EUROPOL
EC3 | European Cybercrime Centre

Check Point
SOFTWARE TECHNOLOGIES LTD

Europol Public Information

Banking Trojans: From Stone Age to Space Era

A Joint Report by Check Point and Europol

The Hague,
21/03/2017

Contents

1 Introduction 3
2 The Founding Fathers 3
3 The Current Top Tier 5
4 The Latest 9
5 Mobile Threat 10
6 Evolutionary Timeline 11
7 Impressions/Current Trends 11
8 Banking Trojans: The Law Enforcement View 12
9 How are Banking Trojans used by Criminals? 13
10 How are the Criminals Structured? 14
11 Building on Public-Private-Partnerships - The Law Enforcement Response 15
12 How to Protect Yourself 16

1 Introduction

The "Holy Grail" for most cybercriminals is to steal the money of unsuspecting users. Unfortunately, there are many ways for cybercriminals to access confidential financial information, including bank account credentials. These methods include phishing campaigns with a fake bank web page, and info-stealing malware with simple keylogging capabilities for documenting victims' usernames and passwords.

Banking Trojans differ from standard Trojans, as they are written for the express purpose of stealing confidential information from victims' bank accounts and online payment services. They are sophisticated and equipped with Man-in-the-Browser (MiB) techniques such as web injections or redirection mechanisms.

2 The Founding Fathers

Zeus and its early competitors were revolutionary in the cyber-crime landscape and were the firsts to use MiB techniques.

Zeus:

Zeus was first observed in the wild in 2007 and most banking Trojans today are its descendants. Zeus is a generic Trojan which targets Windows OS users, has backdoor capabilities, and is capable of executing administrator-level functions on the infected machines. The original Zeus distribution methods were mostly through spam and drive-by-downloads attacks using Exploit Kits.

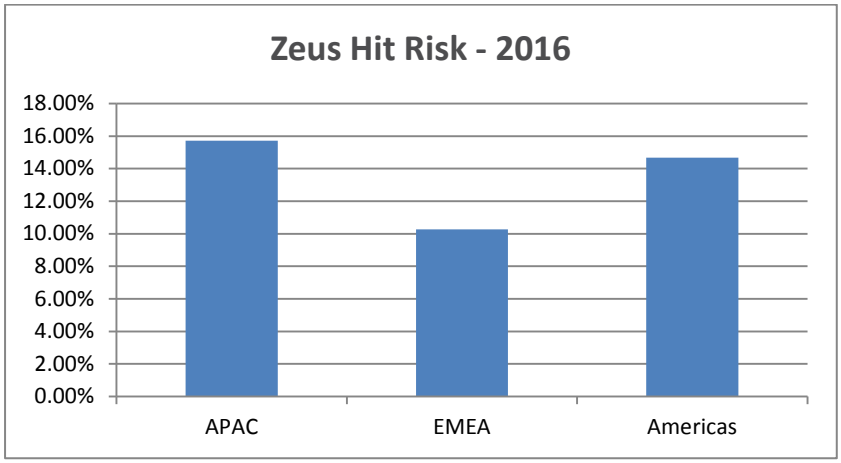
Zeus can run commands and configurations sent from its C&C (including dropping and installing other malware), but it usually arrives with a set of preconfigured functions. Some Zeus functions are web injections via API hooking.

The original Zeus was a malware-as-a-service - a criminal service which enables threat players to purchase the use of a malware. This allows the author to earn money on a regular basis without involvement in the actual money theft. Zeus was the leader in the banking Trojan world until late 2010, when its author "retired" and gave the malware's code to the author of the Spyeye banking Trojan. Zeus' source code was leaked in 2011, and currently many new variants and imitators are used by multiple threat actors.

According the Check Point researchers, the Zeus banking Trojan was revolutionary in several respects:

- It was the first malware to perform web injections.
- It built one of the biggest botnets in history, with millions of infections in the U.S. alone.

- Its polymorphic design made it difficult for security vendors to detect and block attacks based on simple file hashes.
- The original malware and its variants are still relevant today.



Spyeye:

Spyeye first appeared in 2009 as the primary competitor to Zeus. The authors even added a "kill Zeus" feature to their toolkit, which claims to remove Zeus infections from target machines. Although Spyeye displayed similar capabilities to Zeus, it didn't match Zeus' vast distribution and infection numbers, or its popularity among threat actors. In 2010, Zeus' author "retired" and shared the source code with Spyeye's author, who then merged the two toolkits.

Gozi:

Gozi malware first appeared in the wild in late 2006 as a standard info-stealer. Like Zeus, it was a malware-as-a-service Trojan, infecting its victims using a rootkit - a malicious collection of tools which gives an attacker administrator level privileges. In 2010, Gozi's code was accidently leaked by one of its authors. In that same year its authors tried to add web injections capabilities, until one of them was caught by the U.S. authorities. Since then, Gozi's leaked code has been used for the creation of new banking Trojans such as Neverquest/Vawtrak, all of which have similarities to the Zeus source code.

Carberp:

Cerberp is a modular banking Trojan which mostly targets Russian and Ukrainian bank users. It first emerged in 2010, imitating Zeus features such as web injections, stealth and info-stealing capabilities, and having bootkit module, according to Check Point researchers. In the beginning, Carberp's distribution methods included mostly phishing and other forms of social engineering.

After a major arrest of members of Carberp's network in 2012, a decrease in the amount of attack attempts was observed. The malware's source code was leaked in 2013, leading to its comeback under the hands of more threat actors.

Carberp C., a recent variant, appeared in 2015, targeting mostly Australian users. The malware counted over 150,000 infected machines just a few weeks after its discovery.

Torpig:

Torpig was first observed in the wild in 2005 as a Trojan with botnet architecture, demonstrating standard info-stealer capabilities. Similar to other banking Trojans of that time, it also developed MiB capabilities. Torpig's infection method is through drive-by-downloads using the Mebroot rootkit, which modifies the computer's master boot record, thus bypassing security measures found in the operating system. In 2009, researchers from the University of California managed to take over the botnet for ten days and investigate it. They found that the botnet consisted of approximately 180,000 machines with a total theft range of between $83K and $8.3M.

3 The Current Top Tier

Following the leak of Zeus source code, the banking Trojans world flourished, with some exceptional examples.

Game over Zeus (GOZ):

Game Over Zeus, developed in 2011, is a major Zeus variant. Its evolution and significant impact on the banking Trojan landscape was due to its communications method: peer-to-peer. It uses a structure of harvest bots and proxy bots, intermediaries between the harvesters and the C&C. Each bot communicates with its neighbors every 30 minutes, and if no response is received, it tries to contact other bots. As of October 2014, the network contained at least 200,000 bots, divided into several sub-botnets.

Thanks to its P2P network, Game over Zeus doesn't have to rely on a centralized C&C server, making it significantly harder for security vendors and law enforcement agencies to detect its activity, track its operators and take down the infrastructure. However, it still uses a domain generation algorithm as a backup communication method.

Citadel:

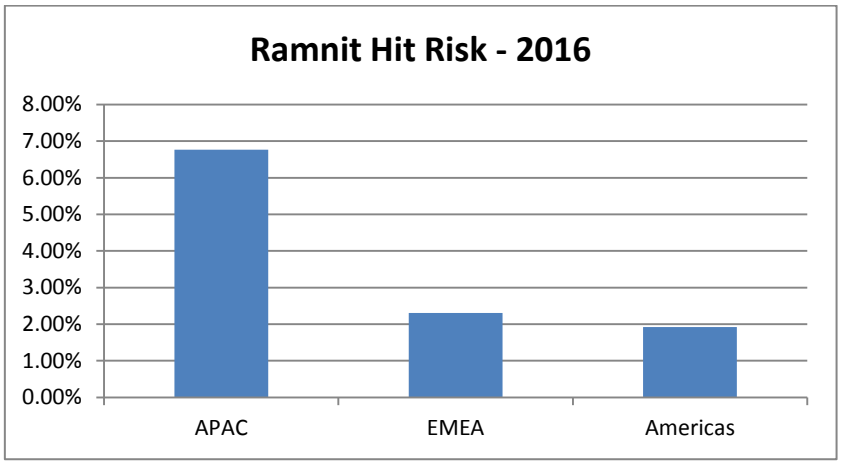
Citadel is a banking Trojan based on Zeus's leaked source code and first appeared in 2011. It is one of the most widespread banking Trojans ever, with millions of compromised computers around the world. Citadel is operated as a malware-as-a-service business, run by a devoted group of authors. The advanced support services,

together with an involved customers' community, explain its vast distribution. The Citadel payload was modified over time to deal with a large variety of websites and services, including password management and authentication solutions, such as "Password safe" or "Keepass".

Ramnit:

Ramnit is a banking Trojan that started out in 2010 as a computer worm. Some time after 2011, it assimilated Zeus' leaked code and was converted into a banking Trojan. Through the years we've seen a growth in Ramnit's distribution, and it currently ranks, together with Zeus and Tinba, on Check Point's list of the top 20 malware.

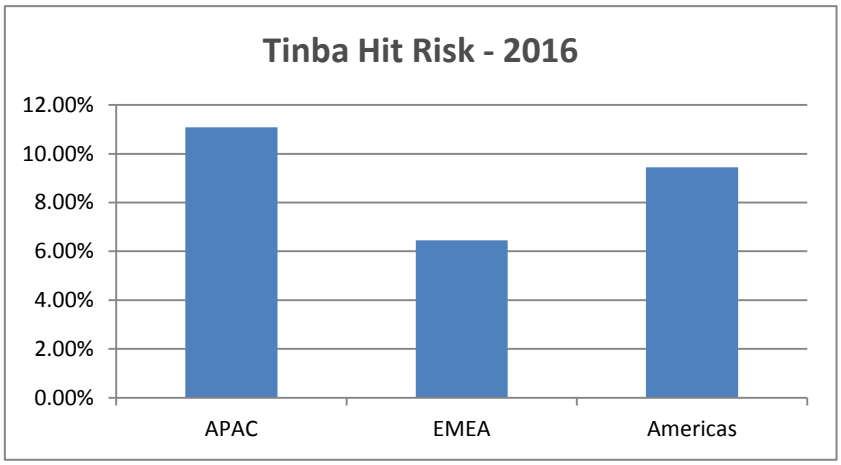
In 2015, Ramnit faced a Europol take-down attempt, yet it survived and somehow recovered. Through 2016, it ran a campaign focusing on customers of major U.K. banks.



Tinba (Tiny Banker):

Tiny Banker, also referred to as Tinba, is the smallest banking Trojan found in the wild. It consists of only 20kb and is written entirely in ASM. It was discovered in 2012, and according to Check Point researchers it boasts capabilities and a botnet architecture that are similar to other major banking Trojans such as Zeus and its variants. Tinba's code is simple and does not include any advanced encryption methods like those found in larger banking Trojans. Tinba also has rootkit capabilities that together with its size makes it hard to detect and unique in the banking Trojan landscape.

Tinba's preferred distribution methods are malvertising, spam campaigns, and Exploit Kits. Its victims can be found around the world and are targeted by geo-specific campaigns.



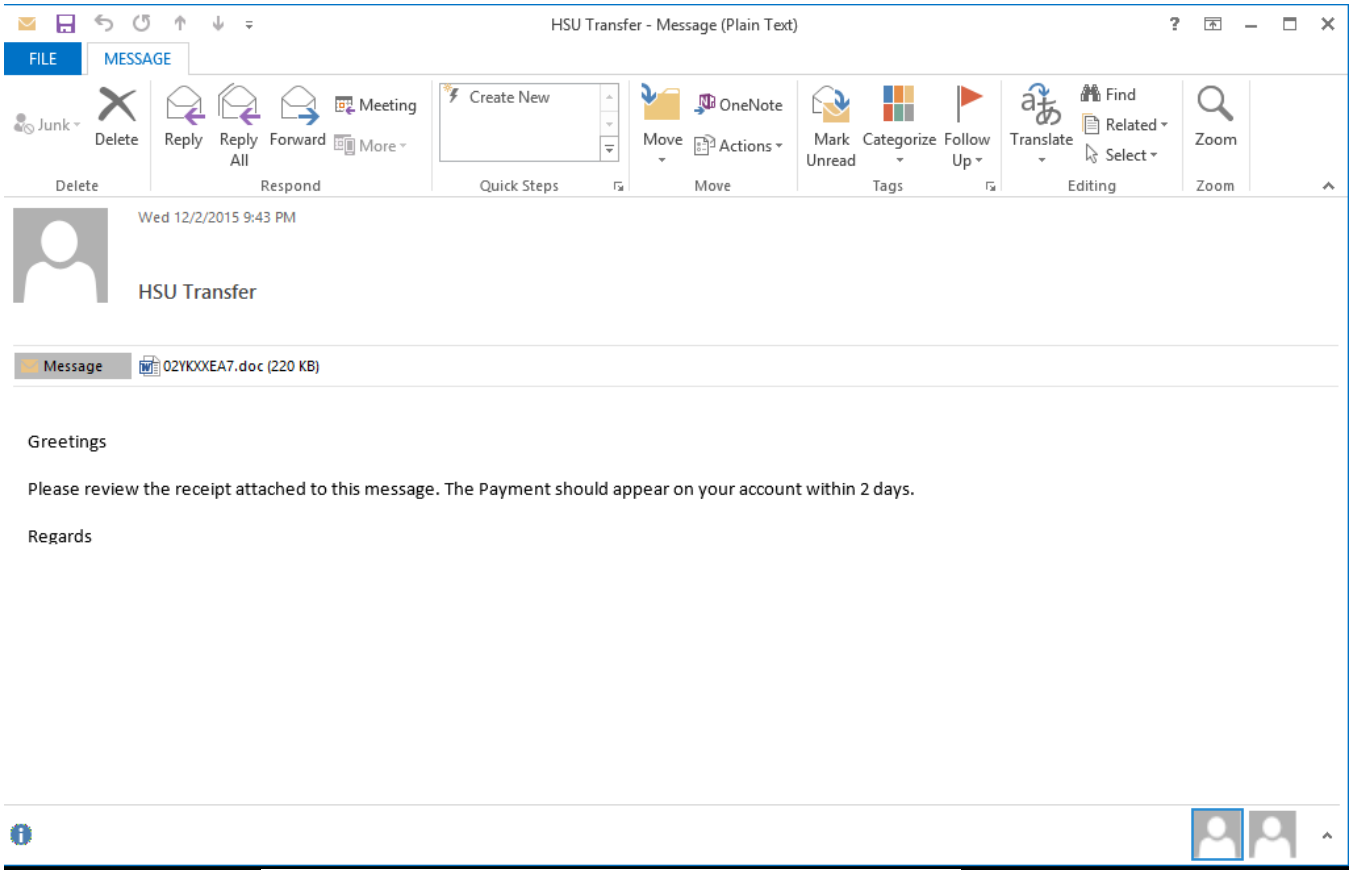
Dridex:

Dridex is a major banking Trojan that first appeared in 2014 and has been active ever since. Dridex was developed based on the source code of CRIDEX (2012), a worm that itself evolved from Zeus and was spread through network drivers and external devices.

According to Check Point researchers, Dridex has the full list of banking Trojans capabilities, such as a modular structure, MiB and info-stealing techniques. In November 2014, its botnet communication method changed from a centralized command and control to peer-to-peer communications. Dridex's botnet is divided into subnets that are able to carry out different missions. Dridex experienced a takedown operation attempt by major law enforcement agencies in October 2015 without severe consequences.

Dridex's advantage over other banking Trojans, which made it one of the most wide-spread ever, is its distribution method: the malware is spread by massive spam campaigns which run Monday-Friday at a high rate. Most of the email messages include fake receipts with malicious macros, which download Dridex to the victim machine. This attack vector has proved itself most effective on businesses and victims who are used to receiving financial information through email messages.

Dridex's victims belong mostly to English-speaking countries, and use a wide range of online financial services portals. The infection rank is pretty high, relative to other banking Trojans. Throughout 2015, at its peak, thousands of machines were incorporated into the Dridex botnet every day.



A typical spam email with malicious attachment

Dyre:

The Dyre banking Trojan first appeared in the wild in 2014. It is spread mostly by spam campaigns with fake receipts or with links to fake webpages. Throughout 2014, Dyre used the Upatre downloader to infect its victims' computers.

Dyre has the full arsenal of banking Trojan capabilities. An additional feature enables it to bypass a website's SSL mechanism by redirecting the victim's traffic as unencrypted while still displaying on an HTTPS encrypted session mark on the victim's web browser. This deception technique is highly effective against security-conscious victims. Unlike most famous banking Trojans, Dyre is unrelated to the Zeus family and its descendants, though some researchers claim to have found a connection to Gozi.

After the info-stealing phase, Dyre frequently deploys other malware on the victim machines. In many cases, it turns them into spam bots which can be used for future infections and various other malicious activities.

Dyre campaigns have been focusing on English-speaking countries. The victims are mostly customers of well-known financial institutions, but some are users of online payment services, HR websites, and even web hosting services.

Vawtrak:

Also referred to as Neverquest, Vawtrak is a descendant of Gozi that was discovered in 2013. Its common distribution method is via spam email messages with a malicious attachment, or through exploit kits. According to Check Point researchers, Neverquest has the usual set of banking Trojans capabilities. In 2015, upon the release of Neverquest V2, the operator divided its botnet into subnets.

4 The Latest

Banking Trojans are still hitting the global economy, with no end in sight. While major banking Trojans, some of which are already active for years, are launching new campaigns, 2016 has witnessed some interesting new families.

Panda:

Panda is a Zeus malware-as-a-service variant that was first observed in the wild at the beginning of 2016, and is distributed via Exploit Kits. Since its initial appearance, Panda has targeted financial services in Europe and North America. This past summer, before the Olympic Games, it also ran a special campaign against Brazilian banks.

Goznym:

Goznym is a hybrid of two malware families: Gozi banking Trojan and Nymaim downloader. Goznym's capabilities include the best of both malware; it is a powerful banking Trojan, responsible for the theft of millions of dollars from customers worldwide. It is believed that the Goznym was developed in 2015 by Nymaim's developers, who also included a Gozi leaked code. Nymain is a powerful two-stage downloader, usually responsible for infecting its victims with ransomware, until its recent shift to the banking Trojan business.

Goznym is still active; it was recently reported to be focusing on users of German financial services and banks.

Trickbot:

Trickbot is a Dyre variant that emerged in October 2016. Since its appearance, it has targeted banking users mostly in Australia and the U.K, and lately it started focusing also on India, Singapore and Malesia. It seems that a professional group of threat actors is behind Trickbot, as it is evolving rapidly. Interestingly, Trickbot banker can pull web-injection instructions from its C&C servers online when the victim tries to reach a website. This is in contrast to most banking Trojans that update their MiB configurations periodically. This feature also helps Trickbot to avoid mistakes caused by an out-of-date configuration that may lead to its discovery.

5 Mobile Threat

The financial world is going mobile, and cybercriminals are following. More and more companies offer comprehensive mobile user portals, enabling users to perform almost all financial activities via their mobile devices. This makes mobile cybercrime more and more attractive.

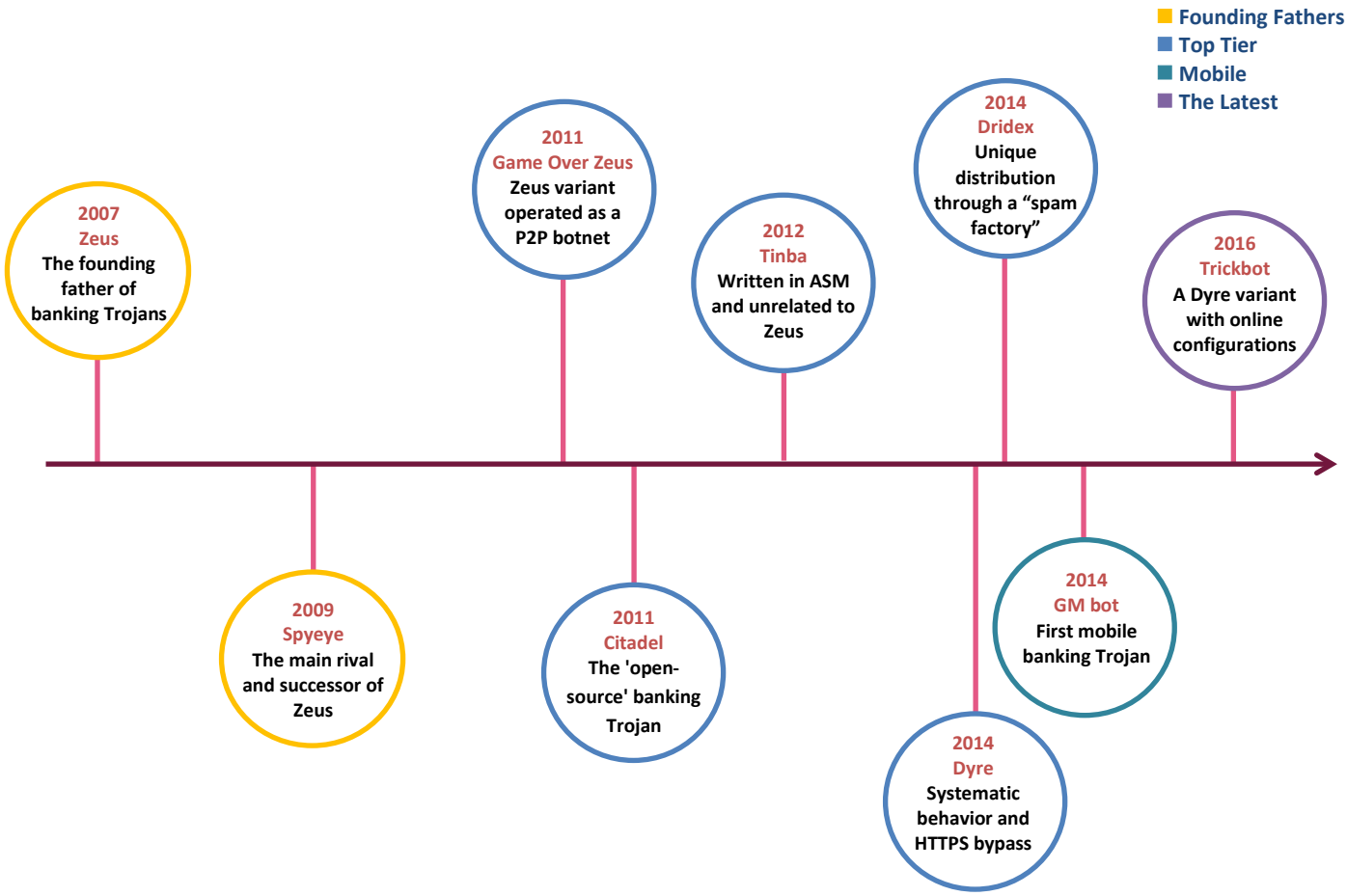
Although there's no exact equivalent to banking Trojans in the mobile world in terms of MiB attacks, these days we are definitely witnessing the evolution of mobile banking Trojans.

The biggest malware type is overlay-malware, which displays fake overlays on the mobile device when a user tries to use an application. The founder of the genre is the GM bot, which was discovered in the wild in 2014. The malware captures victims' banking credentials and confidential data by displaying overlays that look the same as banking apps' login page. The malware also intercepts SMS messages and can therefore deal with two factor authentications and steal the mobile transaction authentication number and mTAN tokens, and initiate remote money transactions.

Other money-stealing techniques currently observed in the wild include "standard" phishing attacks, in which a victim is tempted to enter a fake bank web-page and to give away his/her login credentials, and the spread of malicious fake bank apps. However, at this point, none of those is even close to the capabilities of mobile banking Trojans such as GM bot in terms of flexibility (the amount of financial services vulnerable to them) or performance (the ability to carry out monetary transactions afterward).

Mobile banking Trojans are constantly developing, with 2016 introducing several new malwares or variants. The latest examples are Faketoken, which is capable of running overlay attacks on over 2,000 financial applications, and can encrypt files and perform ransomware attacks; and Tordow, which focus on Russian victims and capable of gaining root privileges over android operating system.

6 Evolutionary Timeline



7 Impressions/Current Trends

- Although new ransomware families are constantly making headlines, pushing the good old banking Trojans out of the focus, Banking Trojans are here to stay. New variants and malwares show up periodically and infection ranks observed by our analysts are constantly on the rise. In fact, during the last year Zeus, Tinba and Ramnit didn't leave the Check Point top 20 malware list.
- Even though a while had passed since its breakdown, Zeus remains "the Greek god" of the banking Trojans world. Zeus variants occupy third place in Check Point's October's most wanted malware report.
- The evolution of the banking Trojan is occurring not only in the malware code, but primarily in the distribution methods (Dyre and Dridex as good examples of successful spam factories). We might even declare that while in the past it was easier to infect than to steal, today it has become the opposite, as there is a

growth in the general awareness to cyber threats and the effectiveness of the measures taken against phishing attacks.

- From the beginning, banking Trojans were focused primarily on financial services in English-speaking countries. This was likely due to the dominance and accessibility of English, compared to other languages. Nowadays we face an increasing trend of geographically and linguistically targeted campaigns, expanding the reach of this threat.
- Beside the technological aspect of banking Trojans, there is the criminal aspect of the money stealing operations. While operating money mules and money laundering becomes more and more difficult, we assume that we will face a growing involvement of major criminal groups in the banking Trojan world. As a result, this will lead to more investment in the banking Trojans themselves and to the development of more malware-spreading capabilities.

8 Banking Trojans: The Law Enforcement View

Over the last three years, two of the most prominent categories of malware reflected in the cases encountered by law enforcement in Europe have been ransomware and banking Trojans, with ransomware having become the norm, overshadowing other malware threats.

Nevertheless, banking Trojans remain a top malware threat and have also been expanding to mobile platforms. They are one of the main pillars of the digital underground, harvesting victims' credentials and logins, and providing attackers with access to their accounts.

More recently, due to the fact that support for many of the 'old school' banking Trojans such as Zeus, Citadel or Spyeye has stopped, either voluntarily or as a result of law enforcement action, new generations of malware like Dyre or Dridex have appeared, the latter targeting back-end payment processing systems, Point of Sale (POS) systems and other types of financial apps as well. Law enforcement also notices a 'comeback' of Ramnit.

New variants often offer different capabilities like DDoS functionality or the possibility to download other malware onto infected systems. Malware is also becoming increasingly 'intelligent' for instance by preventing it either from being deployed or run in a sandbox environment. In this way malware developers can avoid automated analysis of their product, thereby remaining undetected for longer.

Facilitated by a mature and professional 'as-a-Service' digital underground market characterised by a division of labour, banking malware often depends on different criminal activities or services that contribute to the overall attack. Consequently, attacks

may involve several different groups or individuals responsible for developing or providing these activities or services, ranging from coders, bullet-proof hosters and domain registration providers, crypters and spammers to money mule herders, to mention some. Malware is often supplied by resellers rather than the original developers indicating further niche roles in the marketplace.

9 How are Banking Trojans used by Criminals?

The obvious answer is that with the stolen credentials criminals will pretend to be a legitimate online banking system customer and will initiate an electronic payment to an account that is fully controlled by them. The manipulation of a victim's account requires thorough preparation, mostly based on previous experience and knowledge dealing with the particular financial institution, to ensure the success of these transactions. For instance, this may require identifying the reasons why a particular account of a money mule has been blocked or suspended.

Therefore, criminals prefer to deal with the same bank account and internal payments to ensure that such payments will arrive in the money mule's account as soon as possible, preferably on the same day. It should not come as a surprise that criminals are in favour of fast payment options as offered in some countries such as the UK or Germany.

Apart from using the stolen credentials directly, criminals typically do not offer valid banking credentials and "live banking bots with a positive account balance" on underground markets. As an exception, they might share the burden with other close partners for a certain percentage of every successful withdrawal, particularly if a very large number of accounts has been compromised. As mentioned before, most banking Trojans nowadays come with additional functionality so even if the transfer is unsuccessful for instance due insufficient balance, criminal will still try to monetise the install to be used in other criminal schemes such as ransomware.

In the case of a successful transaction, once the money mule's account has been credited, the criminals will make efforts to withdraw the funds as soon as possible. The funds will then be transferred to the cybercriminal in a way initially agreed on. This phase is usually considered as the most risky by criminals as there is no honour among thieves, as the saying goes.

Once the first withdrawal has been successfully completed more fraudulent transactions will follow.

10 How are the Criminals Structured?

Bearing in mind the division of labour model within the underground community, every link in the cybercrime value chain performs their own specialised task (see Figures 1 and 2):

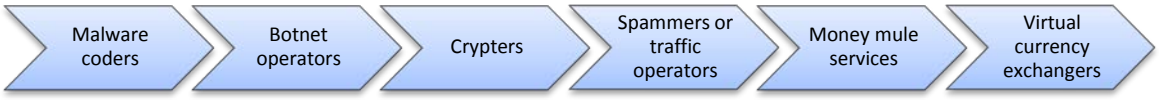


Figure 1: Simplified overview of the banking Trojan cybercrime value change

Botnet operators tend to be relatively small groups of criminals utilising easy-to-deploy malware kits designed for less tech-savvy criminals. Typically these groups consist of at least two to three persons, namely: a person responsible for technical tasks and botnet administration; a few individuals aka "monetisers" responsible for monetising "compromised bots" and taking care of fraudulent transactions; a manager responsible for negotiations with other services offering traffic, exploit kits, cash withdrawals etc.

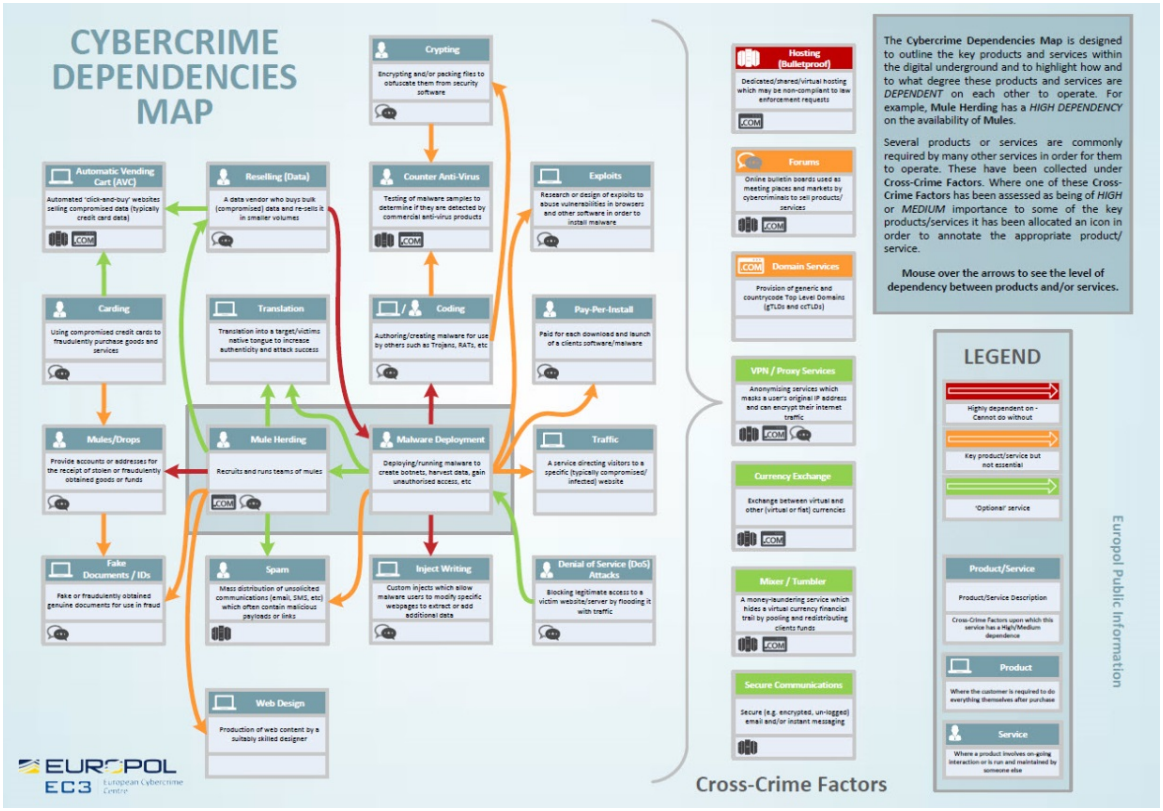


Figure 2: Cybercrime Dependencies Map showing the dependencies between the main products and services in the underground economy[i]

Most of the communication between the criminals takes place through online communication platforms.

In general, cybercriminals tend to be very vigilant and constantly endeavour to hide their identities and take advantage of legitimate technologies, making them harder to trace and identify. Hence, their preference for large networks of money mules to help disguise the illicit origin of fraudulent transactions and evade legal consequences.

Moreover, cybercriminals increasingly make use of malicious kits with advanced stealth features and software specifically designed to evade detection by using multiple layers of obfuscation and anti-forensics techniques. This could include the use of destructive measures targeting the victim's computer once it has been exploited (such as destroying its Master Boot Record) in order to evade detection and prevent malware researchers from analysing the functionality of the banking Trojan.

11 Building on Public-Private-Partnerships - The Law Enforcement Response

Early banking Trojans such as WSNPoem/Zeus and Sinowal/Torpig came rather unexpectedly for the European banking industry and caused significant losses. For many of these banks those were the first encounters with complex targeted online banking Trojans. However, this also marked the beginning of successful intelligence sharing initiatives and closer collaboration amongst banks and with law enforcement.

Nearly a decade later, many banks have seen a decrease in banking Trojans and phishing attacks partly due to the increased collaboration and increased willingness to share intelligence.

For law enforcement one of the top priorities is the apprehension and prosecution of malware developers. Successful law enforcement action on such groups can have considerable impact, not only removing the immediate threat caused by their product but also preventing future product development or refinement by some of the more talented malware developers who are typically also harder to replace in the cybercrime ecosystem.

For law enforcement it is also essential to continue to build and maintain partnerships with the financial sector but also the internet security industry. They hold a contemporary picture of the cybercrime landscape at a broad, strategic level which law enforcement often lacks. The internet security industry also holds a wealth of data which could assist in identifying and prioritising targets. Furthermore, the financial sector and the internet security industry can provide insight into new and emerging threats to allow law enforcement to better prepare and take preventative action. In this

context, security should not be seen as a comparative advantage but a collaborative effort where the attack against one bank equals to the attack against all banks.

12 How to Protect Yourself

We highly recommend you take the following steps to protect yourself from banking Trojans, or at least mitigate its effects:

- **Exercise caution** – Don't open emails you don't expect to receive, and if you are asked to run macros on an Office file, DON'T! The only situation in which you should run macros is in the rare case that you know exactly what those macros will do. Additionally, keep track of the latest major malware campaigns to ensure that you do not fall victim to a new unique phishing technique or download a malicious app.
- **Have a comprehensive, up-to-date, security solution** – High quality security solutions and products protect you from a variety of malware types and attack vectors. Check Point Sandblast Zero-Day Protection efficiently detects and blocks banking Trojans samples, and extracts malicious content from files delivered by spam and phishing campaigns.
- **Be alert for "weird" behavior of banking and financial services websites** – Pay attention to extra login fields you weren't used to seeing in the past (especially of personal data or things that the bank is not supposed to ask for), changes in the login page design, and any tiny flaws noticeable in the web site display. If something looks suspicious, try to login from another device and compare the displays. Always remember that banking actions can also be done through other means.
- **Install mobile applications, and especially bank applications, only from known and trusted sources** such as Google Play and Apple's app store. This will not guarantee that you do not download malicious apps, but will protect you from most threats.
- **Back up your most important files** – Make an offline copy of your files on an external device and an online cloud stage service. Common banking Trojans today follow the infostealing phase with deploying other malware, including ransomware which can hold your files hostage until you pay. Note: External devices should be used for backup ONLY and be disconnected immediately after the backup is completed.

[i] https://www.europol.europa.eu/publications-documents/cybercrime-dependencies-map

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu