Symantec

SECURITY RESPONSE

Financial threats 2015

Candid Wueest

Version 1.0 – March 22, 2016

“The attacks still mostly rely on email, social engineering, and man-in-the-middle browser manipulation through webinjects.”

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

CONTENTS

OVERVIEW

Financial Trojans that target online banking services have plagued financial institutions for over a decade. The attacks still mostly rely on email, social engineering, and man-in-the-middle browser manipulation through webinjects. The cybercriminals behind these threats have well-established methods to circumvent two-factor authentication (2FA) and attack mobile banking. We have also seen an increase in redirection attacks, where the victim is rerouted to a fake website that handles the manipulation of traffic sent from and to the client.

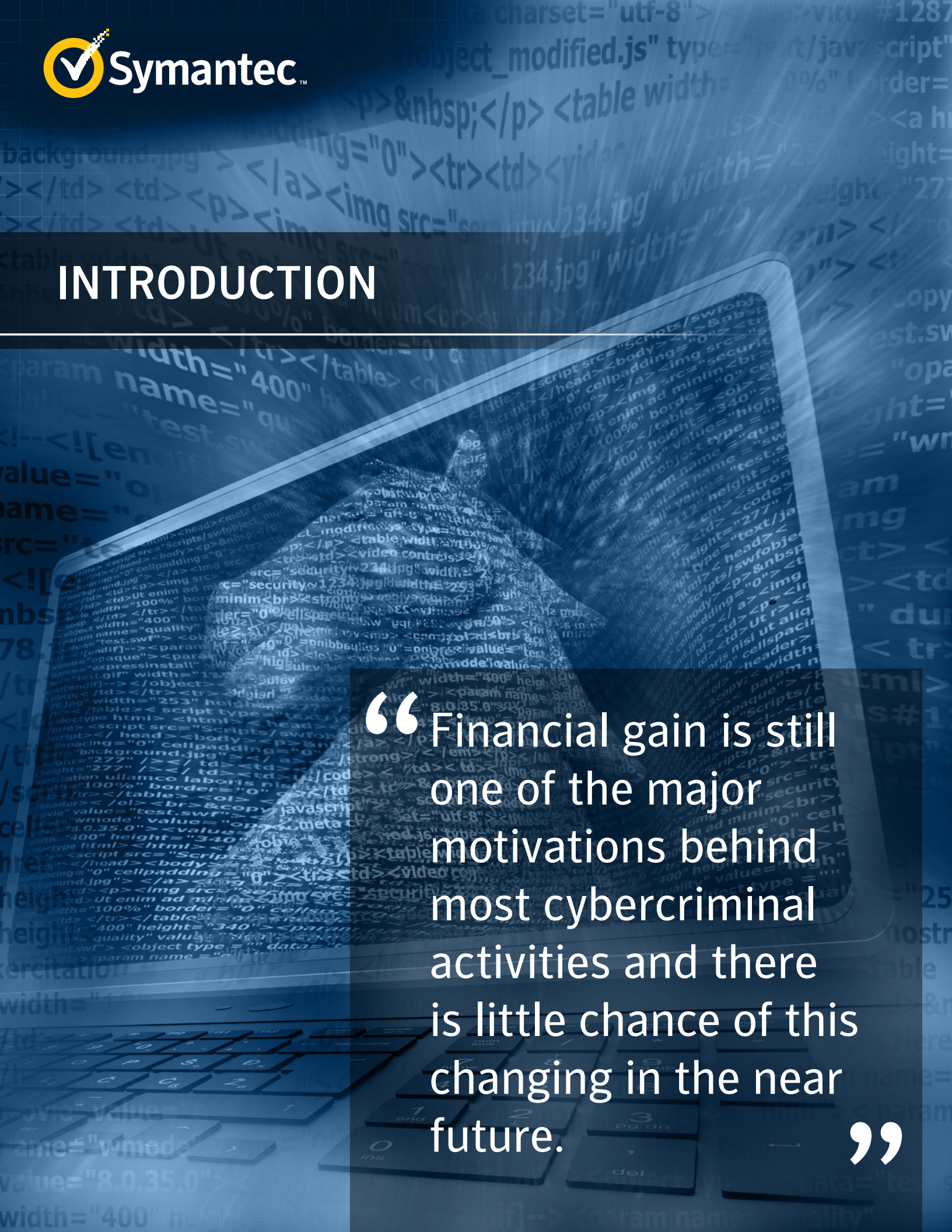
One trend that has become evident over the last year is that cybercriminals are increasingly moving beyond banking customers and are now also targeting financial institutions directly. Once inside the financial institution's network, the attacker can learn how to transfer money, issue fraudulent transactions, or orchestrate ATM machines to dispense cash.

Another scheme that has become more prevalent among criminals is the business email compromise (BEC) scam, whereby the financial department of a company is convinced to carry out a transaction in favor of the attacker. These BEC attacks do not involve malware and do not tamper with the online banking service, but instead rely solely on social engineering.

This paper is an update to last year's paper (The state of financial Trojans 2014) and examines eight of the most common and sophisticated financial Trojans.

Symantec

INTRODUCTION



> “Financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in the near future.”

Key findings

- The number of financial Trojan detections year over year dropped 73 percent in 2015.
- The primary distribution vector for financial fraud malware is through malicious spam email attachments.
- The trend of using Office documents containing malicious macros as droppers continued in 2015.
- 547 institutions in 49 countries were targeted by the 656 analyzed financial Trojans.
- The average number of targeted organizations per sample was 93 in 2015, an increase of 232 percent over the previous year.
- The average number of targeted URL patterns per sample was 283 in 2015, an increase of 405 percent over the previous year.
- Dridex (W32.Cridex) targeted a total of 315 different institutions; Shifu (Infostealer.Shifu) targeted 16.
- The most targeted bank is located in the US and was attacked by 78.2 percent of all analyzed Trojans.
- Dridex infections increased by 107 percent in 2015, making it the fastest growing family of financial Trojans.
- Redirection attacks have increased again.
- The USA is the country with the most infections, followed by Germany and India.
- Stolen accounts are sold for 5-10 percent of the balance value.

Introduction

Financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in the near future. Cybercriminals are constantly trying to make money, as evidenced by the black market industry that has arisen around payment card fraud. Cybercriminals have no problem coming up with different scams to make money. For example, the pump and dump swindle still works; we observed a Waledac spam campaign in November that successfully doubled the targeted stock price for the attackers. Other scammers tried to blackmail users of the Ashley Madison dating service after it was breached. Fake advertisements and advanced-fee scams are widely used as well—on house letting platforms and car buyer forums for example—to con people out of their money.

This whitepaper focuses on attacks against financial institutions and their customers; for example attacks against online banking services, or rather against users of those services, which, besides payment card fraud, is still the most prevalent threat against the financial sector. This is the third annual report we have released in relation to financial threats and scams. These reports document the changes and trends we have seen in attacks on the financial sector. For more information about the history of financial Trojans and the observed evolution of their techniques, have a look at our whitepapers from 2014 and 2013.

The underground financial fraud community is well organized. Everything from malware kits to distribution services to scam configurations are sold or rented out for cash. The community offers specialized and dedicated services for "cash out" (a term used on underground forums, meaning to get money from victim accounts) and for any other aspect of the scam life cycle.

Nowadays, the most widely adopted security measurement in the financial industry is two-factor authentication (2FA). The implementation details vary quite a bit depending on the organization. Such systems greatly enhance the security of online transactions, compared to static

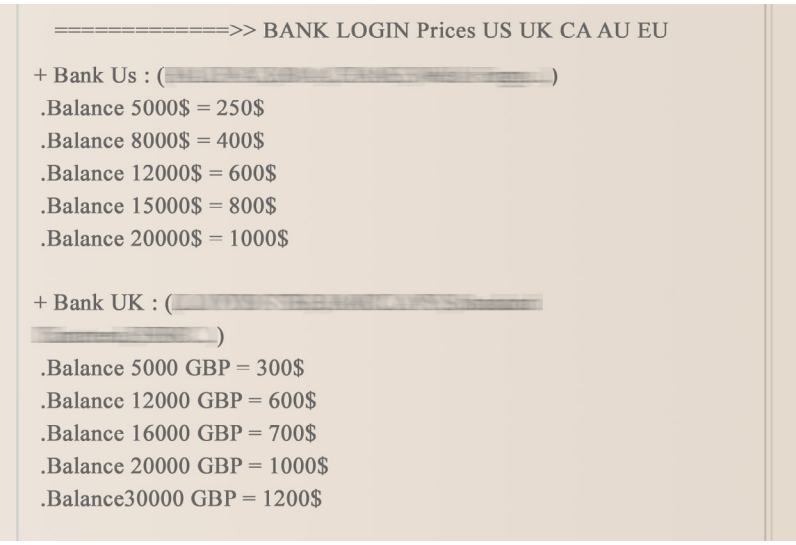


Figure 1. Underground forum advertisement for stolen bank accounts

passwords on their own. Some banks send an SMS with a transaction authentication number (TAN) for authentication, while others go one step further and use transaction signing, where the transmitted code is only valid for one specific transaction. The methods used to secure the transactions have not changed considerably over the last three years. Unfortunately, with convincing social engineering tricks and smartphone malware many of these strong security measures can be circumvented by determined and sophisticated attackers. Some banks are even discussing the possibility of removing 2FA for smaller transactions to save costs.

In terms of the battle for dominance of the financial Trojan market, the number of detections for the Dridex/Cridex family more than doubled in 2015, making it one of the top financial Trojans for last year, followed by Dyre. More information on the technical details of these two threats can be found in the following whitepapers:

- Dyre: Emerging threat on financial fraud landscape
- Dridex: Tidal waves of spam pushing dangerous financial Trojan

Prevalence

To get a feel for the shape of the financial threat landscape, it's useful to take a look at how the space is divided up across the various threat families. For this research we focused on the following commonly used financial Trojans, which represent the current market situation: Dridex/Cridex (W32.Cridex), Zeus (Trojan.Zbot), Citadel (a variant of Zeus), Snifula (Trojan.Snifula), Dyre (Infostealer.Dyre), Bebloh (Trojan.Bebloh), Shifu (Infostealer.Shiz), and Carberp (Trojan.Carberp).

Zeus, along with all its variants, was again responsible for most of the financial Trojan detections in 2015. The Zeus family grew from 400,000 detections in 2012 to nearly 4 million in 2014, but then dropped to just under 1 million in 2015. This is a continuation of the downward trend that we discussed in 2014. This is indication that cybercriminal groups are moving to other, more current, financial malware families with similar features, such as Dridex and Dyre. Other groups have changed to ransomware and other money making schemes.

Table 1. Number of detections of common financial Trojans in 2015 and 2014

Threat	Compromised computers in 2015	Compromised computers in 2014
Zeus/Citadel & variants	960,000	4,000,000
Dridex/Cridex	60,000	29,000
Dyre	55,000	90,000
Bebloh	13,000	11,000
Snifula	4,500	21,000
Carberp	400	500
Shifu	200	N/A

To illustrate how the top players in the world of financial Trojans can fluctuate, let's take a look at Infostealer.Dyre, which emerged and filled some of the void after the Zeus and Shylock takedown operations of 2014. The growing prevalence of Dyre in turn lead to an increased interest from law enforcement into the group behind Dyre. Ultimately, it peaked in a takedown operation in November 2015. As result of law enforcement actions, a number of the financial fraud Trojan groups sustained significant blows, but are still active; although detection figures have declined substantially. Another malware family that profited from the gap created after the takedowns was Dridex, which doubled its infection numbers from 2014 to 2015. Sure enough, this growth caused Dridex to itself become the focus of a takedown effort in October 2015. Figure 3 shows how Dridex/Cridex infections saw a 13-fold increase in May and later dropped again. This reflects the trend we have seen in

2015 of different families spiking temporarily. It also demonstrates that too much dominance in the marketplace will quickly draw the attention of law enforcement.

The downward trend in financial Trojan detections should not be misinterpreted as a sign that the problem is solved and will disappear soon. While it is getting increasingly difficult for the attackers to successfully steal money from financial institutions, it is still an extremely lucrative endeavor for cybercriminals. It should also be noted that Symantec products can offer multiple layers of protection in order to protect customers as early in the infection chain as possible. Therefore we have blocked many users from visiting infected websites and blocked web exploit toolkits from dropping malware onto computers in the first place. This increased success in early prevention leads inevitably to fewer detections of Trojans on computers. Because of this, we cannot always predict which malware would be dropped if the infection attempt had been successful. Therefore, the real number of attempts by the cybercriminals to infect computers with financial fraud Trojans is most likely higher, particularly for some infection routes that groups behind financial Trojans tend to favor.

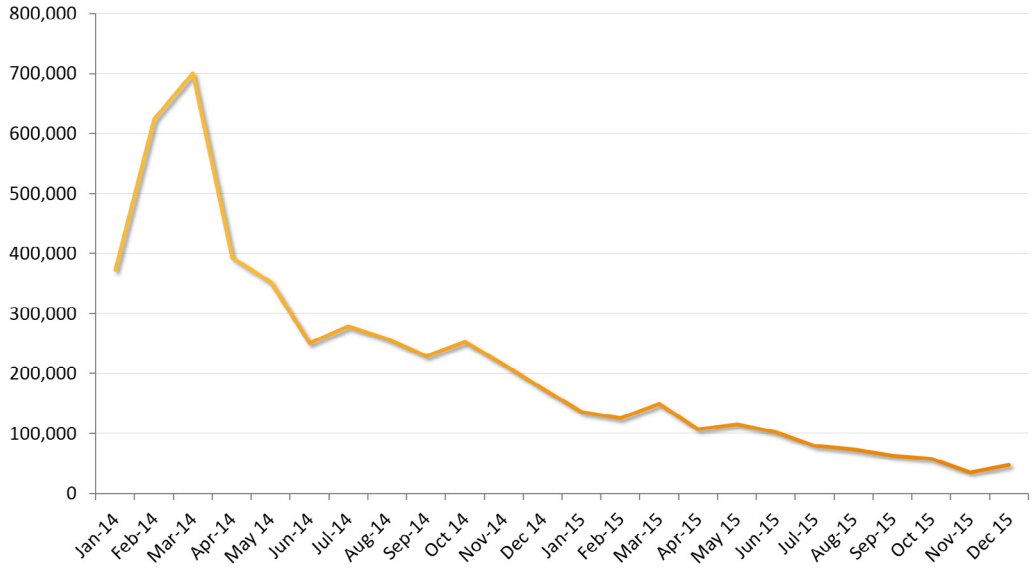


Figure 2. Computers compromised with banking Trojans, 2014 to 2015—showing a major drop

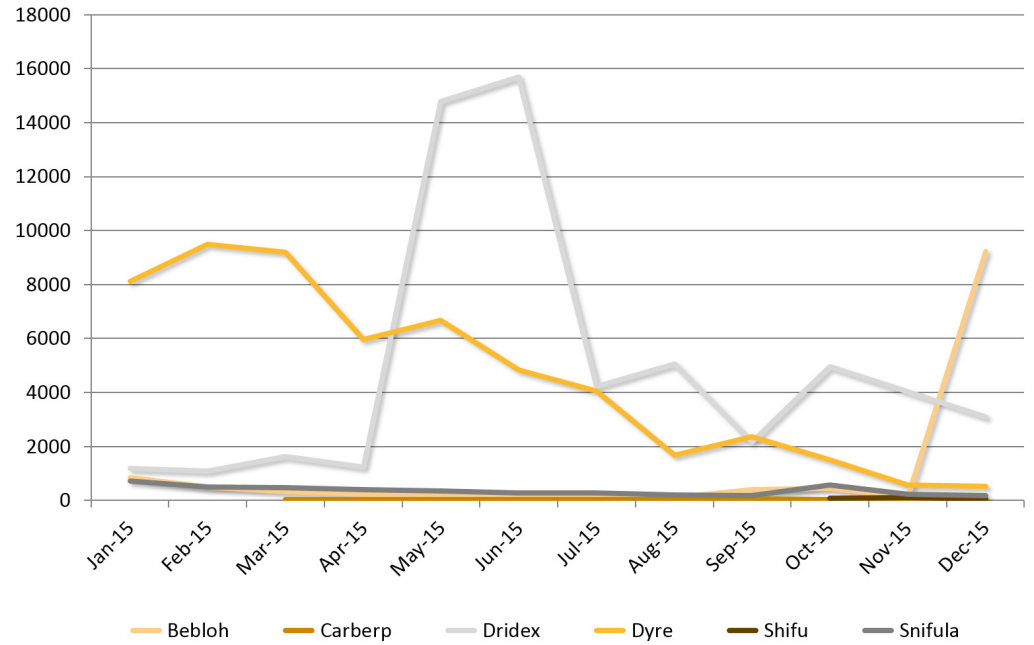


Figure 3. Computers infected in 2015 by the top financial Trojan families (excluding Zeus)

Symantec

GEOGRAPHICAL DISTRIBUTION

> “The USA still ranked first, as it has done for the past three years. This is not too surprising, given the large number of banks and internet users in that country.”

Geographical distribution

Looking at detections by region showed some interesting changes in 2015 in relation to the top 10 rankings. The USA still ranked first, as it has done for the past three years. This is not too surprising, given the large number of banks and internet users in that country. Germany and India have both gradually moved up the rankings over the last three years; India moving up two places in 2015 to the number three spot and Germany moving up one place to take the number two position. However, the absolute numbers did decrease in all countries, as seen by the global trend. The United Kingdom dropped from 2nd to 5th place in 2015. The number of detections in the United Kingdom was 64 percent smaller than the corresponding number of detections in Germany. A few larger spam runs of Dyre contributed to the increased number in Germany. Part of the drop in ranking of the United Kingdom can be attributed to the takedown activities in England. The rest is most likely due to the changing focus of the new malware families that were analyzed this year.

Table 2. Regions ranked by number of financial Trojan infections seen per year

Region	Rank in 2015	Rank in 2014	Rank in 2013
USA	1 →	1	1
Germany	2 ↑	3	4
India	3 ↑	5	7
Japan	4 →	4	2
United Kingdom	5 ↓	2	3

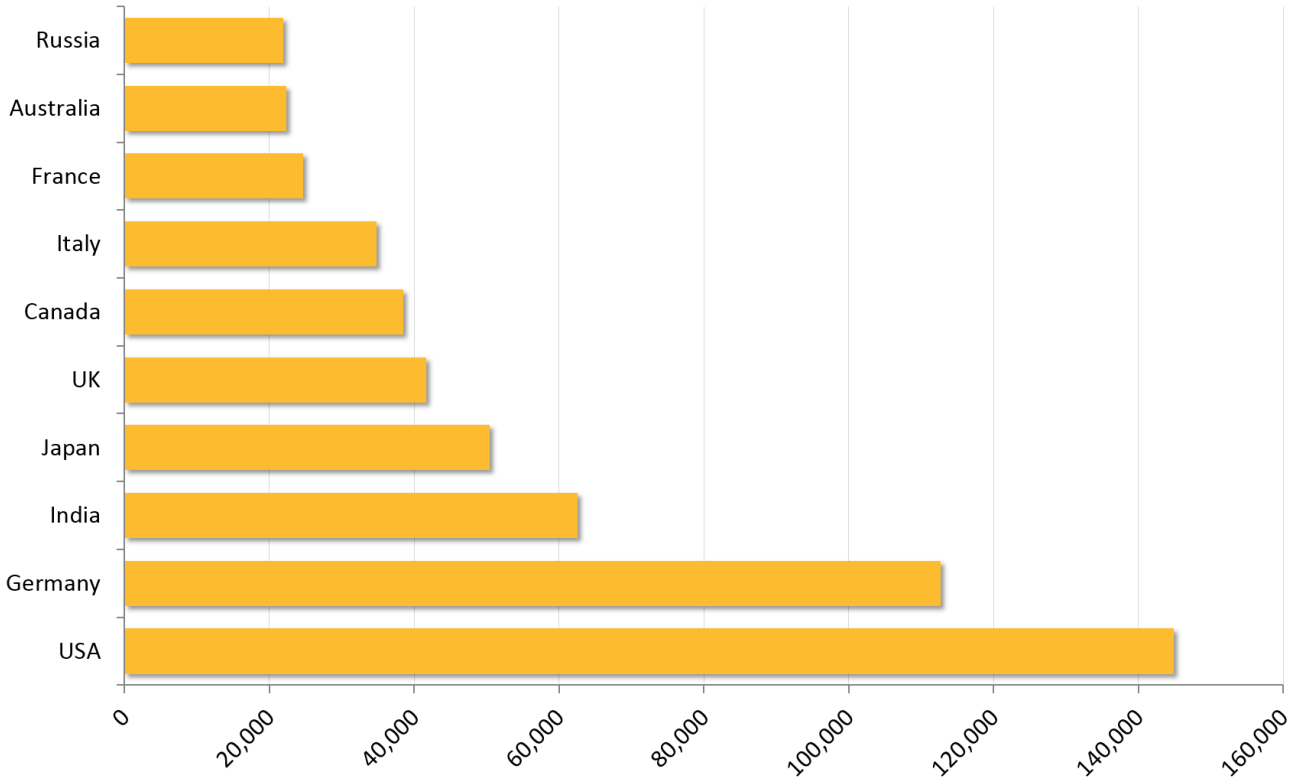


Figure 4. Computers, by country, compromised with banking Trojans in 2015

Some of the threats have a very narrow geographical focus and are not distributed internationally. For example, Infostealer.Shifu, which emerged at the end of 2015, is mainly found in Japan, which explains the low number of infections compared to other threats. The increased activity of financial fraud malware in Japan is a continuation of the trend we observed last year, where threats such as Infostealer.Torpplar, Infostealer.Bankeiya, and Trojan.Snifula were increasingly active in the country. The trend continued with Trojan.Broluxa and Trojan.Bebloh expanding into Japan as well. Therefore, although these threats are not major players on the global cybercrime market, they are very much relevant for their specific region. Such threats have successfully adapted and specialized in their niche. It is unclear if the threats have been sold to new groups in different regions that are now building up their networks, or if the old groups have expanded their reach to encompass these new, previously untapped territories.

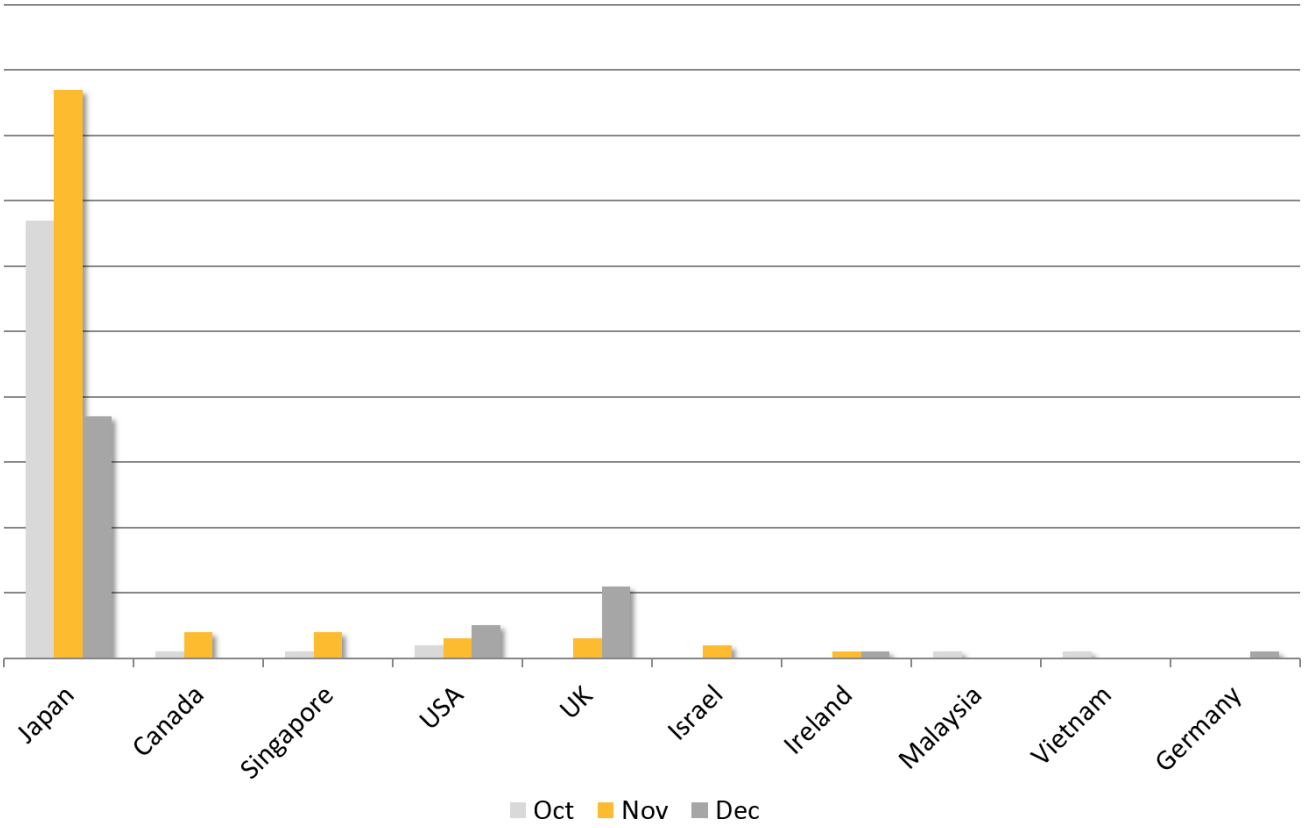


Figure 5. Infostealer.Shifu detections by country, showing a distinct focus on Japan

Symantec

TARGETED INSTITUTIONS

> “All types of financial institutions are targeted, from small local branches to big global players.”

Targeted institutions

One of the attack methods employed by most modern banking Trojans is an updatable and encrypted configuration file stored in the file system, the registry, or embedded in the Trojan itself. This set of configuration directives, often referred to as a webinject, contains the URLs that the Trojan watches for during man-in-the-browser (MitB) attacks. Overtime, new configurations can be pushed down from the command and control (C&C) server if needed; for example, to adapt to changes made by the bank or configurations based on the victim's IP geolocation to better fit the local environment. About 656 configurations were examined in our analysis, which were extracted from recent samples and active C&C servers. Over 2,084 URL patterns belonging to more than 547 distinct institutions in 49 countries were identified.

All types of financial institutions are targeted, from small local branches to big global players. Traditional commercial banking websites were still the focus of most of the campaigns, but attackers were also after credit unions, bank-to-bank services for high value transactions, or clearing houses. Basically, any service that allows the transfer of money is of interest to the criminals.

The majority of the targeted institutions belong to the financial sector, the rest were online services like social media networks, auction houses, and webmail services. Although still low in quantity, we have seen financial threats that target crypto currencies like Bitcoin, as well as voucher and bonus point programs from airlines, hotels, and retailers. Stolen accounts for such services are either sold on underground forums or used to distribute spam. It should be noted that just because a Trojan targets a specific organization it doesn't necessarily mean that it was successful in defrauding customers, as multiple mechanisms may be at play in the background to help prevent fraud; like the correlation of suspicious transactions over multiple accounts or comparison of new transactions to the behavioral history of a client.

Table 3 lists the top 20 institutions ranked by how frequently the Trojan configuration files target them. The targeted institutions have been anonymized; however, specific institution identities are available to financial institutions by request. Seven out of the top 20 targets do not require two factor authentication for the login process, but most of them allow at least the optional setup of a second authentication factor when a new payee account is created. This shows that not only institutions with weak security processes are targeted.

Table 3. Top 20 institutions targeted in Trojan configuration files

Rank	Institutions	Locations	Percentage of Trojans targeting firm
1	Bank 1	United States	78.20%
2	Bank 2	United States	77.90%
3	Bank 3	United Kingdom	69.36%
3	Bank 4	United Kingdom	69.36%
5	Financial services group 1	United States	69.05%
6	Bank 5	United Kingdom	68.45%
7	Bank 6	United States	62.65%
7	Bank 7	Spain	62.65%
9	Financial services group 2	United Kingdom	60.98%
10	Bank 8	United Kingdom	58.54%
11	IT services organization	Russia	58.23%
12	Bank 9	Canada	57.77%
13	Bank 10	Switzerland	57.16%
14	Bank 11	United Kingdom	57.01%
15	Bank 12	United Kingdom	56.55%
16	Bank 13	United Kingdom	55.49%
17	Bank 14	United Kingdom	55.34%
18	Financial services group 3	United Kingdom	54.73%
18	Bank 15	Australia	54.73%
20	Bank 16	Ireland	54.12%

In 2014, the top targeted bank was attacked by 94.5 percent of the samples, in 2015 the same institution was ranked at number 126, with 44 percent of the samples targeting it. This substantial drop is due to the fact that the target URL was previously in the default example configuration file of the Citadel Trojan and therefore very common. Last year the groups seem to have reviewed their strategy and removed the webinject pattern for this particular bank from most samples.

The average number of organizations targeted per sample in 2015 was 93, an increase of 232 percent, compared to an average of 28 in 2014. Although this number heavily depends on the selected sample set, it is still a good indication that the cybercriminals are broadening their scope and attempting to attack more organizations. We have seen more samples with a broader set of targets; this is likely an effort by the criminals to increase their chances of turning a profit. This could be an indication that the malware is being used by a more diverse group and that they are trying to compensate for the declining infection numbers by targeting more organizations.

Table 4. Average number of targeted institutions per malware sample

	2015	2014
Average number of attacked organizations per sample	93	28
Average number of regular expression patterns per sample	283	56

Similar trends can be seen when comparing the average URL patterns listed per sample. In 2015, each sample had 283 URL patterns listed on average, where as in 2014 the average was 56 patterns per sample. This number is also influenced by the higher number of third-party services that offer to create such webinjects and therefore will create their own, slightly different regular expression patterns. Not all of the used regular expression patterns can be assigned unambiguously to a corresponding service URL. For example, the pattern "*/Authentication/Login*" used in many Dyre samples is just too generic and could map to many different service URLs.

The type and number of institutions targeted varies across financial Trojan families. The number and range of targeted institutions is especially high on publically available Trojans, such as Zeus, which are used by many different groups. Other privately held threat families sometimes focus on a handful of organizations, moving to different ones over time in order to stay below the radar of law enforcement or when the efficacy rate drops. Different global factors can also influence attackers' decisions in regards to targeted institutions, such as language considerations and countries where international transactions are more difficult and may require local steps to launder the money. Across all analyzed samples Citadel targets a total of 164 different institutions but the threat only targeted an average of two organizations per sample. This low number can be explained by the fact that these are the default organizations in the example webinject that comes with the Trojan. The author most likely had an issue updating the webinject, for example due to a C&C server that is no longer online, and therefore the Trojan had only two organizations in its setup.

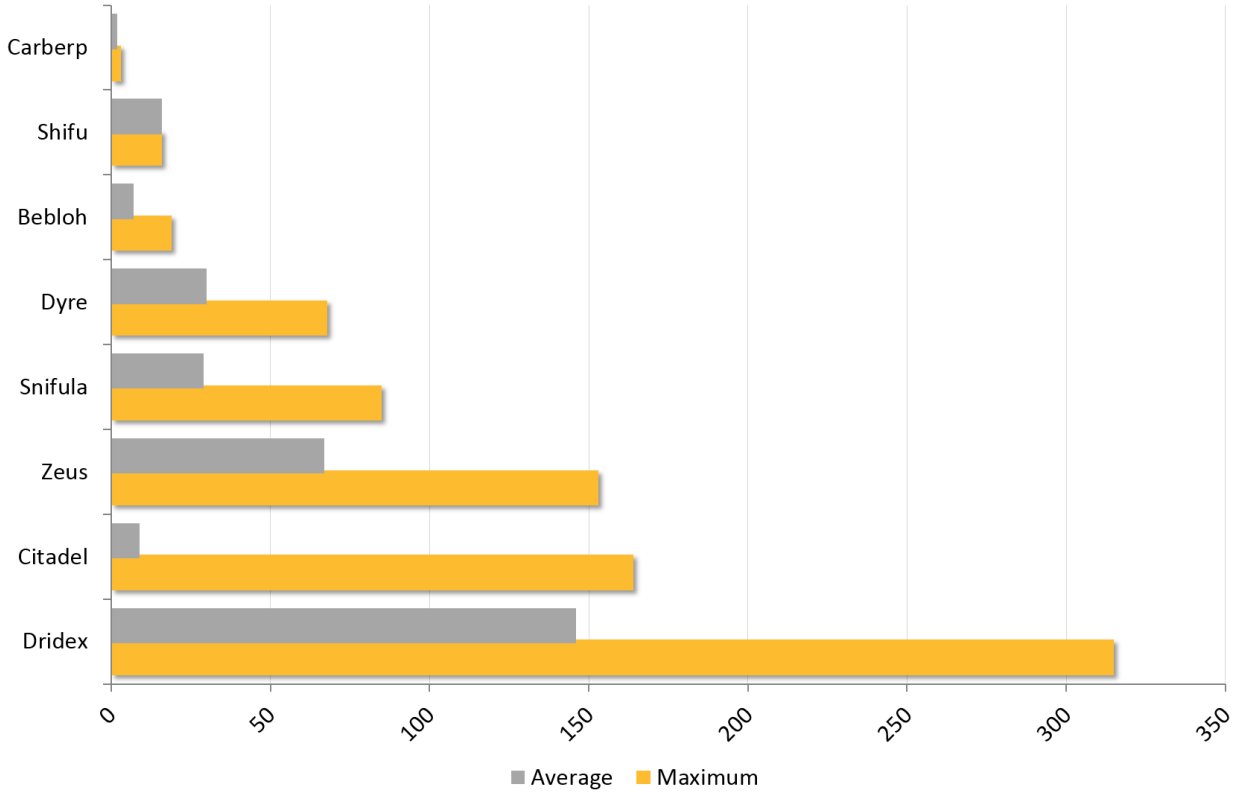


Figure 6. Average and maximum number of institutions targeted by each Trojan family in 2015

Symantec

ATTACK METHODS

> “The most common and well documented method used by financial fraud malware is the MitB attack, often using webinjects.”

Attack methods

There are multiple ways for an attacker to profit from a compromised computer. Infostealer.Shifu, for example, is a sophisticated banking Trojan that contains the typical features used for financial fraud. Shifu steals a large variety of information that victims use for authentication purposes. It uses keylogging to steal passwords, grabs credentials typed into HTTP forms, steals private certificates, provides remote control over compromised computers, and scrapes external authentication tokens used by some applications. Shifu even targets payment card data if it detects that it has compromised a point-of-sale (POS) endpoint computer. Shifu uses many methods to maximize potential profit for its distributors; however, its many features represent just the tip of the iceberg when it comes to all the methods available to the criminals behind financial threats.

The following sections list the most common trends and attack methods, beyond simple keylogging, that we observed in 2015.

Man-in-the-browser attacks

The most common and well documented method used by financial fraud malware is the MitB attack, often using webinjects. This attack method allows the Trojan to locally modify all traffic from and to the browser, opening the field for social engineering or for transactions to take place in the background. The most common way to accomplish a MitB attack is to inject a module into the web browser, which handles the modifications. This method often focuses on the popular browsers, such as Internet Explorer, Firefox, and Chrome.

Newer webinjects often also target the departments in banks that deal with corporate customers, in order to fish for high quality accounts. Readymade webinjects are sold for less than US$100 on underground markets. With this method, the SSL encryption is intact and the browser fingerprint does not change, it is difficult for the user and the financial institution to spot any injected modifications.

For more details on how webinjects work, read our whitepaper: The state of financial Trojans 2014

Redirect attacks

Redirection attacks are not new, in fact they are just evolved phishing attacks and have been around longer than MitB attacks. However, last year we observed an increase in the use of redirect attacks to defraud victims, for example with the Dyre Trojan. The concept is simple: the attacker uses the malware to redirect network traffic to a server controlled by them. Some malware uses a webinject for the redirection; others set a local proxy, manipulate the local DNS resolution, or set a new DNS server altogether. Redirection attacks of old used JavaScript injects, which were loaded from a remote site, to display remote dynamic content inside the empty frame of the banking session.

To make the deception even more credible, the Trojan can install a rogue CA root certificate to spoof all required SSL certificates. Hence, the user won't be alerted by a missing padlock icon in the browser address bar, and verifying the fingerprint of a certificate is not a practical solution for most users. The attacker then waits until the victim logs into the desired online service. Depending on the authentication scheme deployed by the financial service, the attacker can steal the credentials for later use and redirect the user to the original site, act as a completely transparent proxy and modify any transactions that take place, or using a fake copy of the bank website, extract as much data from the user as needed to create a new session and conduct fraudulent transactions in the background.

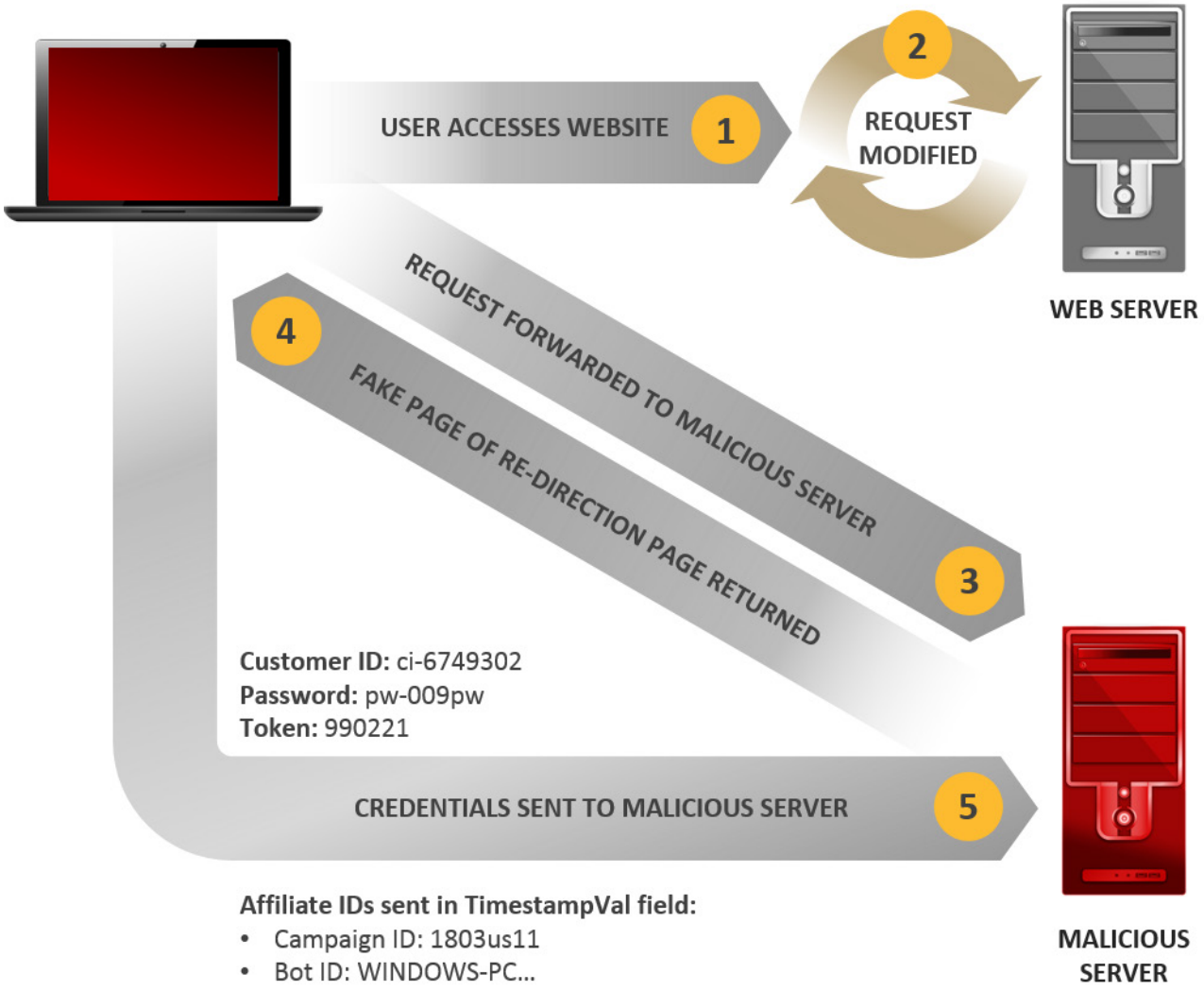


Figure 7. Dyre Trojan redirecting victim to a fake page

The advantage of this method for the attacker is that they can remove the malware from the compromised computer once the redirection is in place. This makes it very difficult to detect the local infection. This approach also makes it easier for the attacker to adjust the logic behind the web modifications when a bank changes its web presence. Fortunately, on the other hand, it does make it simpler for the financial organization to detect the attack, as there will be clusters of suspicious transaction all coming from a few IP addresses with a different browser fingerprint. Furthermore, once the malicious proxy is taken offline, the Trojan will not be able to operate on its own.

Additional payloads

Most of the financial Trojans contain functionality to log keystrokes, take screenshots, and upload and download files. Besides these typical features, they may also have additional capabilities that go beyond defrauding online banking customers. The groups behind these threats have been branching out in order to gather other credentials that could yield a profit; such as account credentials for media streaming services, which can be sold on underground forums; or career and HR related website credentials, which have been a focus for Dyre attacks. As well as this, other threats can also be downloaded by the attackers. Such additional activity, however, raises the risk of the malware being detected and removed from the computer. Dyre, for example, has been seen downloading additional malware to infected computers; in most cases it was a spam bot that helped propagate

the threat further.

We have observed that some groups will wait for a given period of time for the victim to conduct online banking. If such a session does not occur within this time, they will download additional threats, such as Cryptolocker malware, in order to make a profit from the infected computer. Selling compromised systems to a botnet is another method to gain a minimal profit from each infection.

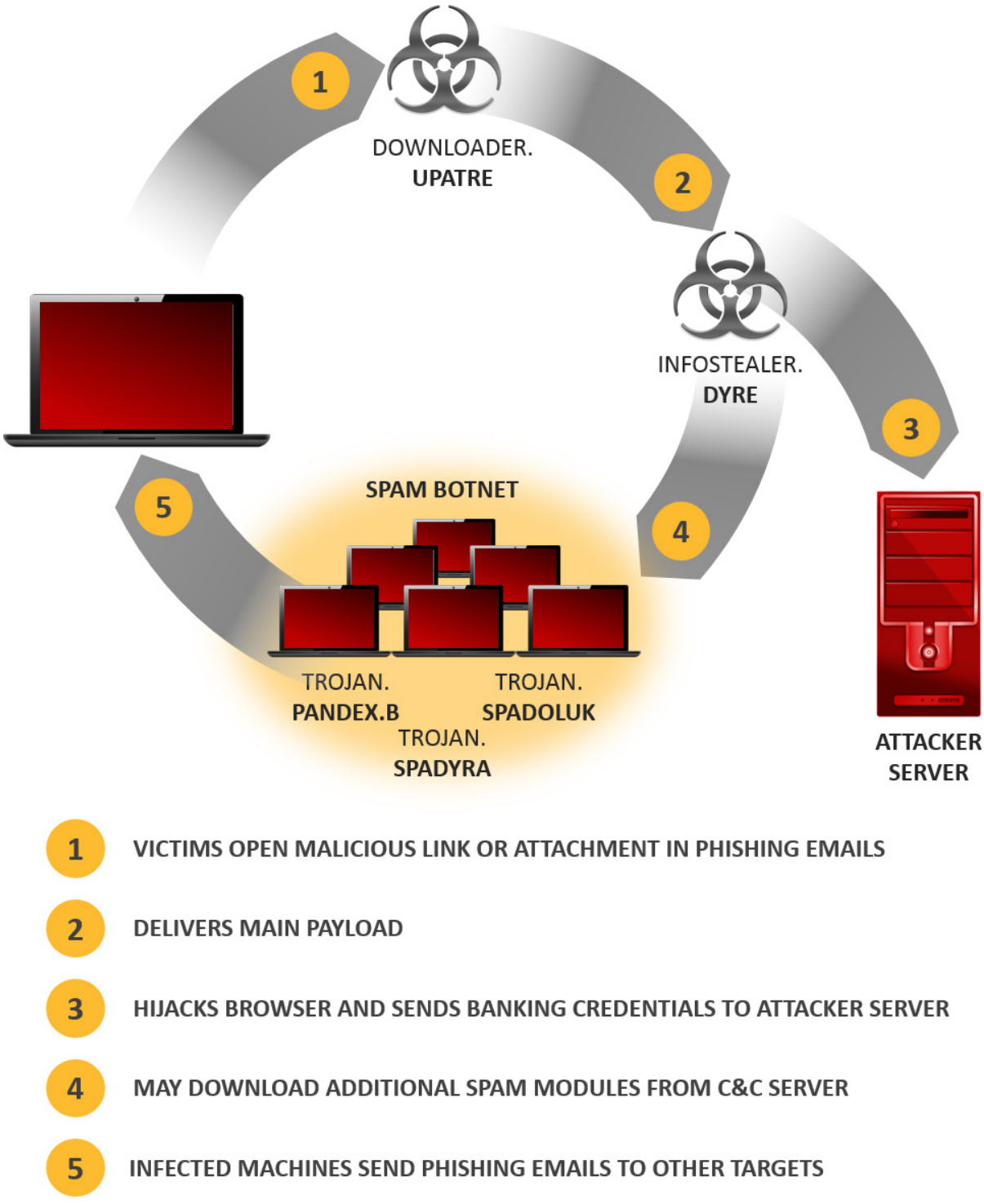


Figure 8. Dyre attack chain

INFECTION VECTORS

> “The infection vector chosen by the attackers depends on the strategy they pursue.”

Infection vectors

The infection vector chosen by the attackers depends on the strategy they pursue. Some groups follow a broad stroke approach, infecting as many computers as possible in the hope that some of those infections will be victims they can make a profit from. Other groups are more focused in the distribution of their malware, attempting to only target people who are users of the financial services the criminals are targeting. There are pros and cons to each approach; such as smaller management overhead for a focused distribution approach; and higher efficacy, albeit with more attention from law enforcement, for a wide distribution approach.

In general, the infection vectors used by financial fraud Trojans are the same four common methods that we see used by any other malware: spear phishing, drive-by downloads, social engineering and, to some extent, supply chain attacks.

Malicious emails

Malicious email is still the most popular way to distribute financial malware. Although well known, plenty of people still get their computers infected through this method. Attachment names like “invoice.pdf.exe” are often used as bait and have a remarkably high success rate. The emails either contain a malicious attachment, a link to a malicious file hosted externally, or a link to a phishing site that can act as a redirection attack.

A good example to illustrate the immense size of such spam campaigns is Dridex, which is almost exclusively distributed through spam emails. Symantec observes multiple Dridex spam campaigns each day, except on weekends. The average number of emails blocked by Symantec per campaign over a 10-week monitoring period in 2015 was 271,019. The largest campaign seen by Symantec resulted in 982,832 emails being blocked.

The vast majority of Dridex spam campaigns involved emails disguised as some sort of financial statement, such as an invoice. Aside from financial data, the only other frequently observed theme was emails purporting to contain scanned documents (usually claiming to be sent by a network connected scanner).

Figure 9. Dridex spam email containing contradictory information about who the sender is

The trend of using Office documents containing malicious macros that emerged in 2014 has

continued in 2015 and was heavily used by Dridex and Infostealer.Shifu. In these attacks, the user has to be convinced to manually enable and run the macro, which will then drop a VBS script that in turn downloads the final malware. Symantec detects these malicious attachments as W97M.Downloader. This fact also highlights another trend that we have noticed. It has become common to use a small dropper malware first, before the final Trojan is deployed. Other threats started to use JavaScript or Batch files as dropper malware.

The rate of phishing emails, which try to lure the user into revealing their credentials on a fake website, declined further in 2015 to 1 in 2,703 emails in December. This type of attack does not usually work well against financial institutions' 2FA mechanisms.

Drive-by download sites

The use of web attack exploit toolkits to infect visitors of websites has been widely used by cybercriminals in the last few years and this activity is still growing. These web attack frameworks are constantly updated to include new exploits for recent vulnerabilities in browsers and third-party plug-ins. Symantec blocked on average more than 1 million web attacks per day in 2015, almost double the amount blocked in 2014. The installed payloads vary, but financial fraud malware and ransomware are among the most common.

Social engineering

Social engineering as a component of the infection process is common, be it a convincing email or a distracting pop-up message. In social networks especially we frequently encounter attacks that try to use sensational messages to trick the user into visiting a link in a post. Once the user falls for the bait, a redirection will lead to a prompt to install an update for a video plugin or some other software. There is, however, no update and the victim is actually installing malware. In this case, since the threat is downloaded and installed by the user without the help of any exploits, it may bypass some browser protection technologies.

Supply chain hack

Supply chain attacks have become an increasingly popular method for targeted attacks in the past few years and have gained some popularity with cybercriminals as well. The method involves the attackers breaching a vendor's website and replacing a software update with a Trojanized package, which later gets downloaded by unknowing victims. Since there are no exploits involved in dropping the malware onto the user's system, and the domain accessed is trusted, the download is often executed without a second thought.

Symantec

TARGETED ATTACKS AGAINST FINANCIAL INSTITUTIONS

> “The financial sector was the highest targeted sector in January 2016 with 40.2 percent of all spear-phishing attacks.”

Targeted attacks against financial institutions

As predicted in our previous report, we have seen an increase in attacks directed against financial institutions themselves. Although such targets are harder to compromise than a home user's computer, if the attack is successful it can potentially yield much higher profits with larger transaction values. The financial sector was the highest targeted sector in January 2016 with 40.2 percent of all spear-phishing attacks. This underlines the high level of interest from attackers to infiltrate financial institutions and profit from the large numbers of financial transactions that flow through them.

The Carbanak cybercrime group, which made headlines in February 2015, is a perfect example of a financial threat that is not just focusing on users of online banking services. This is a skilled group of attackers, capable of gaining a foothold on the networks of targeted banks through malware hidden in spear-phishing emails. Once inside, the group patiently and stealthily move across the network of a bank, gathering intelligence and compromising enough computers until it has the resources and intelligence to launch a successful attack. The Carbanak group employed two main tactics to cash out: in some cases, it transferred funds to accounts under its control; and in other instances, it compromised and hijacked ATMs in order to dispense funds to people working for the group. The exact amount stolen by the Carbanak group is unknown but estimates range from tens of millions of US dollars up to $1 billion.

With such a successful attack, it should come as no surprise that we have seen other groups employ similar tactics. One noteworthy attack was carried out in Russia in 2015 by an attack group named Metel. This gang targets computers inside financial institutions that have access to money transaction records, such as customer support machines. Once the group secures access to these computers through lateral movement, they then use their privileges to rollback specific ATM transactions. An accomplice can then drive from ATM to ATM emptying the whole money cassette in each and, thanks to the rollbacks, the account balance remains unchanged.

Another interesting cash out strategy was used by different attackers against an Eastern European financial institution. The attackers tried to manipulate the currency exchange rates. According to a news report, the group successfully infiltrated the financial institution with malware in order to manipulate the exchange rate. The rate between Ruble and Dollar did indeed fluctuate by as much as 15 percent but it is unclear if this was caused by the malware attack. Furthermore, it is unknown if the attackers were able to profit from the attack; however, one bank claims to have lost the equivalent of over 3 million US dollars due to the incident. From the many attacks in the past against virtual currency exchange rates, mostly against Bitcoin, it is evident that attacks against exchange rates can lead to substantial profit for attackers.

The Butterfly group is yet another example of an attack group with a taste for defrauding the financial market. This group compromised various multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and consulting sectors. This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases but is instead focused on high-level corporate information, such as information about acquisitions and unreleased financial records. The Butterfly group may be selling this information to the highest bidder or may be operating as hackers for hire. Another theory is that the stolen information could be used for insider-trading purposes in order to profit on the stock market.

Financial Trojans can also be used for espionage attacks, and has been reported on before. Using a financial scam Trojan in an APT attack is not as absurd as it might seem. Many organizations are used to fighting Zeus and similar Trojans and the detection of such threats may disguise the true objectives of the attackers. This allows the sophisticated attackers to hide in plain sight and still exfiltrate passwords and other information useful for espionage.

Mobile platform

Across all regions we observed an increase in the use of smartphones for online banking services in 2015. Many institutions now offer an Android application as a 2FA token. This expedites the trend of mobile malware further. The most common attack method is to intercept text messages that are part of the 2FA process and forward them to the malware's C&C server to be used by the attacker. As usual with Android malware, the application requests the permissions to receive, write, and send text messages, as well as several other permissions during its installation phase.

In a typical 2FA system, the second factor—normally a generated one-time passcode (OTP)—is sent to the user's registered mobile number through SMS. To improve the security of OTP delivery, some financial organizations have begun delivering OTPs through voice calls instead of SMS. In the last quarter of 2015 we found a new variant of Android.Bankosy, an information stealing Android threat, that is capable of deceiving 2FA systems that use voice calls. The C&C server of the threat can instruct the infected smartphone to forward all calls by using a special service code.

Another class of attacks that has increased is the use of standalone fake bank applications. These can be very convincing for users, such as when mobile malware poses as a legitimate 2FA token app. The most dangerous aspect of this type of malicious app is that it asks the user for their account name and password during the installation phase, gaining all the information needed for the scam to work. This can lead to defrauded bank accounts without the need for an infected desktop computer. In other cases, attackers replace the legitimate and already installed mobile banking software with their own malicious version.

Another Android threat called Android.Fakelogin, uses flexible social-engineering techniques to steal banking credentials from a wide range of users. Rather than disguising itself as a specific app, Android.Fakelogin identifies the banking app that's running on the device and overlays a customized, fraudulent login page over the user interface. It does this by accessing cloud-based logic hosted on a remote C&C server to determine the exact phishing page to display. If the user tries to log in through the fraudulent page, their login credentials will be sent directly to the attackers' C&C server. Although the malware targets legitimate apps available on Google Play, the apps that download Fakelogin are not available on Google Play.

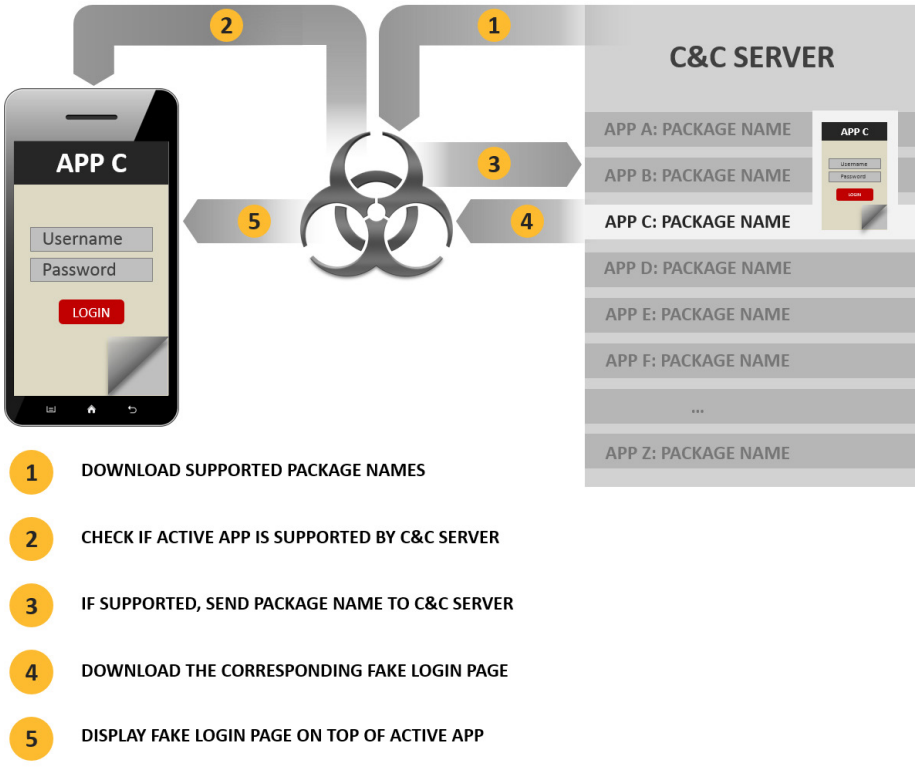


Figure 10. Android.Fakelogin steals login credentials from compromised devices by leveraging cloud-based logic from its C&C server

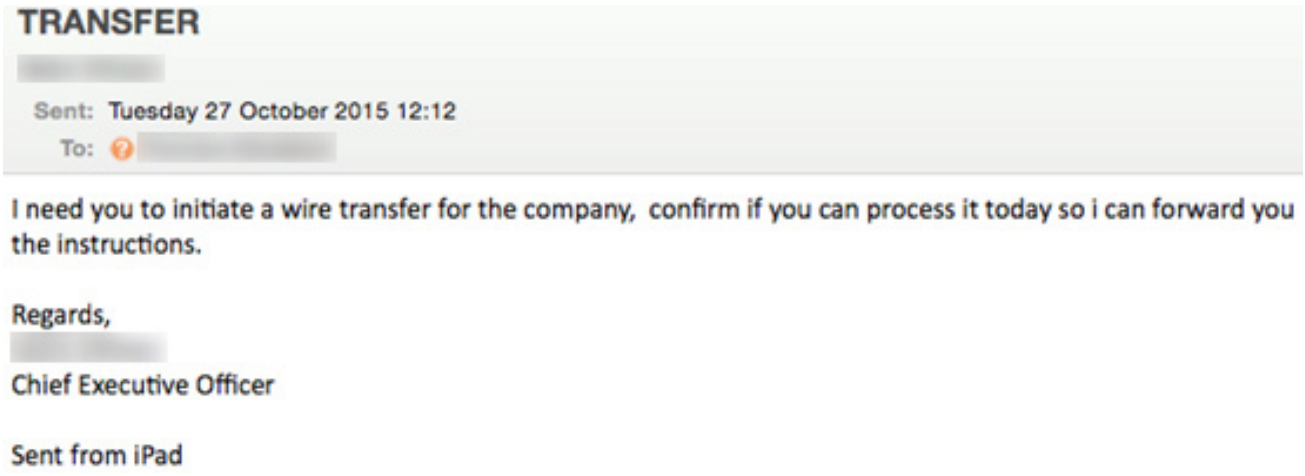
In reaction to increasing threats, newer releases of Android, including KitKat (4.4), Lollipop (5.x), and Marshmallow (6.x), improved the security of Android devices with the introduction of different hardening mechanisms. For example, an app can no longer abort the SMS receive action, making it difficult for a Trojan to steal 2FA SMS codes without the user noticing. Another example

is the depreciation of the getRunningTasks API, which is often used by malware to find the currently active app in order to know when to overly a fake page. This steady series of improvements to Android's security make it increasingly difficult for financial scam apps on smartphones. However, malware authors are trying to adapt as well and there are still a lot of smartphones running older versions of the Android out there. Therefore, it is a certainty that we will have to fight these threats for some time to come.

Business email compromise

In order to maximize their profits and increase the value per transaction many attackers have started to target corporate accounts that often have higher funds at their disposal. Besides attacking the corporate branch of online banking services, the attackers go after the corporate clients directly. With so called business email comprise (BEC) scams, sometimes also referred to as whaling, the attackers try to infiltrate high ranking employees at the target company. There are two variants of this type of attack: with and without the help of malware.

In the variant of the attack that doesn't use malware, the scammers target senior financial staff at medium and large corporations, attempting to trick them into carrying out large wire transfer payments. The attack is simple and straight forward. The scammers send the first email, asking the CFO if they can carry out an urgent wire transfer. If the recipient responds positively, the attackers send a follow-up email with the necessary details for the wire transfer. If there is no response, the scammers may send a second email to the CFO or they may try to target another member of the finance department. Information about these individuals can be easily gleaned from social networks. A cover story, such as a secret acquisition, is often used to ensure the victim doesn't talk with others about the transaction and to build up a sense of urgency to issue the transaction as soon as possible. The credibility of the attacker can be boosted by using publicly available information. We have even noticed scammers registering similar looking domain names to the targeted firm, as well as scammers breaking into the organization's mail server in order to learn the email writing style of individuals they are spoofing. Others successfully compromised VoIP systems in order to call targeted staff members or provide an internal number for call backs.


TRANSFER

Sent: Tuesday 27 October 2015 12:12

To:

I need you to initiate a wire transfer for the company, confirm if you can process it today so i can forward you the instructions.

Regards,

Chief Executive Officer

Sent from iPad

Figure 11. Example of a wire transfer scam email

A variation of the same BEC scam is commonly used against industrial companies. Here, the attacker poses as a supplier and informs the company that the bank account details for their invoices have changed. If the deception is successful, the company will send the outstanding balance for the invoices to the new account controlled by the attacker.

This scam usually does not involve malware and relies heavily on social engineering. For the bank such a

transaction is difficult to spot since it is conducted from the legitimate account with non-stolen credentials. Even if the bank representative calls the issuer of the transaction for confirmation they will confirm it due to the social engineering cover story.

Symantec has also observed attackers compromising targets with remote administration Trojans (RATs). Once a computer is compromised, the attackers spend time assessing it to find out the best way to steal money. In some cases, attackers have even been known to download user manuals to help figure out how to use certain financial software. The goal is to transfer money to an account under the attackers' control. If this isn't possible with the privileges that they obtain the attackers can still send emails from the compromised accounts, conducting a BEC scam with just social engineering.

The FBI has warned users about BEC scams and estimates the losses caused by this emerging trend to be millions of US dollars per month. As an example, there have been reports about an Austrian aerospace company that appears to have fallen for a BEC scam attack in 2015. According to an ongoing investigation, the scammer managed to have the equivalent of over US$55 million transferred to various accounts under the attacker's control.

Takedowns

Over the last few years the collaboration of different law enforcement entities and private sector companies has increased and resulted in a number of significant takedown operations against larger botnets, such as Simda, Changeup, and Ramnit, as well as some financial Trojan botnets. Besides the disruption of the botnet infrastructure, some malware authors have also been arrested and charged.

The cybercrime group controlling the Dyre Trojan appears to have suffered a major blow following a Russian law enforcement operation in November 2015. Dyre is primarily spread through email spam campaigns containing the Upatre downloader (Downloader.Upatre), which will download the Dyre Trojan to the compromised computer. The Dyre group had been running email campaigns during most weekdays, dispatching up to 15 separate email campaigns per day. However, Dyre-related spam campaigns halted abruptly on November 18, 2015, indicating a major disruption in the group's operations.

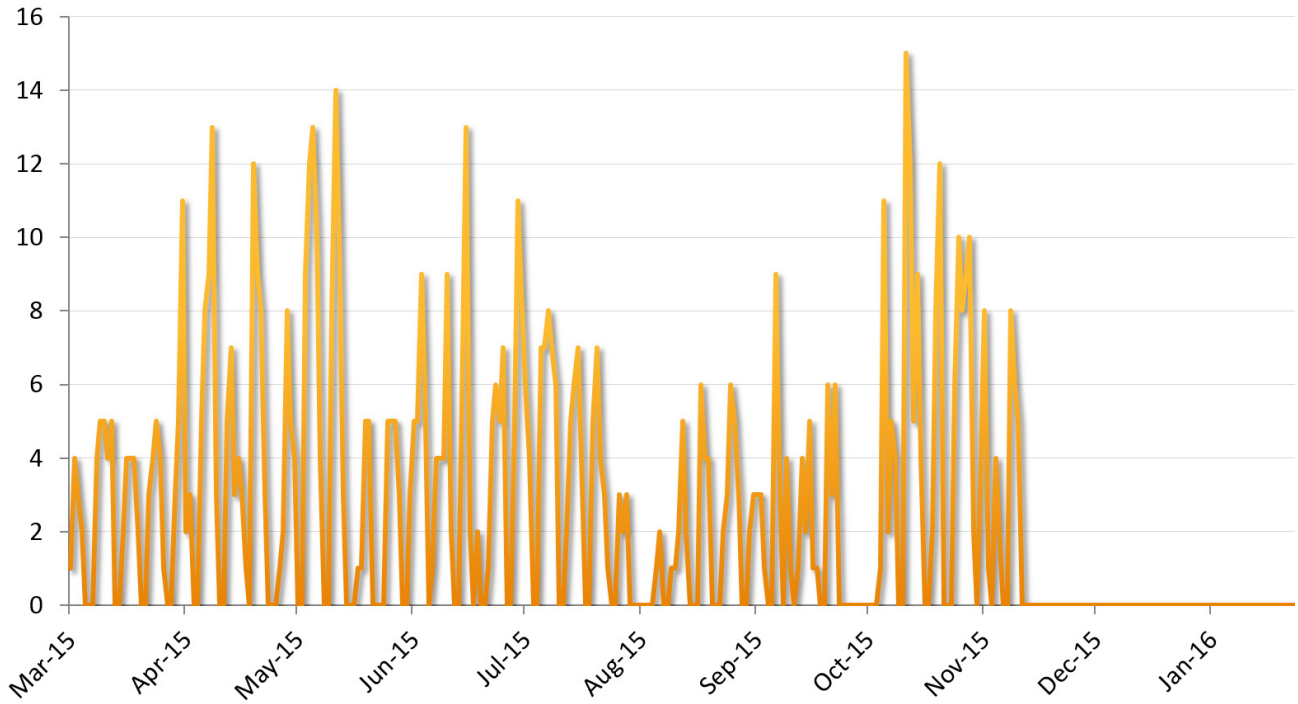


Figure 12. Dyre-related spam campaigns per day from March 2015 onwards—activity ceases on November 18, 2015

Upatre collects information about the victim's computer, attempts to disable security software, then finally downloads and installs the Dyre Trojan. The Dyre group has been one of the main users of Upatre over the past year. Symantec telemetry indicates a huge fall in the number of Upatre infections since November, which coincides with a drop in Dyre detections. The monthly infection rate for Upatre has fallen below 20,000, after reaching a high of more than 250,000 in July 2015.

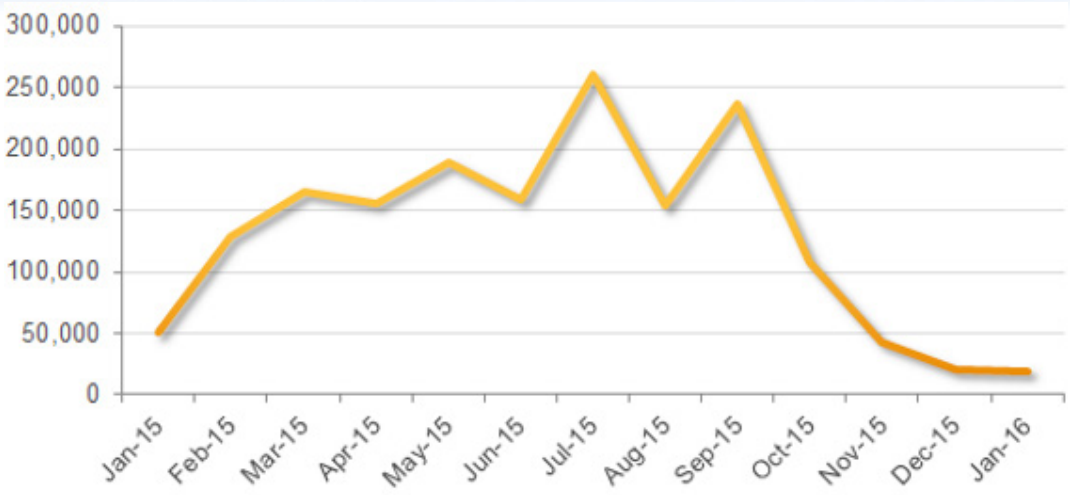


Figure 13. Upatre infections since January 2015, showing a massive fall in late 2015

There is much debate about how effective such take down operations are in the long term. The move against Dyre appears to be one of the more successful of a number of recent takedown operations against financial fraud threats. Unless all of the key figures are arrested and major infrastructure seized, cybercrime groups can quickly rebuild their operations in the aftermath of a law enforcement swoop.

Unfortunately, a long lasting effect is not always achieved. For example, in October 2015 an operation against Dridex seems to have had a limited impact on its operations. While one man was charged and thousands of compromised computers were sinkholed, the rate of Dridex/Cridex infections did not abate much following the takedown.

Fighting the threat of botnets is no easy task, as it is difficult to eradicate a botnet completely. Whenever there is a takedown operation, other attackers can come back with a newer version and fill the gap. After all, the cybercriminals are making millions in profits so they have strong motivation for continuing their financial fraud activities. Symantec continues to collaborate with law enforcement—for example we recently signed a MoU with Europol—in an effort to stop cybercriminals in their tracks and make the internet a safer place for everyone.

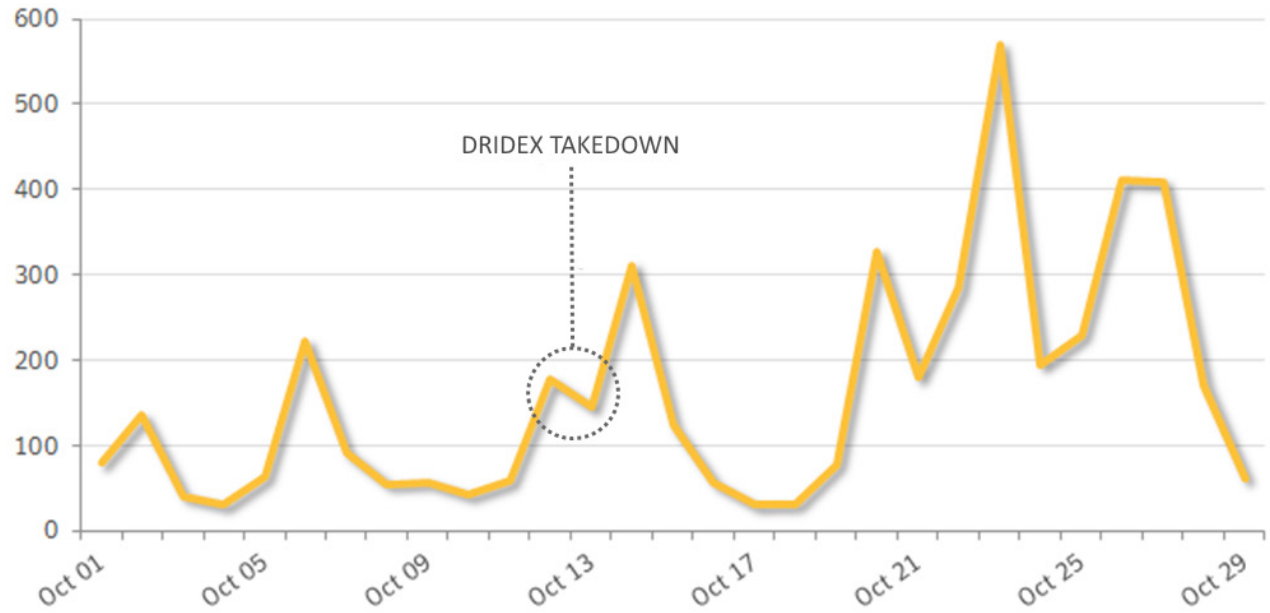


Figure 14. Takedown operation during October 2015 had little impact on Dridex infections

Symantec™

PROTECTION

“The end user still remains the weakest link in the chain during an online transaction”

Protection

Symantec and Norton customers are protected against financial Trojans through our multilayered security approach.

- Antivirus and Intrusion Prevention System (IPS) detections are in place for each of the discussed threat families
- Browser protection can protect against web based attacks that use exploits
- Norton Safeweb blocks users from visiting malicious websites
- Insight can proactively block files associated with financial Trojans and detects them as WS.Reputation.1
- Behavior-based detection blocks suspicious processes using the SONAR series of detections
- Email-filtering services such as Symantec Email Security.cloud can block emails associated with these attacks before they can reach users
- Symantec Messaging Gateway's Disarm technology can also protect computers from many email borne attacks by removing the malicious content from the attached documents before they even reach the user
- Symantec's Advanced Threat Protection solution allows customers to uncover attacks that would otherwise evade detection
- Symantec's Cyber Security Services can help organizations achieve a higher level of security with our leading cyber threat experts for global threat and adversary intelligence, advanced threat monitoring, cyber readiness, and incident response

In addition, users should adhere to the following advice to ensure the best possible security:

- Exercise caution when receiving unsolicited, unexpected, or suspicious emails or phone calls
- Keep security software and operating systems up to date
- Enable advanced account security features, such as 2FA, if available
- Use strong passwords for all your accounts
- Always log out of your session when done
- Enable account login notification if available
- Monitor your bank statements regularly for suspicious activity
- Notify your financial institution of any strange behavior while using their service
- Exercise caution when conducting online banking sessions, in particular if the behavior or appearance of your bank's website changes
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- Establish enhanced authorization business processes for transactions to avoid falling for BEC scams

Conclusion

As in previous years, the financial Trojan ecosystem is still thriving and is a profitable endeavor for cybercriminals. However, the number of detections of financial Trojans has decreased by 73 percent in 2015. It's difficult to know the exact reasons behind this drop. It's most likely a combination of several different factors. Some arrests and takedown operations in 2015 successfully disrupted some of the infrastructure behind these threats. Furthermore, some groups have moved to attack the financial institutions directly, or branched off to favor other schemes like BEC scams or ransomware. In addition to this, security software has improved further and is able to more proactively block the Trojans before they are dropped onto the computer.

In 2015, email was the most prevalent distribution method for financial Trojans. Also popular were Office document attachments with malicious macros that, once enabled by the user, download malware. It has also become common to use a small dropper malware, such as Upatre, to establish an initial foothold on the computer before downloading the final malware. The successful detection of the dropper malware diminishes

the infection numbers for the corresponding financial Trojan.

MitB attacks with webinjects are still the preferred method for attackers to manipulate transactions and steal credentials, but we have seen some groups increasingly use redirection attacks. In redirection attacks, the Trojan will redirect the victim to the phishing server where a fake site steals passwords or acts as a transparent proxy and modifies transactions.

The average number of targeted organizations per sample increased by 232 percent to 93 in 2015 as most financial Trojans broadened their reach in an attempt to increase the efficacy of defrauding victims.

USA was, for the third consecutive year, the country with the most detections of financial Trojans, followed by Germany and India. Some Trojans shifted their focus to new regions like Japan, which was targeted by many new threat families, such as Infostealer.Shifu.

Having said all this, the techniques deployed by the attackers did not change much in 2015. The end user still remains the weakest link in the chain during an online transaction; even the strongest technologies are susceptible to social engineering attacks. Institutions need to be open about these risks and continue to educate their customers about security issues they may encounter. Until adequate protections become ubiquitous, cybercriminals will continue to defraud institutions and their customers out of millions of dollars annually.

Author

Candid Wueest
Princ Software Engineer

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/social/.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com