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 attachment 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 occurred 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

© 2019 The Author(s). Published by KKG Publications. This is an Open Access article distributed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0.
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 an email on the user’s computer. After execution of the 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:**

- **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.
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 downloaded as follows.
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**: After 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-Tech2, 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.

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.
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](image)

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 snapshots 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](image)
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 occurred. 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. 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].

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