.59                  0                                       Interrupts and DPCs
csrss.exe             456                         1.23 MB                                 Client Server Runtime P
wininit.exe           492                         876 kB                                  Windows Start-Up App
  services.exe        584   0.19                  4.05 MB                                 Services and Controller
    svchost.exe       708                         2.48 MB                                 Host Process for Windo
    VBoxService.exe   768   0.01   82 B/s         1.47 MB                                 VirtualBox Guest Additi
    OSPPSVC.EXE       2356                        2 MB                                    Microsoft Office Softwa
  lsass.exe           592                         2.66 MB                                 Local Security Authorit
  lsm.exe             600                         1.18 MB                                 Local Session Manager
csrss.exe             500   0.04                  1.38 MB                                 Client Server Runtime P
  conhost.exe         832                         840 kB        WIN-6MF...\Arsh Arora     Console Window Host
winlogon.exe          548                         1.55 MB                                 Windows Logon Applic
svchost.exe           820                         2.41 MB                                 Host Process for Windo
svchost.exe           924                         14.4 MB                                 Host Process for Windo
  audiodg.exe         3536                        14.65 MB                                Windows Audio Device
svchost.exe           996                         37.3 MB                                 Host Process for Windo
  dwm.exe             2400                        1.05 MB       WIN-6MF...\Arsh Arora     Desktop Window Mana
svchost.exe           1028  0.03                  7.3 MB                                  Host Process for Windo
svchost.exe           1056  0.02                  19.45 MB                                Host Process for Windo
  taskeng.exe         3552                        900 kB                                  Task Scheduler Engine
  taskeng.exe         2728                        1.2 MB        WIN-6MF...\Arsh Arora     Task Scheduler Engine
svchost.exe           1236                        10.84 MB                                Host Process for Windo
spoolsv.exe           1440                        5.25 MB                                 Spooler SubSystem App
taskhost.exe          1472  0.01                  11.89 MB      WIN-6MF...\Arsh Arora     Host Process for Windo
svchost.exe           1508                        9.25 MB                                 Host Process for Windo
svchost.exe           1624                        2.52 MB                                 Host Process for Windo
sppsvc.exe            1888  0.01                  1.95 MB                                 Microsoft Software Pro
dllhost.exe           1276  0.01                  2.8 MB                                  COM Surrogate
msdtc.exe             1540                        2.32 MB                                 Microsoft Distributed T
svchost.exe           2256                        4.13 MB                                 Host Process for Windo
explorer.exe          2412  0.03                  36.61 MB      WIN-6MF...\Arsh Arora     Windows Explorer
  VBoxTray.exe        2544  0.03   144 B/s        1.58 MB       WIN-6MF...\Arsh Arora     VirtualBox Guest Additi
  ProcessHacker.exe   1116  1.38                  7.38 MB       WIN-6MF...\Arsh Arora     Process Hacker
  Wireshark.exe       868   0.26   80 B/s         173.32 MB     WIN-6MF...\Arsh Arora     Wireshark
    dumpcap.exe       1296  0.05   64 B/s         2.4 MB        WIN-6MF...\Arsh Arora     Dumpcap
SearchIndexer.exe     2808                        17.36 MB                                Microsoft Windows Sea
wmpnetwk.exe          2944                        3.27 MB                                 Windows Media Player
UBDetect.exe
```

CPU Usage: 3.00% Physical memory: 772.45 MB (21.58%) Processes: 40

Fig. 1. Wireshark and process hacker image from a clean machine

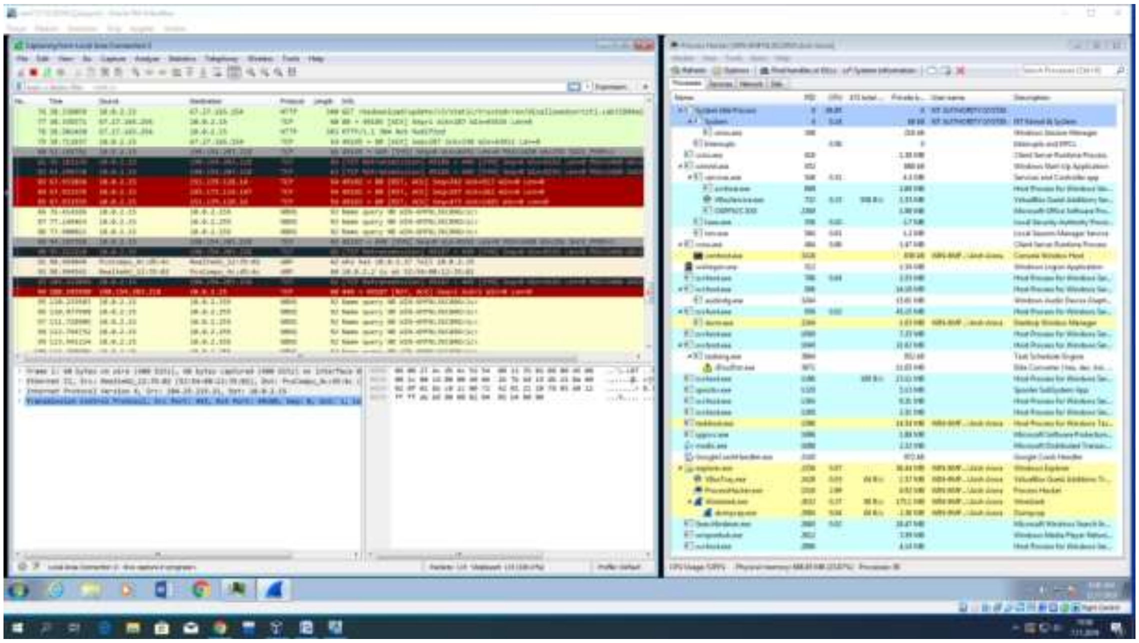
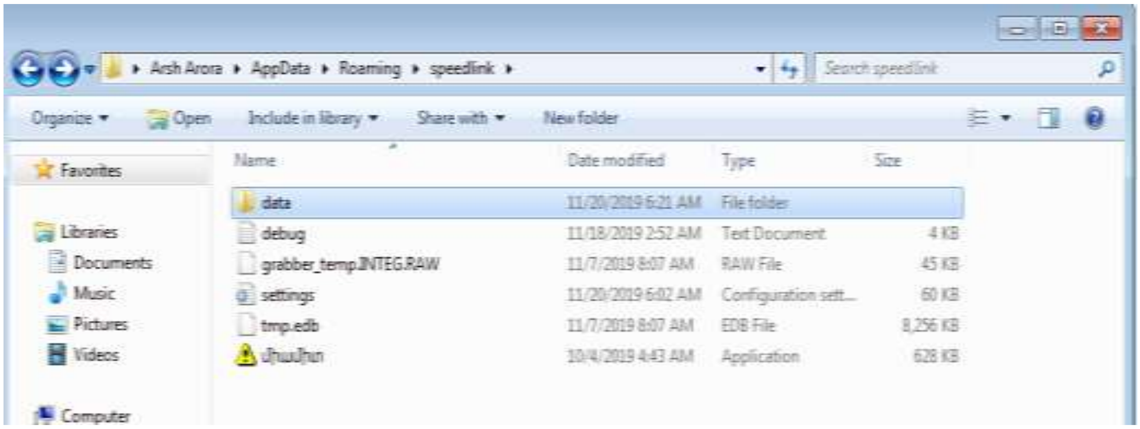


Fig. 2. Wireshark and process hacker image from an infected machine

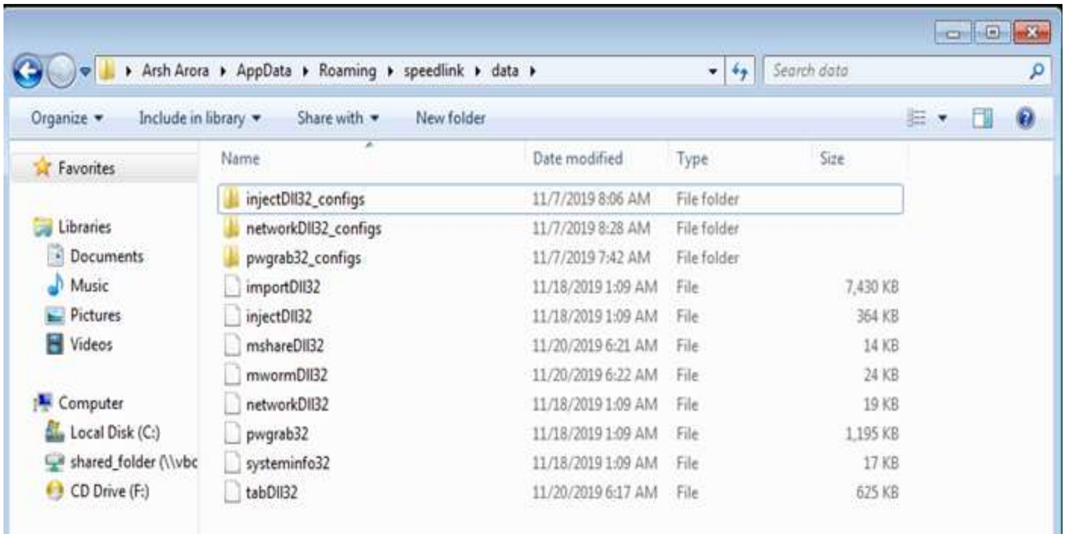
After Trickbot infection, it is checked that any file is downloaded into the machine. When we execute the Trickbot binary on our virtual machine, it creates a folder named speedlink into APPDATA/Roaming to replicate itself and download more files which works for Trickbot. We can see the files created by Trickbot in Fig. 3. In Fig. 4, we could see the download files for different purposes.

We can explain the files that Trickbot has dowloaded as follows.



Name	Date modified	Type	Size
data	11/20/2019 6:21 AM	File folder	
debug	11/18/2019 2:52 AM	Text Document	4 KB
grabber_temp.INTEG.RAW	11/7/2019 8:07 AM	RAW File	45 KB
settings	11/20/2019 6:02 AM	Configuration sett...	60 KB
tmp.edb	11/7/2019 8:07 AM	EDB File	8,256 KB
dJhuuJhn	10/4/2019 4:43 AM	Application	628 KB

Fig. 3. Image of the data file created by TrickBot



Name	Date modified	Type	Size
injectDll32_configs	11/7/2019 8:06 AM	File folder	
networkDll32_configs	11/7/2019 8:28 AM	File folder	
pwgrab32_configs	11/7/2019 7:42 AM	File folder	
importDll32	11/18/2019 1:09 AM	File	7,430 KB
injectDll32	11/18/2019 1:09 AM	File	364 KB
mshareDll32	11/20/2019 6:21 AM	File	14 KB
mwormDll32	11/20/2019 6:22 AM	File	24 KB
networkDll32	11/18/2019 1:09 AM	File	19 KB
pwgrab32	11/18/2019 1:09 AM	File	1,195 KB
systeminfo32	11/18/2019 1:09 AM	File	17 KB
tabDll32	11/20/2019 6:17 AM	File	625 KB

Fig. 4. Downloaded module binaries after infection

1) The purposes of downloaded modules: The purposes of downloaded modules are as follows.

- injectDll32 module: This encrypted module monitors websites that banking applications can use. It is also used to inject an encrypted code using the technique called Reflective DLL Injection (a library injection technique that uses the concept of reflective programming to perform the loading of a library from memory into a host process). InjectDll32 requires monitoring banking websites for two different credential stealing methods: When a user logs into websites that include banks in countries such as Canada, Spain, Germany, and Japan, Trickbot takes immediate action to obtain the user's login credentials. Second, Trickbot monitors whether a user has access to certain websites related to different international banks and directs users to fake phishing websites. Banking URLs targeted by Trickbot are mostly from the United States, Canada, England, Germany, Australia, Austria, Ireland, London, Switzerland and Scotland.
- networkdll32: Trickbot uses this encrypted module to scan the network and steal relevant network information (personal credentials). It uses different commands to gather information about the infected virtual machine.
- pwgrab32 module: Trickbot's new module, pwgrab32 or PasswordGrabber, steals credentials from popular applications such as Filezilla, Microsoft Outlook, and WinSCP. In addition to stealing personal information, personal data from applications, it also steals the following information from popular search engines (Google Chrome, Mozilla Firefox, Internet Explorer, and Microsoft Edge) such as user names and passwords, cookies, search history, autofills, HTTP posts.
- importDll32 module: This module is responsible for stealing browser data such as browsing history, cookies, and plugins.
- systeminfo32 module: fter successfully installed in a virtual machine, Trickbot collects system information such as operating system, CPU and memory information, user accounts, lists of installed programs and services.
- mailsearcher32 module: This module searches the infected system's files to collect all e-mail addresses stored in the virtual machine to steal information. Collecting e-mail addresses for the needs of spam campaigns is the most obvious behavior of malware.
- shareDll32 module: Trickbot uses the shareDll32 module to spread itself secretly across the network. To make the malware more permanent, there is an auto-start service that keeps Trickbot running every time when the machine is turned on. This service may have the following display names such as Service Technology, Service-Techno2, Techniques-Service2, Technoservices Advanced-Technic-Service, ServiceTechno5.
- networkdll32: Using this encrypted module, Trickbot uses the network to scan through and steal relevant network information to find out useful information. It aim is to collect information about the infected system [13, 14].

2) Revealing TrickBot web injections: After infection, Trickbot created itself in a different directory, and added as a task under Windows taskeng.exe. It runs all downloaded DLL files into Svchost processes (Svchost.exe is a system application that enables execution of processes initiated from DLL files). This application is important for maintaining the stable and secure structure of the operating system and should not be terminated. DLL files that are not executable because they need a launcher, which is the svchost.exe. Fig. 5 shows Http filtering from injectDll32 related svchost process.

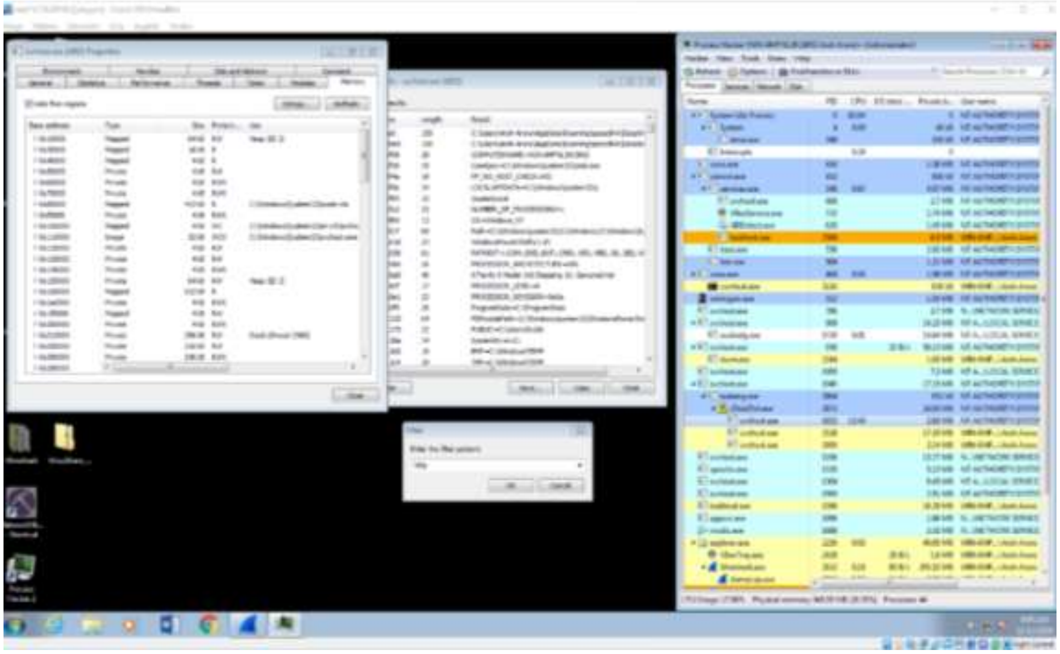
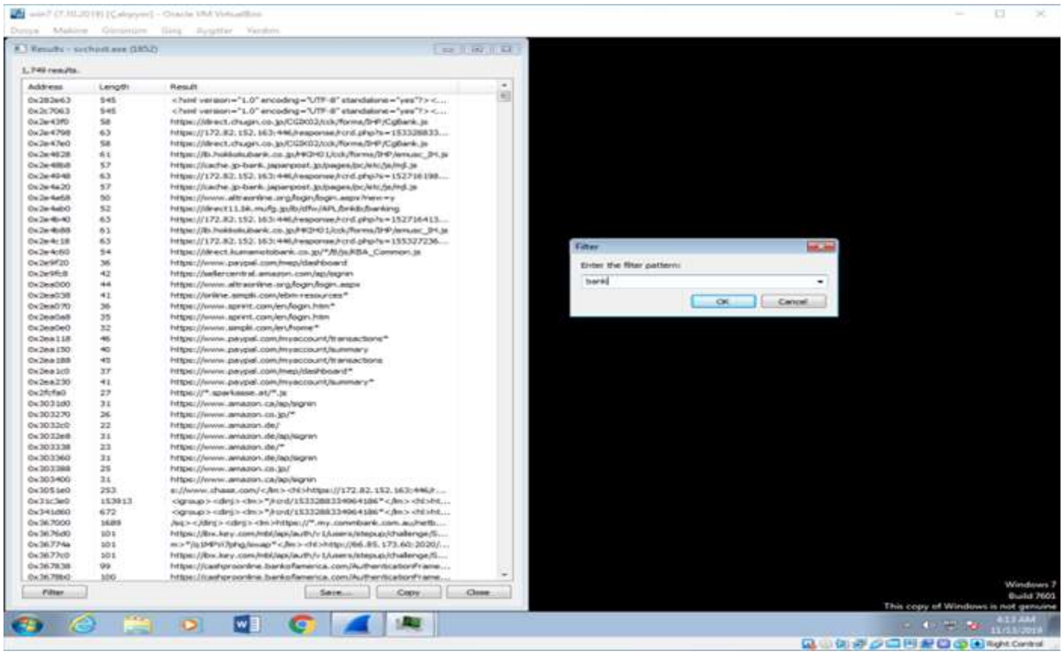


Fig. 5. Http filtering from injectDll32 related svchost process

After selecting the strings tab in the memory, a filtering process is carried out. We first look at the http strings in the memory to find out targeted banks. As a result of string filtering, we have seen 1749 bank related strings [5]. Fig. 6 shows bank related strings in svchost process.


win7 (7.10.2019) [Çalışıyor] - Oracle VM VirtualBox
Dosya
Makine
Görünüm
Giriş
Aygıtlar
Yardım
Results - svchost.exe (1852)
Filter
Save...
Copy
Close
Windows 7
Build 7601
This copy of Windows is not genuine
4:13 AM
11/11/2019
Right Control

1,749 results.

Address	Length	Result
0x282e63	545	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><...
0x2c7063	545	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><...
0x2e43f0	58	https://direct.chugin.co.jp/CGDC02/cck/forms/SHP/Cgbank.js
0x2e4798	63	https://172.82.152.163:446/response/rcrd.php?s=153328833...
0x2e47e0	58	https://direct.chugin.co.jp/CGDC02/cck/forms/SHP/Cgbank.js
0x2e4828	61	https://ib.hokkokubank.co.jp/HKDH01/cck/forms/SHP/emusc_JH.js
0x2e48b8	57	https://cache.jp-bank.japanpost.jp/pages/pc/etc/js/mdj.js
0x2e4948	63	https://172.82.152.163:446/response/rcrd.php?s=152716198...
0x2e4a20	57	https://cache.jp-bank.japanpost.jp/pages/pc/etc/js/mdj.js
0x2e4a68	50	https://www.altraonline.org/login/login.aspx?new=y
0x2e4ab0	52	https://direct11.bk.mufg.jp/ib/dfw/APL/bnkib/banking
0x2e4b40	63	https://172.82.152.163:446/response/rcrd.php?s=152716413...
0x2e4b88	61	https://ib.hokkokubank.co.jp/HKDH01/cck/forms/SHP/emusc_JH.js
0x2e4c18	63	https://172.82.152.163:446/response/rcrd.php?s=155327236...
0x2e4c60	54	https://direct.kumamotobank.co.jp/*/B/js/KBA_Common.js
0x2e9f20	36	https://www.paypal.com/mep/dashboard
0x2e9fc8	42	https://sellercentral.amazon.com/ap/signin
0x2ea000	44	https://www.altraonline.org/login/login.aspx
0x2ea038	41	https://online.simplii.com/ebm-resources*
0x2ea070	36	https://www.sprint.com/en/login.htm*
0x2ea0a8	35	https://www.sprint.com/en/login.htm
0x2ea0e0	32	https://www.simplii.com/en/home*
0x2ea118	46	https://www.paypal.com/myaccount/transactions*
0x2ea150	40	https://www.paypal.com/myaccount/summary
0x2ea188	45	https://www.paypal.com/myaccount/transactions
0x2ea1c0	37	https://www.paypal.com/mep/dashboard*
0x2ea230	41	https://www.paypal.com/myaccount/summary*
0x2fcfa0	27	https://*.sparkasse.at/*.js
0x3031d0	31	https://www.amazon.ca/ap/signin
0x303270	26	https://www.amazon.co.jp/*
0x3032c0	22	https://www.amazon.de/
0x3032e8	31	https://www.amazon.de/ap/signin
0x303338	23	https://www.amazon.de/*
0x303360	31	https://www.amazon.de/ap/signin
0x303388	25	https://www.amazon.co.jp/
0x303400	31	https://www.amazon.ca/ap/signin
0x3051e0	253	s://www.chase.com/</tm><ht>https://172.82.152.163:446/r...
0x31c3e0	153913	<igroup><dinj><tm>*/rcrd/1533288334964186*</tm><ht>ht...
0x341d60	672	<igroup><dinj><tm>*/rcrd/1533288334964186*</tm><ht>ht...
0x367000	1689	/sq></dinj><dinj><tm>https://*.my.commbank.com.au/netb...
0x3676d0	101	https://ibx.key.com/mbl/api/auth/v1/users/stepup/challenge/S...
0x36774a	101	m>*/ip1MPVI?phg/iwap*</tm><ht>http://66.85.173.60:2020/...
0x3677c0	101	https://ibx.key.com/mbl/api/auth/v1/users/stepup/challenge/S...
0x367838	99	https://cashproonline.bankofamerica.com/AuthenticationFrame...
0x3678b0	100	https://cashproonline.bankofamerica.com/AuthenticationFrame...

Filter

Enter the filter pattern:

bank

OK

Cancel

Fig. 6. Filtering bank related strings in the svchost process

In Fig. 7, we see the svchost.exe memory string results of other banks targeted by Trickbot. Via choosing 3 of the banks that Trickbot targets, we will discover the web injections on the websites of these banks.

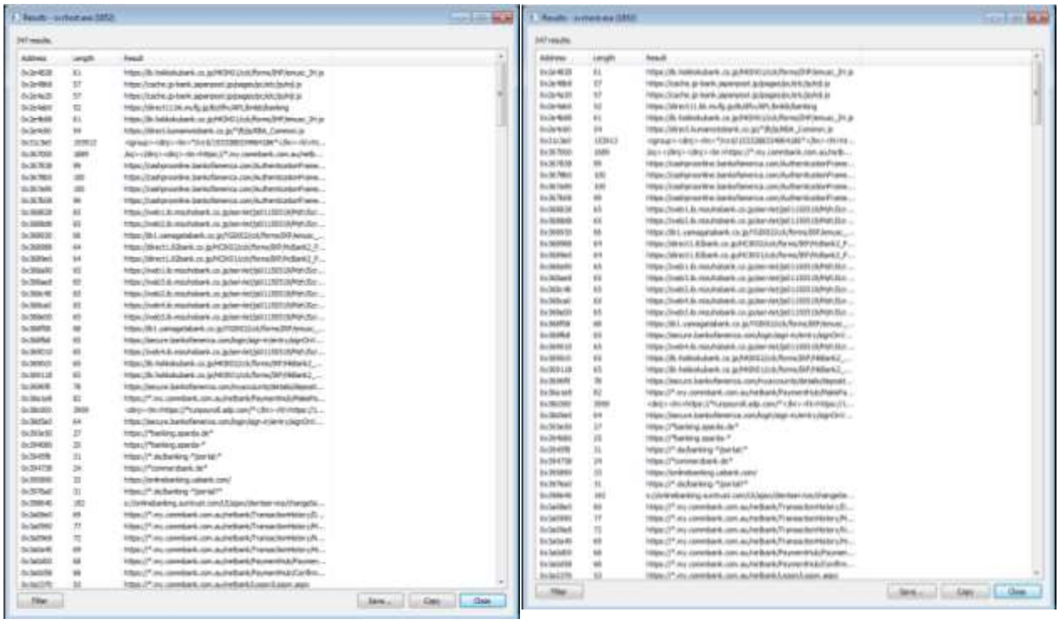


Fig. 7. Results of bank websites in Svchost memory strings

We have looked at 3 popular online banking websites that Trickbot trojan injected its malicious binaries into their official websites. For those 3 banks, we take some snaphots from clean and infected machines. When we carefully examined the HTML source code of the official bank websites, we found out that the clean and virtual machine's html codes are not the same. We encountered some web injections due to Trickbot infection. After logging into the banking account with false user information, we right-click on the online banking website to view the page source.

Then, we examined whether these codes are the same or not. When the URL address are entered from a clean machine and infected machine, both websites look like each other. It is not possible to understand which website belong to infected machine. If we enter our personal information into Trickbot infected machine, perhaps all of our credit card or banking information may have been stolen. Fig. 8 shows the html source codes of displayed web pages. It could be seen that, some web injections occured into Trickbot infected machine. If we carefully examine the screenshots in Fig. 8, after line 754, script codes differ from each other. It appears that these injected codes contain some cookie information.

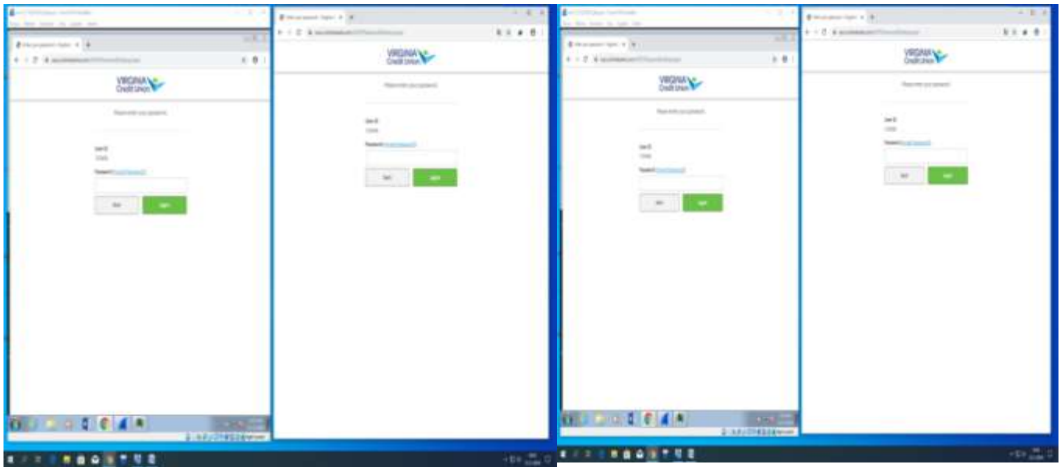


Fig. 8. Html source code comparison of an international bank official website with Trickbot infected and a clean machine

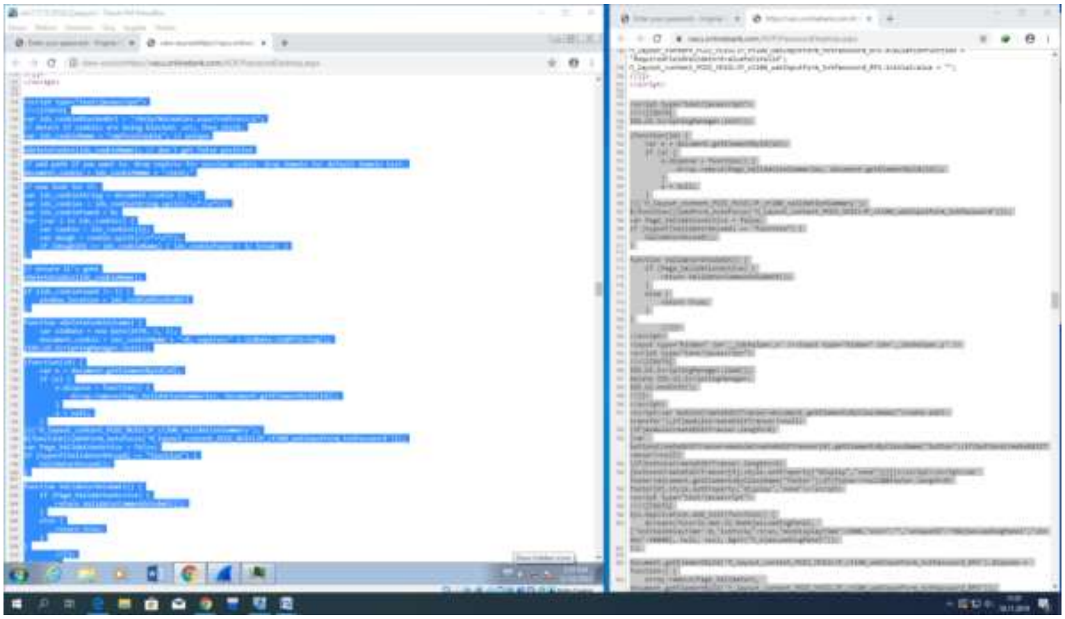


Fig. 9. Screenshot of official website of an international bank from clean and infected machine

When we look at another international bank website after Trickbot infection, at first there is no difference as could be seen in Fig. 10. But when the page source code is displayed (in Fig. 11), we have discovered some web injections had occured. When we carefully examine source code, we have seen that Trickbot uses addEventListener and prevDefault javascript commands. These commands allow Trickbot to perform its malicious functions for replication and information stealing.

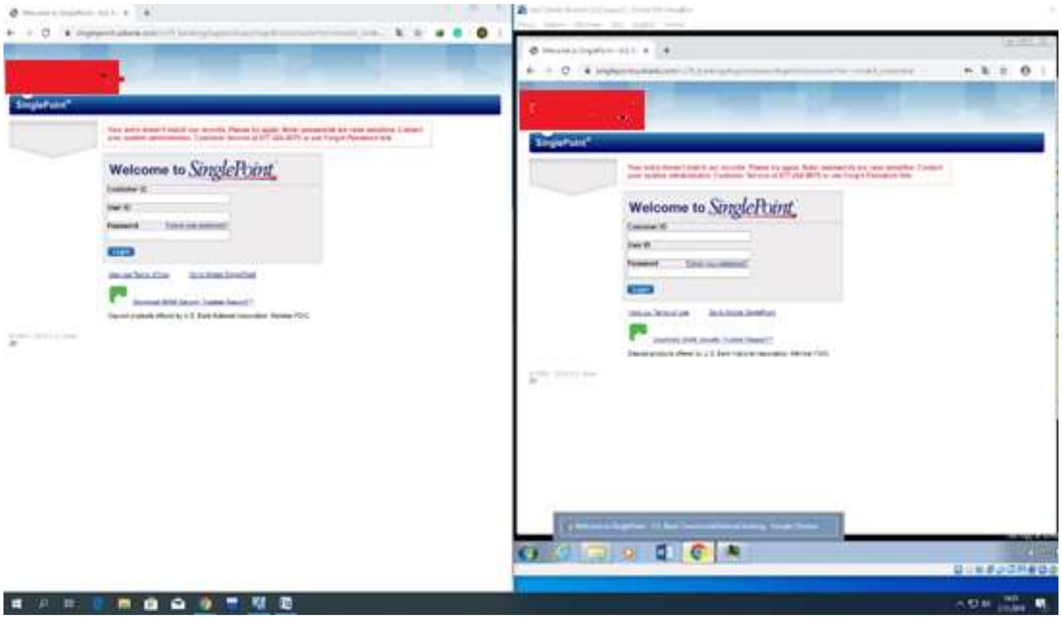
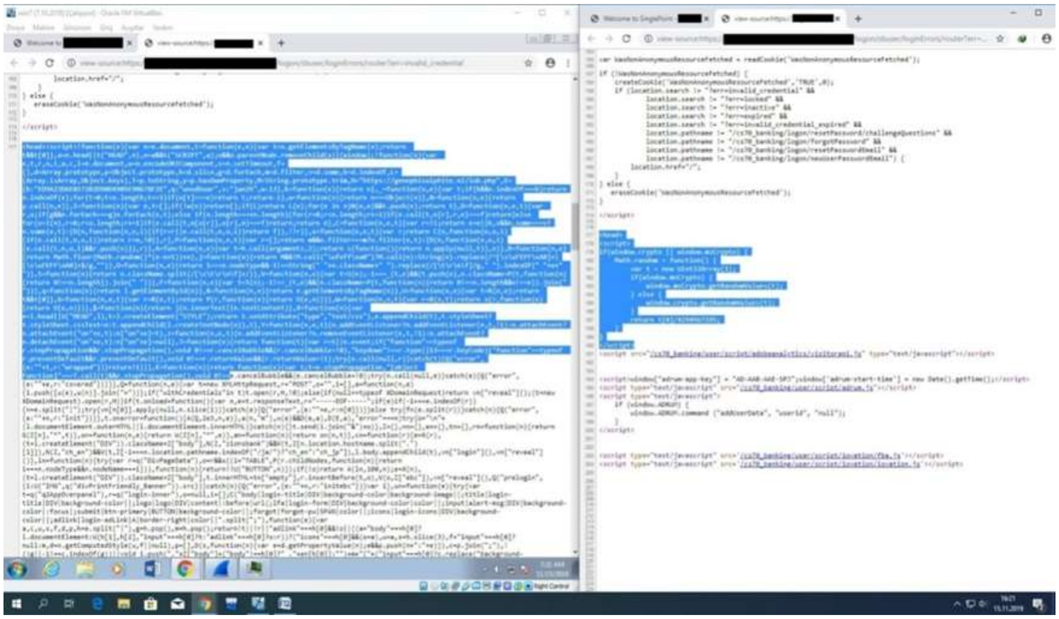


Fig. 10. Image of an online login website on a clean and infected machine of another international bank



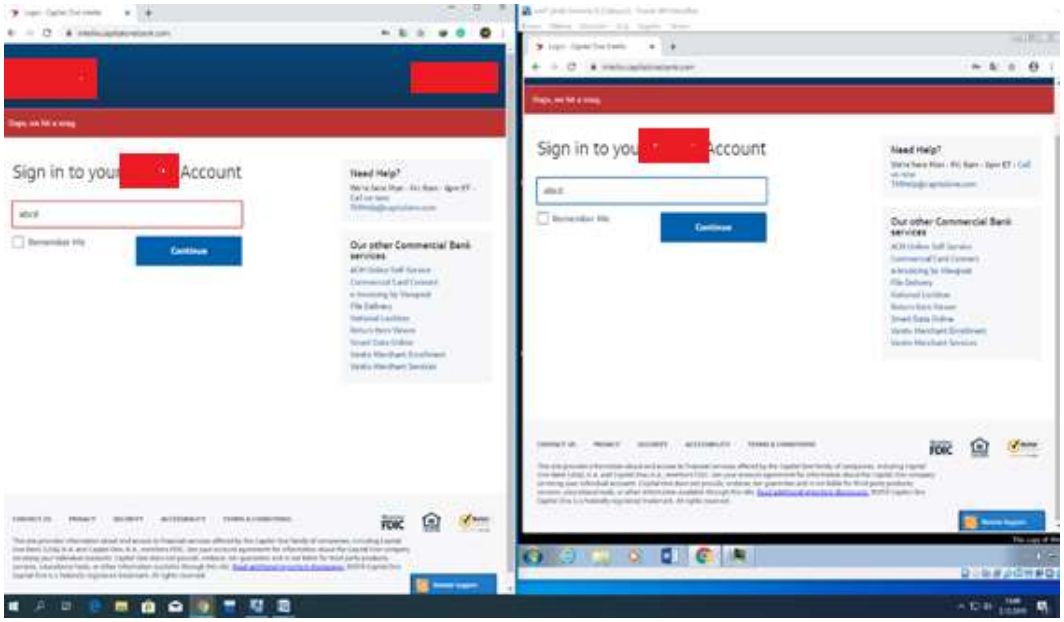
Welcome to [redacted]
view-source:https:/[redacted]
view-source:https://[redacted]/logon/sbuser/loginErrors/router?err=invalid_credential
Welcome to SinglePoint - [redacted]
view-source:https:/[redacted]

```
        location.href="/";
    }
} else {
    eraseCookie('wasNonAnonymousResourceFetched');
}

</script>
```

```
var wasNonAnonymousResourceFetched = readCookie('wasNonAnonymousResourceFetched');

if (!wasNonAnonymousResourceFetched) {
    createCookie('wasNonAnonymousResourceFetched','TRUE',0);
    if (location.search != "?err=invalid_credential" &&
            location.search != "?err=locked" &&
            location.search != "?err=inactive" &&
            location.search != "?err=expired" &&
            location.search != "?err=invalid_credential_expired" &&
            location.pathname != "/cs70_banking/logon/resetPassword/challengeQuestions" &&
            location.pathname != "/cs70_banking/logon/forgotPassword" &&
            location.pathname != "/cs70_banking/logon/resetPasswordEmail" &&
            location.pathname != "/cs70_banking/logon/newUserPasswordEmail") {
        location.href="/";
    }
} else {
   eraseCookie('wasNonAnonymousResourceFetched');
}

</script>

<head>
<script>
if(window.crypto || window.msCrypto) {
    Math.random = function() {
        var t = new Uint32Array(1);
        if(window.msCrypto) {
            window.msCrypto.getRandomValues(t);
        } else {
            window.crypto.getRandomValues(t);
        }
        return t[0]/4294967295;
    }
}
</script>
<script src="/cs70_banking/user/script/adobeanalytics/visitorapi.js" type="text/javascript"></script>

<script>window["adrum-app-key"] = "AD-AAB-AAE-SPJ";window['adrum-start-time'] = new Date().getTime();</script>
<script type="text/javascript" src="/cs70_banking/user/script/adrum.js"></script>
<script type="text/javascript">
    if (window.ADRUM) {
        window.ADRUM.command ("addUserData", "userId", "null");
    }
</script>


<script type="text/javascript" src='/cs70_banking/user/script/location/fba.js'></script>
<script type="text/javascript" src='/cs70_banking/user/script/location/location.js'></script>
```

Fig. 11. Image of the source codes the Bank webpage from infected and clean machine

When we look at the 2nd international bank in Fig. 10, there is no difference when we enter the clean and virtual machine. But when the page source is displayed (in Fig. 11), we have discovered cryptic codes with a different id in javascript codes. Fig. 12 shows one of the 3rd international US banks. Again, as in the website of other banks, there is no difference on the page. however, in the page view in Fig. 13, we have seen that Trickbot uses addEventListener and prevDefault() javascript commands. These commands allow the Trickbot to perform its own functions such as replication and information stealing [15, 16].



[redacted] [redacted]

Oops, we hit a snag.

Sign in to your [redacted] Account

abcd

□ Remember Me

Continue

Need Help?

Our other Commercial Bank services

FDIC

Oops, we hit a snag.

Sign in to you[redacted]Account

abcd

□ Remember Me

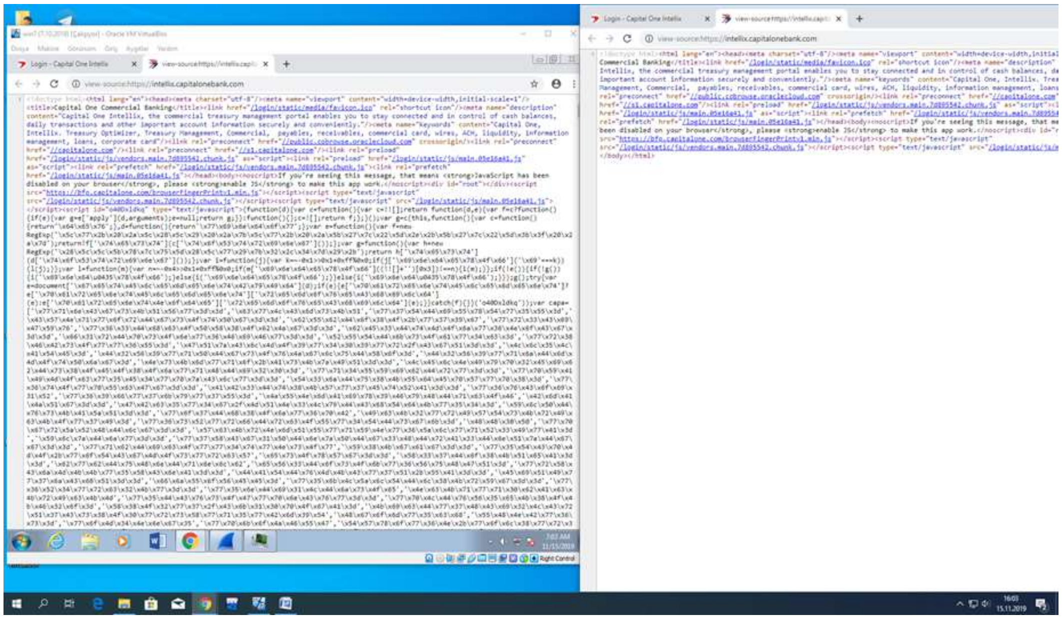
Continue

Need Help?

Our other Commercial Bank services

FDIC

Fig. 12. Image of an online login website on a clean and infected machine of an international bank



```
view-source:https://intellix.capitalonebank.com
<!doctype html><html lang="en"><head><meta charset="utf-8"/><meta name="viewport" content="width=device-width,initial-scale=1"/>
<title>Capital One Commercial Banking</title><link href="/login/static/media/favicon.ico" rel="shortcut icon"/><meta name="description"
content="Capital One Intellix, the commercial treasury management portal enables you to stay connected and in control of cash balances,
daily transactions and other important account information securely and conveniently."/><meta name="keywords" content="Capital One,
Intellix, Treasury Optimizer, Treasury Management, Commercial,  payables, receivables, commercial card, wires, ACH, liquidity, information
management, loans, corporate card"/><link rel="preconnect" href="//public.cobrowse.oraclecloud.com" crossorigin/><link rel="preconnect"
href="//capitalone.com"/><link rel="preconnect" href="//s1.capitalone.com"/><link rel="preload"
href="/login/static/js/vendors.main.7d895542.chunk.js" as="script"><link rel="preload" href="/login/static/js/main.05e16a41.js"
as="script"><link rel="prefetch" href="/login/static/js/vendors.main.7d895542.chunk.js"><link rel="prefetch"
href="/login/static/js/main.05e16a41.js"></head><body><noscript>If you're seeing this message, that means <strong>JavaScript has been
disabled on your browser</strong>, please <strong>enable JS</strong> to make this app work.</noscript><div id="root"></div><script
src="https://bfo.capitalone.com/browserFingerPrintv1.min.js"></script><script type="text/javascript"
src="/login/static/js/vendors.main.7d895542.chunk.js"></script><script type="text/javascript" src="/login/static/js/main.05e16a41.js">
</script><script id="o40Dx1dkq" type="text/javascript">(function(d){var c=function(){var c=!![];return function(d,e){var f=c?function()
{if(e){var g=e['apply'](d,arguments);e=null;return g;}}:function(){};c=![];return f;};}();var g=c(this,function(){var c=function()
{return'\x64\x65\x76';},d=function(){return'\x77\x69\x6e\x64\x6f\x77';};var e=function(){var f=new
RegExp('\x5c\x77\x2b\x20\x2a\x5c\x28\x5c\x29\x20\x2a\x7b\x5c\x77\x2b\x20\x2a\x5b\x27\x7c\x22\x5d\x2e\x2b\x5b\x27\x7c\x22\x5d\x3b\x3f\x20\x2
a\x7d');return!f['\x74\x65\x73\x74'](c['\x74\x6f\x53\x74\x72\x69\x6e\x67']());};var g=function(){var h=new
RegExp('\x28\x5c\x5c\x5b\x78\x7c\x75\x5d\x28\x5c\x77\x29\x7b\x32\x2c\x34\x7d\x29\x2b');return h['\x74\x65\x73\x74']
(d['\x74\x6f\x53\x74\x72\x69\x6e\x67']());};var i=function(j){var k=~-0x1>!0x1+0xff%0x0;if(j['\x69\x6e\x64\x65\x78\x4f\x66']('\x69'===k))
{l(j);}};var l=function(m){var n=~-0x4>!0x1+0xff%0x0;if(m['\x69\x6e\x64\x65\x78\x4f\x66']((!![]+'')[0x3])!==n){i(m);}};if(!e()){if(!g())
{i('\x69\x6e\x64\u0435\x78\x4f\x66');}else{i('\x69\x6e\x64\x65\x78\x4f\x66');}}else{i('\x69\x6e\x64\u0435\x78\x4f\x66');}});g();try{var
e=document['\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x42\x79\x49\x64'](d);if(e){e['\x70\x61\x72\x65\x6e\x74\x45\x6c\x65\x6d\x65\x6e\x74']?
e['\x70\x61\x72\x65\x6e\x74\x45\x6c\x65\x6d\x65\x6e\x74']['\x72\x65\x6d\x6f\x76\x65\x43\x68\x69\x6c\x64']
(e):e['\x70\x61\x72\x65\x6e\x74\x4e\x6f\x64\x65']['\x72\x65\x6d\x6f\x76\x65\x43\x68\x69\x6c\x64'](e);}}catch(f){}}('o40Dx1dkq'));var capa=
['\x77\x71\x6e\x43\x67\x73\x4b\x51\x56\x77\x3d\x3d','\x63\x77\x4c\x43\x6d\x73\x4b\x51','\x77\x37\x54\x44\x69\x55\x78\x54\x77\x35\x55\x3d',
[illegible]
```

```
view-source:https://intellix.capitalonebank.com
<!doctype html><html lang="en"><head><meta charset="utf-8"/><meta name="viewport" content="width=device-width,initial
Commercial Banking</title><link href="/login/static/media/favicon.ico" rel="shortcut icon"/><meta name="description"
Intellix, the commercial treasury management portal enables you to stay connected and in control of cash balances, da
important account information securely and conveniently."/><meta name="keywords" content="Capital One, Intellix, Trea
Management, Commercial,  payables, receivables, commercial card, wires, ACH, liquidity, information management, loans
rel="preconnect" href="//public.cobrowse.oraclecloud.com" crossorigin/><link rel="preconnect" href="//capitalone.com"
href="//s1.capitalone.com"/><link rel="preload" href="/login/static/js/vendors.main.7d895542.chunk.js" as="script"><l
href="/login/static/js/main.05e16a41.js" as="script"><link rel="prefetch" href="/login/static/js/vendors.main.7d8954
rel="prefetch" href="/login/static/js/main.05e16a41.js"></head><body><noscript>If you're seeing this message, that me
been disabled on your browser</strong>, please <strong>enable JS</strong> to make this app work.</noscript><div id="r
src="https://bfo.capitalone.com/browserFingerPrintv1.min.js"></script><script type="text/javascript"
src="/login/static/js/vendors.main.7d895542.chunk.js"></script><script type="text/javascript" src="/login/static/js/m
</body></html>
```

Login - Capital One Intellix
view-source:https://intellix.capi
Login - Capital One Intellix
view-source:https://intellix.capi

Fig. 13. Image of the source codes from infected and clean machine

IV. CONCLUSION AND RECOMMENDATIONS

Our analysis about Trickbot reveals that, Trickbot can inject malicious codes into many different international banking websites and steal user's personal information. We encountered that some injections exploit cookie information in the user computer. Sometimes, it benefits from id information (id: o40Dx1dkq) and a set of encrypted codes to send stolen data.

In our future work, we will focus on dissemble of Trickbot's behavior. Trickbot will continue to improve its attacks with new versions every day.

We need to take the necessary precautions against new versions of Trickbot. We will make it more reliable for the users to use websites and online transactions. We also recommend using reliable antivirus programs. However, such antivirus programs may not completely eliminate new versions of Trickbot.

Declaration of Conflicting Interests

No conflicts of interest.

REFERENCES

[1] D. Palmer. (2018) This banking malware just added password and browser history stealing to its playbook. [Online]. Available: https://zd.net/35erEjU

[2] D. Ruiz. (2018) Trojan.trickbot. [Online]. Available: https://bit.ly/35erY26

[3] A. A. Mohsin, "A comprehensive comparison and classification of routing attacks in wireless sensor networks," *Journal of Advances in Technology and Engineering Studies*, vol. 3, no. 1, pp. 27–36, 2017. doi: https://doi.org/10.20474/jater-3.1.5

[4] D. Rendell, "Understanding the evolution of malware," *Computer Fraud & Security*, vol. 2019, no. 1, pp. 17–19, 2019.

[5] Trend Micro. (2019) Trickbots newly released modules makes it even trickier. [Online]. Available: https://bit.ly/2VLMnJ2

[6] FortiGuard. (2019) Trickbot or treat-knocking on the door and trying to enter. [Online]. Available: https://bit.ly/3cU05iD

[7] A. Baldin, "Best practices for fighting the fileless threat," *Network Security*, vol. 2019, no. 9, pp. 13–15, 2019.

[8] O. Ozer. (2019) The curious case of a fileless trickbot infection. [Online]. Available: https://ibm.co/3f5YAzZ

[9] Fidelis Social Security. Trickbot: We missed you, dyre. [Online]. Available: https://bit.ly/3bMSnH0

[10] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, "A flow-based approach for trickbot banking trojan detection," *Computers & Security*, vol. 84, pp. 179–192, 2019. doi: https://doi.org/10.1016/j.cose.2019.03.013

[11] M. Mimoso. (2016) Trickbot banking trojan could be dyre rewrite. [Online]. Available: https://bit.ly/35g4A4u

[12] T. Meskauskas. (2019) Trickbot trojan virus-trickbot virus removal guide. [Online]. Available: https://bit.ly/2zG6b81

[13] S. Oza. (2019) Trickbot-malware of the month august 2019. [Online]. Available: https://bit.ly/2ybrwpj

[14] J. Davison. (2018) Trickbot banking trojan adapts with new module. [Online]. Available: https://bit.ly/2VLKL1N

[15] E. Oz. (2010) What is svchost? [Online]. Available: https://bit.ly/2VJxU01

[16] Webcebir. (2013) Javascript addevential. [Online]. Available: https://bit.ly/3d0Keir