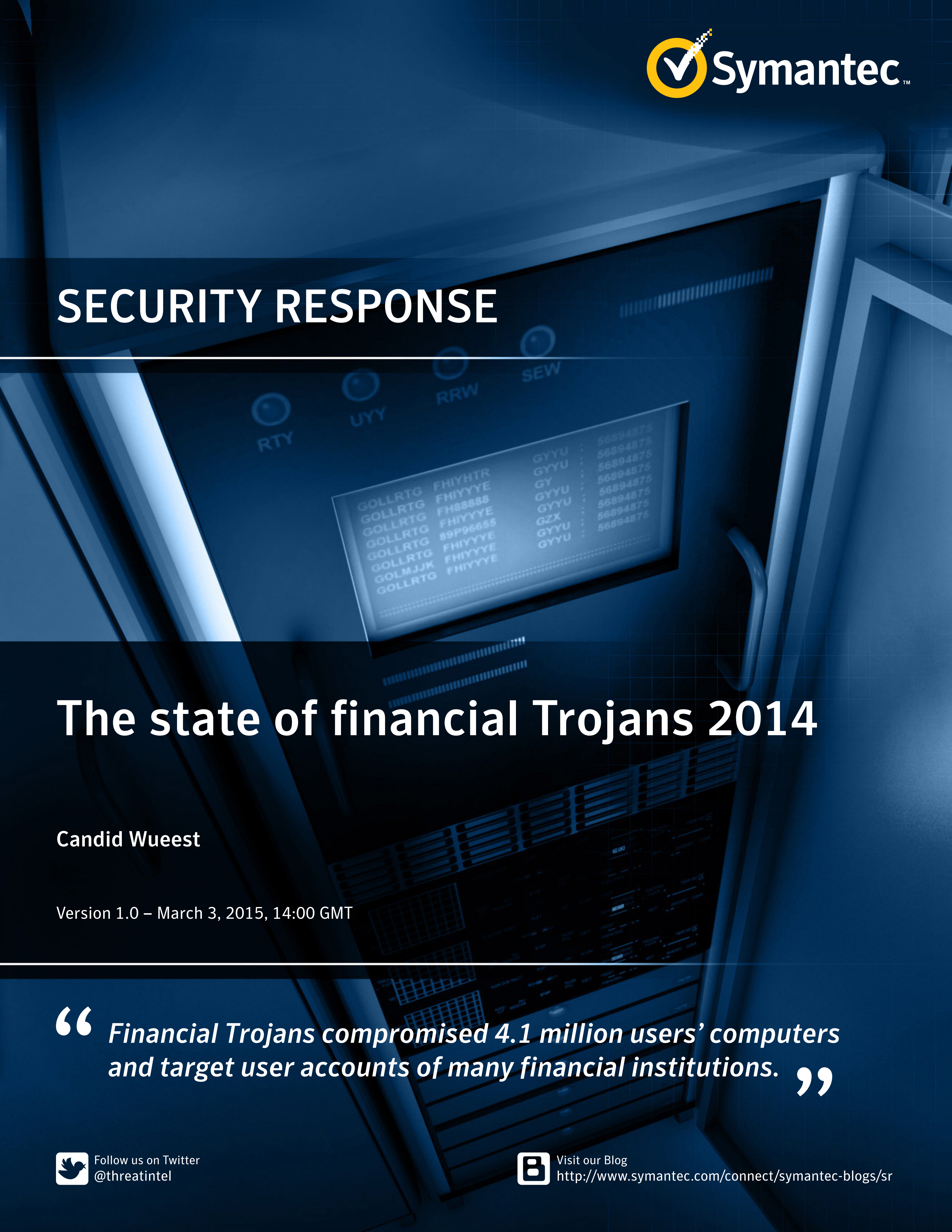


SECURITY RESPONSE

The state of financial Trojans 2014

Candid Wueest

Version 1.0 – March 3, 2015, 14:00 GMT

> *Financial Trojans compromised 4.1 million users' computers and target user accounts of many financial institutions.*

Follow us on Twitter
@threatintel

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

CONTENTS

OVERVIEW

Financial institutions have been fighting malware targeting online banking for over a decade. Attackers have evolved their techniques over the years to try and circumvent new security measures like two-factor authentication (2FA) or mobile banking. Financial institutions had to adapt their security policies to protect online transactions from fraud conducted by cybercriminals using sophisticated banking Trojans.

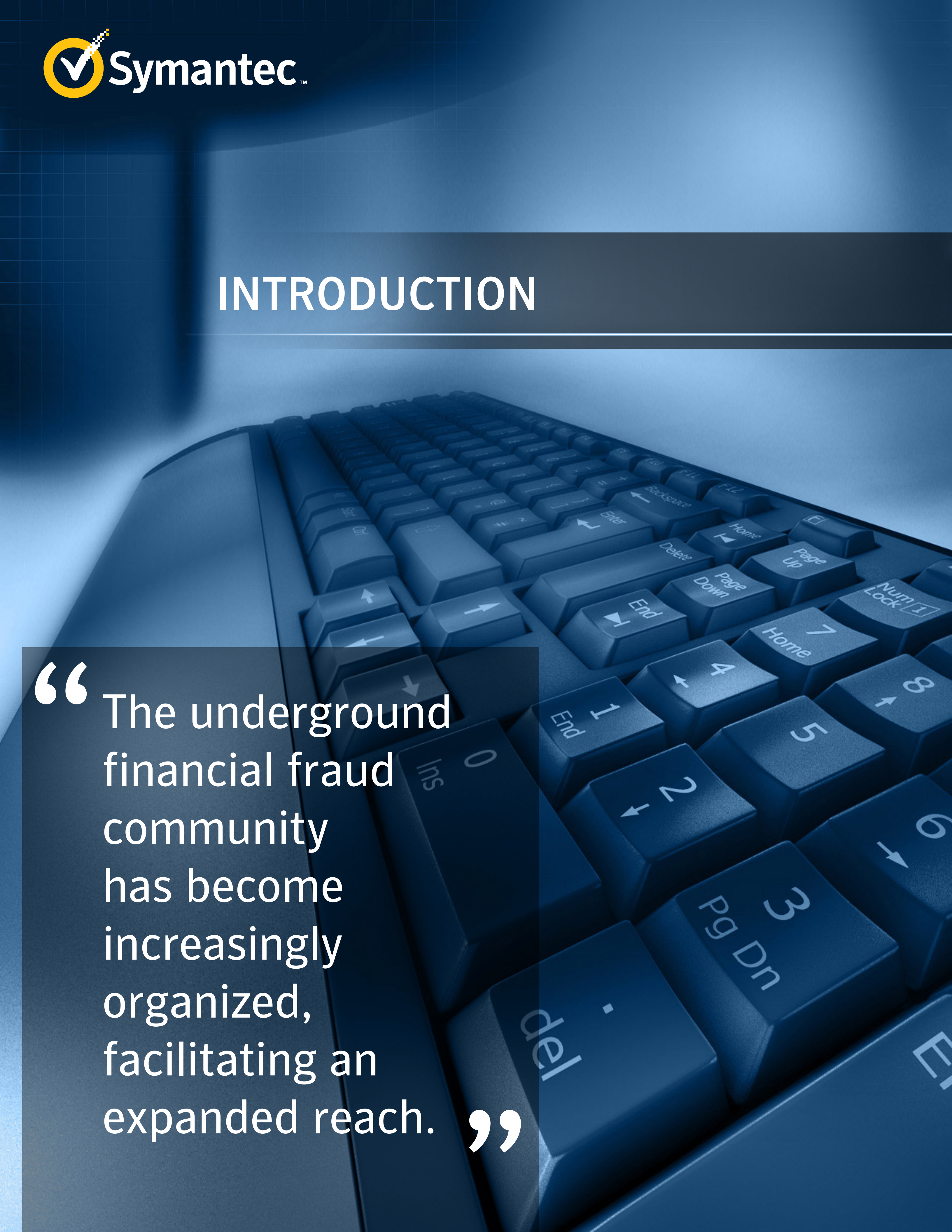
Despite these efforts, many security implementations are ineffective at protecting against modern banking Trojans. Although the attack methods have not changed drastically over the last year and still mainly rely on social engineering and man-in-the-middle browser manipulation through web injects, they are often still successful. Cybercriminals are motivated by financial reward and are using these advanced Trojans to commit large scale financial fraud, targeting institutions across the globe.

This report is an update to the 2014 edition and examines nine of the most common and sophisticated financial Trojans. These Trojans compromised 4.1 million users' computers and target user accounts of many financial institutions. Analysis of the configuration files for these Trojans revealed that customers of 1,467 institutions are being targeted. Nearly 95 percent of these organizations belong to the financial sector, spanning a broad range of institutions. Some attackers also went after special targets such as the Brazilian payment system Boleto or cryptocurrencies like Bitcoin. These figures don't mean that cybercriminals are stealing everything from the affected accounts unhindered, but the attackers are still trying to bypass any online security hurdle deployed by each of these financial institutions. The exact details of the techniques used against specific financial institutions are withheld, but are available to the financial institution by request.

As many banks are adopting stronger security implementations, attackers have shifted focus onto the institutions with weaker account security. For example, as predicted in last year's report, we have seen a spike in attacks targeting Asia in 2014.

As financial institutions assess the threat of modern financial Trojans, the adoption of adequate security measures will undoubtedly increase. Providing a secure environment where customers can confidently authorize transactions is essential.

INTRODUCTION



> "The underground financial fraud community has become increasingly organized, facilitating an expanded reach."

Key findings

- Around 1,467 financial institutions in 86 countries are targeted with financial Trojans.
- The top nine targeted financial institutions were attacked with more than 40 percent of the Trojans.
- The most targeted financial institution is located in the US and was attacked with 95 percent of all analyzed Trojans.
- Attackers are focusing on new targets outside of online banking, such as Boleto, Bitcoin, and password managers.
- The number of financial Trojans has dropped by 53 percent in 2014.
- Traditional phishing email rates have dropped by 74 percent in 2014.
- The number of infections of Zeus (Trojan.Zbot) and its variants grew by ten times from 2012 to 2014.
- Cridex (W32.Cridex) infections decreased by 88 percent and Spyeye (Trojan.Spyeye) infections dropped by 87 percent from 2012 to 2014.
- The US is the country with the most financial Trojan infections, followed by the UK and Germany.
- Stolen bank accounts are sold for 5-10 percent of the balance value on underground cybercrime forums.

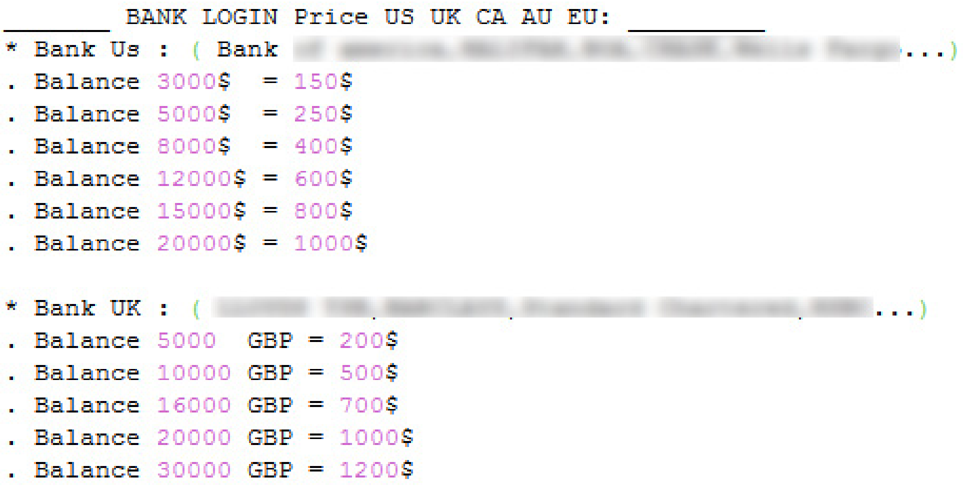
Introduction

Trojans targeting financial institutions have become one of the most prevalent threats on the internet today. A successful compromise of an online bank account can be very profitable for the attacker. Some financial threat families are constantly being updated and adapted to thwart newer protection methods, and enjoy great popularity among cybercriminals.

(For more details around the history of financial Trojans and the observed evolution of their techniques, have a look at the last year's version of our whitepaper.)

The underground financial fraud community has become increasingly organized, facilitating an expanded reach. Everything from bots and intelligent configurations to localized distribution channels are being bought, sold, or rented out as a service. Attackers are no longer just participating in financial fraud; some are dedicated to creating tools to facilitate these activities. Attackers can leverage third-party services to operate more efficiently and can even outsource the cash-out process. Compromised banking accounts are traded for five to ten percent of their current balance.

As a result of this underground economy, less effort is required to maintain attack infrastructure and Trojan configurations. Attacks that can intelligently target large numbers of institutions concurrently will intensify. Sophisticated cybercriminal groups are already using advanced techniques such as automated transaction services (ATS) and traffic direction services (TDS), and the underground service community is streamlining them further.



```
________ BANK LOGIN Price US UK CA AU EU: __________
* Bank Us : ( Bank [redacted]...)
. Balance 3000$  = 150$
. Balance 5000$  = 250$
. Balance 8000$  = 400$
. Balance 12000$ = 600$
. Balance 15000$ = 800$
. Balance 20000$ = 1000$

* Bank UK : ( [redacted]...)
. Balance 5000  GBP = 200$
. Balance 10000 GBP = 500$
. Balance 16000 GBP = 700$
. Balance 20000 GBP = 1000$
. Balance 30000 GBP = 1200$
```

Figure 1. Advertisement for stolen bank accounts

One of the most widely adapted security measurements in the financial industry is the use of transaction authentication numbers (TAN) and two-factor authentication (2FA) methods. In rare cases, banks use transaction-signing, where the transmitted code is only valid for one specific transaction and cannot be used to authorize another.

One implementation uses out-of-band challenge-response mechanisms that contain a transaction verification step on external chip card readers with displays (chipTAN). Other vendors rely on text messages or mobile apps to provide the TAN to the user. In these cases, organizations send the TAN to their customer as an additional authentication measure on top of their online banking password. The message with the TAN also typically mentions some of the transaction details for verification purposes. Such systems greatly enhance the security of online transactions, compared to static passwords on their own.

A strong security measure is likely to prevent an unsuspecting user from proceeding with a fraudulent transaction on a computer that has been compromised with an advanced financial Trojan. Unfortunately, with convincing social engineering tricks and smartphone malware, many of these strong security measures can nonetheless be circumvented by sophisticated attackers. Customer data could be under greater threat in future, as some banks are having discussions about removing the use of 2FA for smaller transaction to save costs.

Cybercriminals can try many different tricks in order to evade local detection or stop any security product from properly functioning or updating. For example, a recent variant of Trojan.Snifula targeting Japan simply filtered out advertisement banners that banks used to promote the use of antivirus software to protect computers. Other malware tries to tamper with local security products by either preventing them from updating their signatures or completely uninstalling them. Such simple methods can lead to malware not being detected for a long period of time.

Attackers are also experimenting with different command-and-control (C&C) communication methods. For example, in November last year, we saw a wave of Trojan.Bankrif attacks in South Korea that used comments on Pinterest to send commands to infected computers. Other malware used the drafts folder of Gmail to covertly communicate with the compromised computer. Of course, Trojans still frequently employ well established C&C methods such as peer-to-peer (P2P) networks, TOR hidden services, and domain generator algorithms (DGA).

Prevalence

For this research, we concentrated on the nine commonly used financial Trojans (Table1).

With the exception of Infostealer.Dyranges, all of the most prevalent banking threats were from previously known malware families. Dyranges, on the other hand, first appeared in June 2014 and its use has skyrocketed since.

The number of total financial Trojan infections around the world has steadily decreased after a spike in March 2014 and is now at a similar level as the number seen at the end of 2012. This represents a drop of 53 percent from January to December, 2014.

The visible drop could be attributed to various takedown operations and malware author arrests, which were carried out last year. Some attackers switched to new malware families over the year as a result.

Table 1. Number of detections in 2014

Threat	Compromised computers in 2014
Trojan.Zbot and its variants	~4,000,000
Infostealer.Dyranges	~90,000
W32.Cridex	~29,000
Trojan.Snifula	~21,000
Trojan.Bebloh	~11,000
Trojan.Shylock	~9,000
Trojan.Spyeye	~6,700
Trojan.Mebroot	~5,700
Trojan.Carberp	~500

It should also be noted that Symantec uses multiple layers of protection in order to block the malware as early in the infection chain as possible. As a result, we have prevented many users from visiting infected websites and

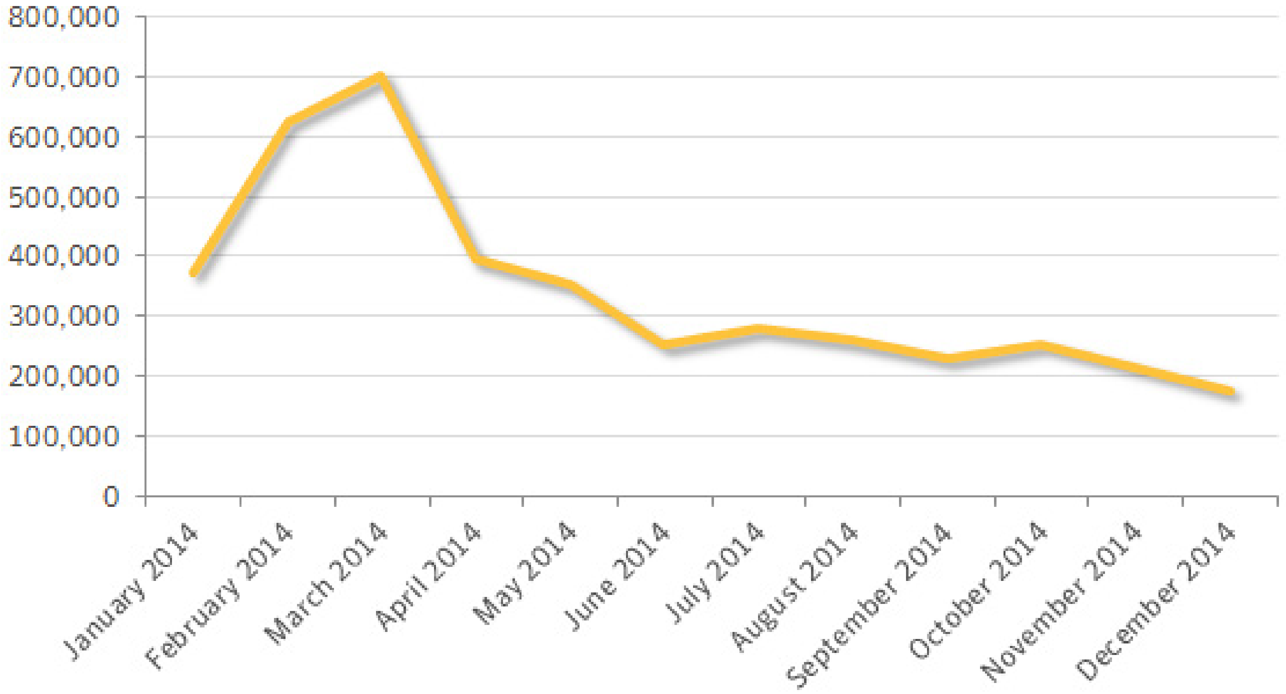


Figure 2. Computers compromised with banking Trojans in 2014

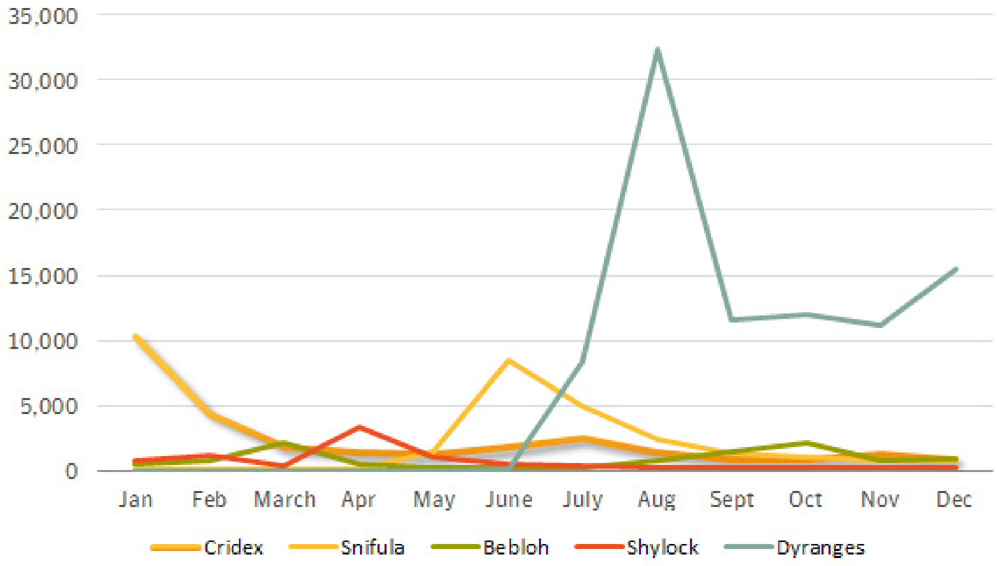


Figure 3. Financial Trojan infections in 2014

stopped many exploit kits from dropping financial Trojans onto the user's computer. For example the number of times that Symantec's products have blocked network access to Angler exploit toolkits increased by three times in the last six month. This ultimately led to fewer file based detections of the Trojans on customers' computers.

Zeus' many variants and offshoots, such as like Gameover and Citadel, are still responsible for the most financial Trojans infections Trojans infections by far. This cluster of families grew from 400,000 detections in 2012 to nearly 4 million in 2014. Other threat infections decreased substantially, including Cridex, which dropped 88 percent, and Spyeye, which decreased by 87 percent from 2012 to 2014.

When looking at the top ten regions with the highest financial Trojan detection rates, the US remained at the top spot between 2013 and 2014. The UK came second in 2014, moving up from third in 2013. Germany came third in 2014, rising from fourth in the previous year.

Between 2013 and 2014, Japan fell from having second highest financial Trojan detection rates to the fourth highest. India moved up from seventh highest in 2013 to fifth highest in 2014 (Table 2).

Table 2. Regions ranked by financial Trojan detection rates

Country	Rank in 2014	Rank in 2013
US	1	1
UK	2	3
Germany	3	4
Japan	4	2
India	5	7

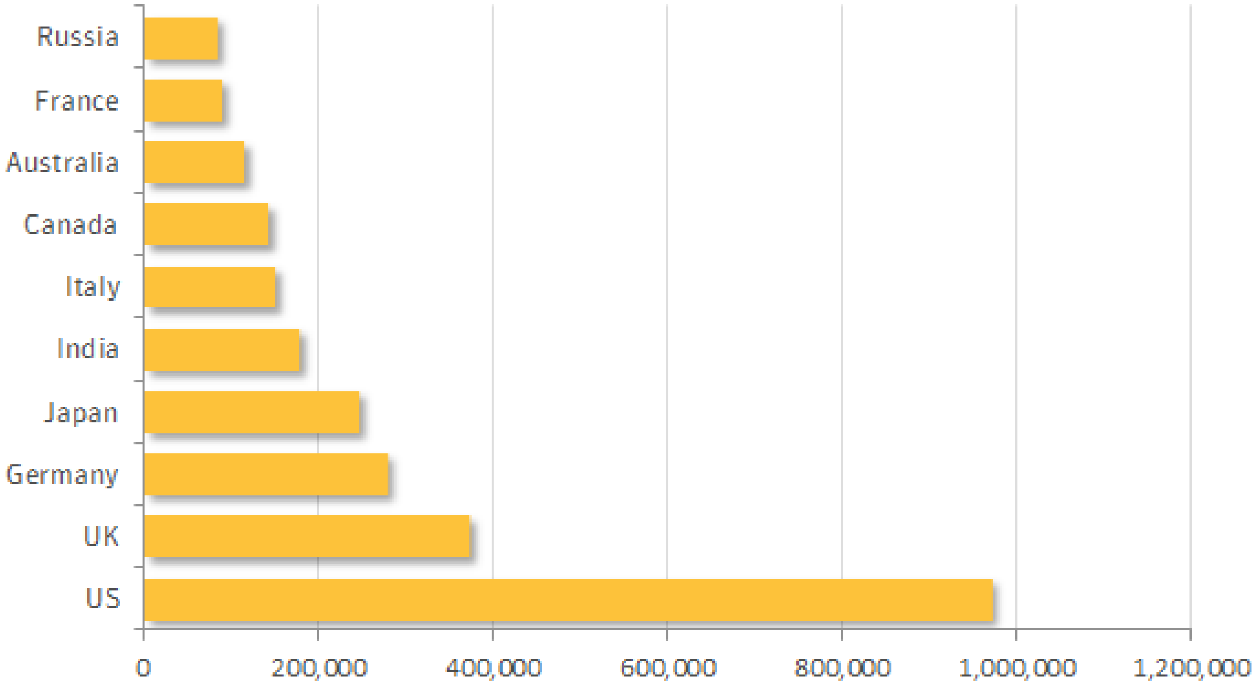


Figure 4. Computers compromised with financial Trojans by country in 2014

TARGETED INSTITUTIONS

> “Nearly every flavor of financial institution is targeted, from commercial banks to credit unions.”

Targeted institutions

Modern banking Trojans typically use an updatable and encrypted configuration file stored in the file system, the registry, or actually embedded in the Trojan itself. Over time, the Trojan's C&C server can push out new configurations if needed. In our analysis, we extracted and analyzed 999 configurations from recent threat samples. According to our research, the configuration files included 1,994 domains belonging to 1,467 distinct institutions. In nearly 95 percent of cases, financial sector institutions were targeted. The remaining five percent were for online services like social media, employment websites, auction houses, and email services.

Nearly every flavor of financial institution is targeted, from commercial banks to credit unions. Traditional banking websites are still the focus of most of the campaigns, but attackers are also exploring different institutions that provide online transactions. Institutions that facilitate high value transactions have been targeted as well as platforms shared by a number of banks and even payroll systems.

One of the Citadel variants indicates that attack groups are trying to expand their target list beyond financial entities. The Citadel malware has been upgraded to target the master password for password manager tools as well. This allows the Trojan to steal the encrypted database of all stored passwords and upload the database together with the master password needed to unlock it. This could potentially lead to the compromise of many other accounts owned by the user.

We have also seen threats that include features to let them target cryptocurrencies like Bitcoin, vouchers and loyalty programs of hotels and retailers, or country-specific payment systems like the Brazilian Boleto Bancário. Attackers have even been observed using financial Trojans for espionage.

Table 3 ranks banks by how frequently financial Trojan configuration files target them. The identities of specific institutions are available to the relevant financial organization by request.

Table 3. Top 25 institutions targeted in configuration files

Rank	Institution	Region	Percentage of configuration files targeting institutions
1	Bank 1	US	94.49%
2	Bank 2	US	46.55%
3	Bank 3	US	46.45%
4	Bank 4	Canada	46.25%
5	Bank 5	US	46.05%
6	Online payment service	US	45.85%
7	Bank 6	UK	44.74%
8	Auction platform	US	43.64%
9	Bank 7	UK	40.44%
10	Bank 8	US	39.84%
11	Bank 9	UK, Spain	38.24%
12	Bank 10	UK, Italy	38.24%
13	Bank 11	UK	38.14%
14	Bank 12	US	38.04%
15	Bank 13	UK	37.84%
16	Bank 14	US	37.64%
17	Bank 15	UK	37.04%
18	Bank 16	US	36.94%
19	Bank 17	UK	36.64%
20	Bank 18	UK	35.84%
21	Bank 19	UK	35.74%
22	Bank 20	US	35.34%
23	Bank 21	France	35.34%
24	Bank 22	UK, Ireland	33.53%
25	Bank 23	Australia	33.53%

The selected institutions to target depend on the

Trojan's configuration file and the attacker's methods. The type and number of targeted institutions vary both within and across financial Trojan families. This variation is particularly evident in publically available Trojans, which are involved in the most diverse set of campaigns conducted by different groups.

Targeted organizations within the configuration files of private and custom-made Trojans vary to a lesser degree, as access to these Trojans is more tightly controlled. This results in a limited number of attackers using these threats to target a smaller set of targeted institutions.

The targets can change over time as attackers move to focus on different countries or banks if they see their campaigns' efficiency rate dropping or fear a law enforcement operation's scrutiny. Different global factors can also influence attackers' decisions, such as spoken languages and regions where international transactions are more difficult to conduct and require local steps to launder the money.

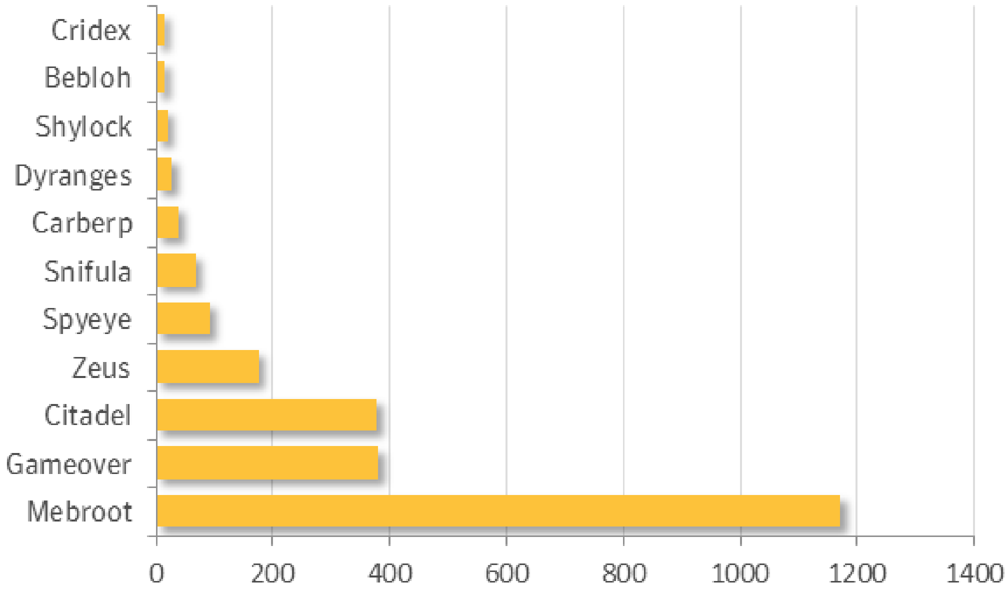


Figure 5. Number of institutions targeted by each Trojan

For example, Trojan.Snifula, which had a spike of activity in Japan in mid-2014, grew over the summer from targeting eight organizations to attacking 37 different financial institutions. This includes 12 smaller regional banks in Japan, indicating that the attackers tried to expand their operational scope to other niche organizations beyond the big players.

Man-in-the-browser (MITB) attacks

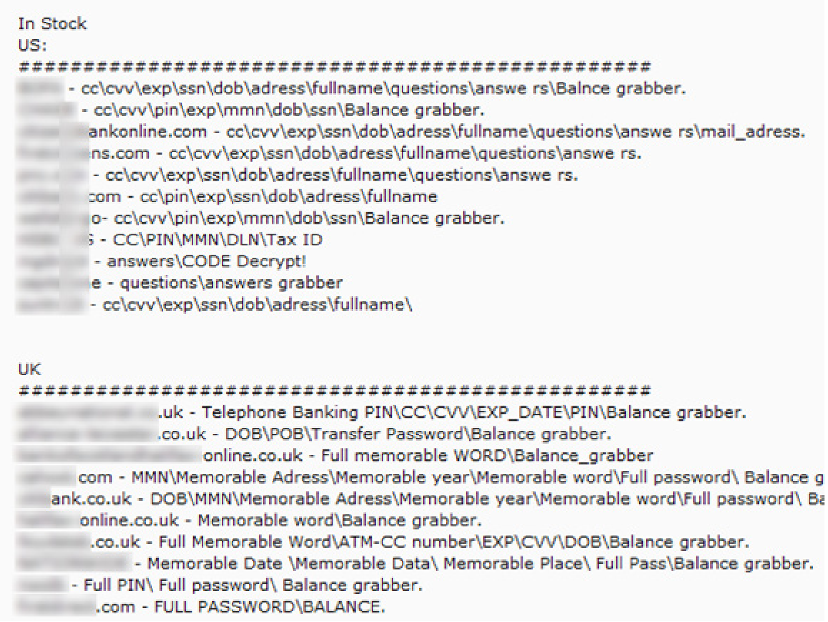
Since most major financial institutions facilitate online banking through a standard web browser, it is not surprising that modern banking Trojans are targeting this software. Man-in-the-browser (also known as web injects) is the most commonly used attack technique in financial Trojans. In MITB attacks, the malware hooks into the browser and manipulates data before it is displayed to the user or sent to the network. This can be done by hooking various APIs or by using browser extensions that can manipulate the Document Object Model (DOM) structure. As the MITB attack happens at the presentation layer, there are no obvious indications of malicious activity. The domain is legitimate and the security certificate has not been tampered with, which all adds credibility to the attackers' requests and can end up fooling the user. The victim's data is also intercepted before it is encrypted through Secure Sockets Layer (SSL).

A web inject could display a legitimate-looking popup message, advising the user to wait due to website maintenance. This gives the attacker time to clear out the account in the background. More complex web inject scripts are capable of dynamically loading important data for the attackers, such as the percentage of the account's money to steal to avoid attention and the destination money mule accounts as listed in the C&C server.

More sophisticated scripts can automatically execute transactions in the background from within the user's authenticated session. Such advanced web injects have to be created individually for every institution being targeted. This has resulted in a growing underground market focused on web inject scripts, which are sold or requested by cybercriminals.

The price tag for a custom web inject is usually less than US$100. The details needed by the script are often very similar over multiple Trojans and can easily be adapted to work with any malware family if the attacker decides to switch to use a different Trojan.

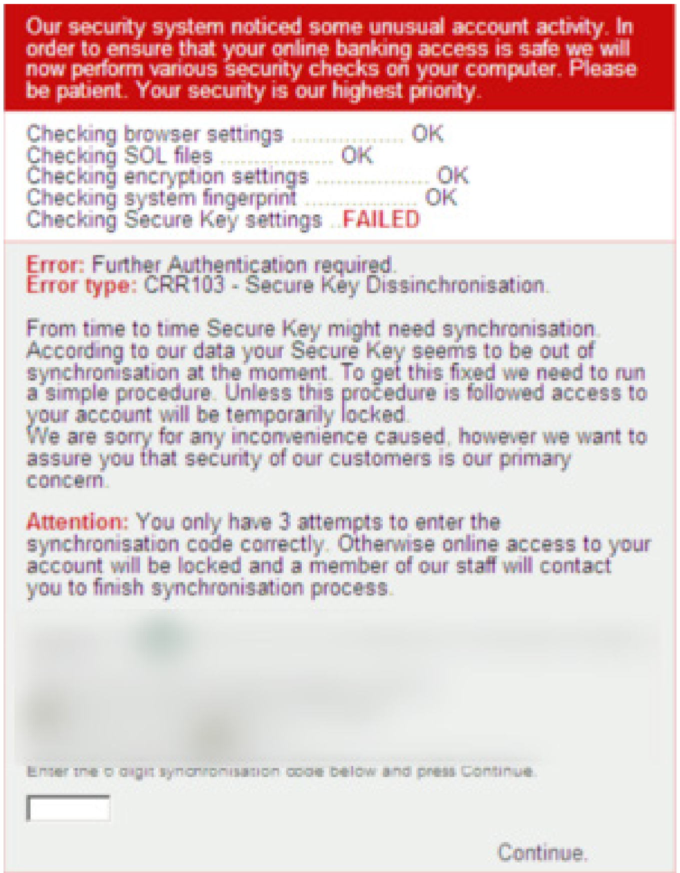
There are a few well known groups and platforms creating web injects, such as Yummba, Injeria, and ATSEngine. The platforms provide their own remote control panel and are linked to in the web inject. This allows the attacker to manage and update the web inject's code through this panel, letting the Trojan access the current version of the web inject script when needed. Web injects also upload the entire HTML code of transaction requests, allowing the attacker to analyze why an automated transfer might not have worked. Other plugins, such as Jabber alerts, help attackers to stay notified of unusual activity.



```
In Stock
US:
####################################################
[redacted] - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs\Balnce grabber.
[redacted] - cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.
[redacted]ankonline.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs\mail_adress.
[redacted]ns.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs.
[redacted] - cc\cvv\exp\ssn\dob\adress\fullname\questions\answe rs.
[redacted]com - cc\pin\exp\ssn\dob\adress\fullname
[redacted]o- cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.
[redacted]S - CC\PIN\MMN\DLN\Tax ID
[redacted] - answers\CODE Decrypt!
[redacted]e - questions\answers grabber
[redacted] - cc\cvv\exp\ssn\dob\adress\fullname\


UK
####################################################
[redacted].uk - Telephone Banking PIN\CC\CVV\EXP_DATE\PIN\Balance grabber.
[redacted].co.uk - DOB\POB\Transfer Password\Balance grabber.
[redacted]online.co.uk - Full memorable WORD\Balance_grabber
[redacted]com - MMN\Memorable Adress\Memorable year\Memorable word\Full password\ Balance g
[redacted]ank.co.uk - DOB\MMN\Memorable Adress\Memorable year\Memorable word\Full password\ Ba
[redacted]online.co.uk - Memorable word\Balance grabber.
[redacted].co.uk - Full Memorable Word\ATM-CC number\EXP\CVV\DOB\Balance grabber.
[redacted] - Memorable Date \Memorable Data\ Memorable Place\ Full Pass\Balance grabber.
[redacted] - Full PIN\ Full password\ Balance grabber.
[redacted].com - FULL PASSWORD\BALANCE.
```

Figure 6. Advertisement for web injects on cybercrime forums



Our security system noticed some unusual account activity. In order to ensure that your online banking access is safe we will now perform various security checks on your computer. Please be patient. Your security is our highest priority.

Checking browser settings .... OK
Checking SQL files .... OK
Checking encryption settings .... OK
Checking system fingerprint .... OK
Checking Secure Key settings ..FAILED

Error: Further Authentication required.
Error type: CRR103 - Secure Key Dissinchronisation.

From time to time Secure Key might need synchronisation. According to our data your Secure Key seems to be out of synchronisation at the moment. To get this fixed we need to run a simple procedure. Unless this procedure is followed access to your account will be temporarily locked.
We are sorry for any inconvenience caused, however we want to assure you that security of our customers is our primary concern.

Attention: You only have 3 attempts to enter the synchronisation code correctly. Otherwise online access to your account will be locked and a member of our staff will contact you to finish synchronisation process.

[redacted]

Enter the 6 digit synchronisation code below and press Continue.

Figure 7. Fake popup message generated by Trojan.Shylock

INFECTION STRATEGIES

> “There are two main approaches that have been observed: broad strokes and focused attacks.”

Infection strategies

The infection vector chosen by the attackers depends on the strategy that they pursue. There are two main approaches that have been observed: broad strokes and focused attacks.

Broad strokes

Attackers can use the broad strokes approach to try to infect as many users as possible. The malware used in this approach involves the use of attack scripts aimed at many different banks in the hope that one of them will fit the user's habits. This is a pure numbers game where the attacker aims to make enough profit from a small percentage of the infected computers.

One of the challenges in this approach is that the attacker needs to keep updating the web injects for many banks. In order to cope with this challenge, some of the attackers work with other groups that offer the service of updating web injects when needed.

Such noisy attacks also raise the attention of the bank, security companies, and law enforcement agencies, so they are often conducted in short bursts against a large amount of targets.

Focused attacks

Focused attacks target a smaller, well-defined set of users, such as a specific area in a country where a regional bank brand might be very popular. The attacks typically begin with spear-phishing or drive-by download sites that only infect victims from a predefined IP address range. Compromised computers that were not used for fraud can be resold to other cybercriminals.

With the advent of location-aware exploit packs and traffic-direction services, localized attacks are easy to launch. This strategy suits attackers with limited resources, but also scales well to larger operations. Using this approach usually takes longer to compromise a large number of victims, but the success rate of finding an ideal victim is higher. Besides this, the attack is less noisy and could run for a longer period of time without attracting too much attention.

One special type of focused attack seeks enterprise accounts. These corporate accounts often have a higher balance and are used to make large transactions. This may allow the attacker to steal high volumes of money in a short time period. For example there is a reported case of a company in Switzerland that was compromised with a financial Trojan sent in a spear-phishing email. The Trojan blocked local access to the computer, giving the attackers time to remotely transfer more than US$1 million to different accounts in Poland and China.

In general, the infection vectors used by financially motivated Trojans are the same four common methods that we see with many other malware campaigns: malicious emails, drive-by download sites, social engineering, and supply-chain attacks.

Infection vectors

Malicious emails

Although sending emails with malicious attachments is one of the oldest attack methods, it is still popular among attackers. With an average of 21 data breaches per month in 2014, there is also no shortage of leaked personal information like names and email addresses, which can be misused for spear-phishing attacks.

Most of the time, the attachments are executable binary files disguised with a double extension in the file name, such as “invoice_2014.pdf.exe”. The emails' content, used to build up the credibility of the message, varies from online shopping invoices to news alerts.

In December 2014, 1 in 195 emails analyzed by Symantec contained a malicious attachment, an increase of 16 percent over the yearly average. Around 14 percent of the emails contained a URL to a malicious site. Classic phishing attacks, where the user is lured to a fake website that tricks them into revealing their credentials, have dropped by 74 percent in 2014. These phishing attacks have not been working against financial institutions for a while and so have been abandoned for this sector, but we still see them used against social networking sites or email services.

Attackers are experimenting with different tactics, such as encrypting malware in a zip archive with a password and then compressing this file once more, hoping to bypass email gateway filters. Other attackers link to websites that display a CAPTCHA before letting the user download the Trojanized invoice. Another method that we observed is how emails with website links are sent out during the night. The page behind the URL is clean and gets switched to a malicious site before morning to try and fool URL scanners.

We even saw a revival of Microsoft Office macros with the latest Cridex variant, referred to as Dridex. This threat has recently been distributed through emails with malicious Word document attachments which download the malware using macros embedded in the document. The emails use the brands of legitimate firms and claim that the attached documents are invoices from these companies. The documents actually contain a VBA macro that downloads the threat onto the user’s computer. Once the malware has compromised the computer, it steals login credentials for online banking sites.

Drive-by download

Attackers have been widely using exploit kits to infect visitors of compromised or malicious websites in the last few years. These frameworks are constantly updated to include new exploits for recently discovered vulnerabilities in browsers and third-party plugins. Symantec blocks more than 500,000 exploit attempts per day on our customers’ computers. These attempts include malvertising, which involves the use of malicious advertisements to redirect users to infected websites.

Social engineering

Social engineering is a component of most attacks that we observe, be it a convincing message in an email or a distracting popup from a web inject. On social networks, we frequently encounter attacks that try to trick the user into visiting a website by including a sensational news headline in the post. Often, the headline claims that the link leads the user to the “most shocking video you have ever seen.”

If the user clicks on the link, they are redirected to another website and are prompted to install an update for a video plugin in order to see the content. However, this “plugin update” is actually a Trojan. Since the user deliberately downloads and installs the threat, the attack may bypass some browser protection technologies.

Supply-chain attack

This method, which has been popular for targeted attacks in the past, has seen an increasing popularity with cybercriminals as well. In supply-chain attacks, attackers compromise a company’s network and Trojanize their software updates, allowing the threat to spread to any computer or device that avails of the update. Since there is no exploit involved in dropping the malware onto the user’s computer and the domain that the update is accessed from is trusted, it is difficult to prevent the threat from being written to disk in the first place. The supply-chain attack approach works well for a focused attack, as the criminals can control who gets compromised.

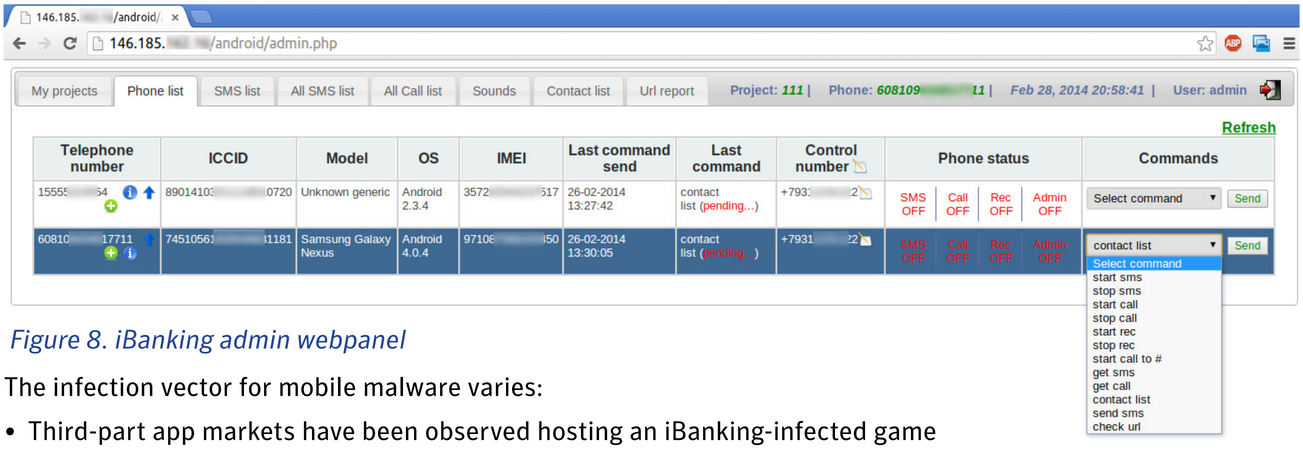
One example of a supply-chain attack is a case where Trojan.Snifula compromised the software update of a computer peripheral company in Japan in order to spread. In 2014, there have been cases where banking Trojans masqueraded as ICS and SCADA software updates.

Mobile platform

The trend of mobile malware intercepting text messages and gathering 2FA credentials continued in 2014. For example, researchers found a pirated version of a popular paid gaming app on a third-party Android market which was infected with Android.Smsstealer. The application requested permission to receive, write and send text messages, and more during its installation phase. Any intercepted messages were then encrypted and sent to the C&C server, allowing the attacker to break into the victim's online bank account.

Another sign that suggests that this method works well was the emergence of the Android.iBanking Trojan. This specialized malware was advertised as having a software-as-a-service business model on underground forums for the high price of US$5,000. The Trojan disguises itself as social networking, banking, or security applications. Android.iBanking initially just stole SMS messages, but now allows attackers to take full control of the smartphone.

In February 2014, Android.iBanking's source code was leaked, resulting in rapid growth of its usage. Despite the availability of a free leaked version, our research suggests that most of the large cybercrime actors are continuing to opt for the paid-for version. They appear to be willing to pay a premium for the updates and support provided by iBanking's author.



146.185.[redacted]/android/admin.php

Project: 111 | Phone: 608109[redacted]11 | Feb 28, 2014 20:58:41 | User: admin

Telephone number	ICCID	Model	OS	IMEI	Last command send	Last command	Control number	Phone status	Commands
15555[redacted]54	89014103[redacted]0720	Unknown generic	Android 2.3.4	3572[redacted]517	26-02-2014 13:27:42	contact list (pending...)	+793[redacted]2	SMS OFF Call OFF Rec OFF Admin OFF	Select command ▾ Send
60810[redacted]17711	74510561[redacted]1181	Samsung Galaxy Nexus	Android 4.0.4	97108[redacted]450	26-02-2014 13:30:05	contact list (pending...)	+7931[redacted]22	SMS OFF Call OFF Rec OFF Admin OFF	contact list ▾ Send

Figure 8. iBanking admin webpanel

The infection vector for mobile malware varies:

- Third-part app markets have been observed hosting an iBanking-infected game
- Malware infecting Windows computers has been seen redirecting the user to the iBanking Trojan and encouraging its installation
- Social engineering emails have been observed disguising the iBanking Trojan as an official-looking 2FA token banking application.

The dangerous part about mobile banking Trojans is that they can ask the user for their account name and password during installation and hand every bit of information needed for the scam to the attacker. This can allow attackers to compromise online bank accounts without having to infect the desktop computer with malware—they would just need the infected mobile phone on its own. In other cases, the attackers replaced the compromised device's already-installed mobile banking software with their own malicious versions.

At the end of last year, two banking malware applications were found on the official Google Play market in Brazil. As industry peers pointed out, the apps were created with a simple app-creation wizard that does not require any coding skills at all. Nevertheless, the resulting phishing apps succeeded in the attacks, as it is still common in Brazil to have static passwords as the only authentication method for online banking, rather than 2FA.

With banks' ongoing trend of moving to the mobile platform, such as developing mobile payment or mobile banking applications, we expect an increased focus of attacks against these devices in the future. Most banks carefully sandbox their mobile application to allow it to defend against local attacks from threats on the smartphone.

Boleto malware in Brazil

Brazil has long been targeted with financial Trojans and we regularly block large spam waves that try to install financial malware onto Brazilian users' computers. Financial mobile malware has also been prevalent in this region.

One of the things that make the Brazilian ecosystem unique is the region's wide use of the Boleto (short for Boleto Bancário) payment system. This is a payment method that allows anyone to create something like a payment slip with a unique account ID and barcode containing all of the payment's required information. These Boleto payment instructions can then be paid easily by anyone from various devices, including mobile phones and computers. All that is required for payment is the ID number or the barcode which contains the necessary information.

Everyone in Brazil is familiar with Boletos, including cybercriminals as there are a handful of different malware families that target the Boleto payment system, such as Infostealer.Boleteiro. Whenever a compromised computer displays a Boleto payment slip in the browser, the Trojan can modify it on the fly, similar to how web injects modify traditional online banking transactions. By overlaying the information with its own payment instructions, the malware can redirect the victim's payment to the attacker instead of the original recipient. In addition, the malware can monitor any form fields in online banking where a Boleto payment ID is entered and then swap it for the attackers ID.

This is another example of how cybercriminals have adapted and are applying traditional techniques to localized payments systems. Even though the Boleto market is localized to Brazil, cybercriminals realized the potential gains by targeting this system. Regardless of where money is transferred online, attackers will try to intercept and redirect it.

Financial attacks in Japan

Japan has experienced a rise in the number of attacks targeting banking customers over the last few years. Japan's law enforcement recorded 1,876 banking Trojan attacks in 2014, up by 43 percent. The loss in savings amounted to approximately 2.9 billion yen (US$24 million) in 2014.

Table 4. Loss in savings due to banking Trojans in Japan from 2012 to 2014

Year	Number of incidents	Amount lost	Amount lost in US dollars
2014	1,876	2.9 billion yen	US$24 million
2013	1,315	1.4 billion yen	US$14 million
2012	64	48 million yen	US$480,000

There have been a few interesting cases where financial Trojans specifically targeted Japan in 2014. Similar attack waves have been seen in other countries like South Korea and India. In 2014, Infostealer.Torpplar targeted confidential information related to Japanese online banks and credit cards.

Variants of Infostealer.Bankeiya used numerous methods, including zero-day exploits, to target Japanese users. In February 2014, attackers exploited the Microsoft Internet Explorer Use-After-Free Remote Code Execution Vulnerability (CVE-2014-0322) to infect users' computers with Infostealer.Bankeiya. The attackers compromised many Japanese websites in order to spread the threat to their preferred targets.

Infostealer.Bankeiya is a classic example of a focused attack against a specific region. The compromised websites included TV channel sites, a lottery site, as well as online shops, community websites, and personal websites. Sinkholing the C&C servers for one week in May revealed that up to 20,000 computers were compromised by this threat in that period alone.

In May, the next version of this Trojan, Infostealer.Bankeiya.B, started exploiting the newly discovered Adobe Flash Player Buffer Overflow Vulnerability (CVE-2014-0515) to spread. When we first noticed this particular exploit in the wild, more than 90 percent of the attacks targeted Japanese users. Legitimate websites were compromised to host the exploit, including travel sites, blog services, and a video-sharing platform.

The attackers then changed their tactics to carry out the classic supply-chain attack. They compromised the website of a Japanese computer peripheral company and replaced the driver updates with a Trojanized version. The company quickly noticed the attack and cleaned its website a few hours after the incident. By then, the malicious driver had already been downloaded over 850 times.

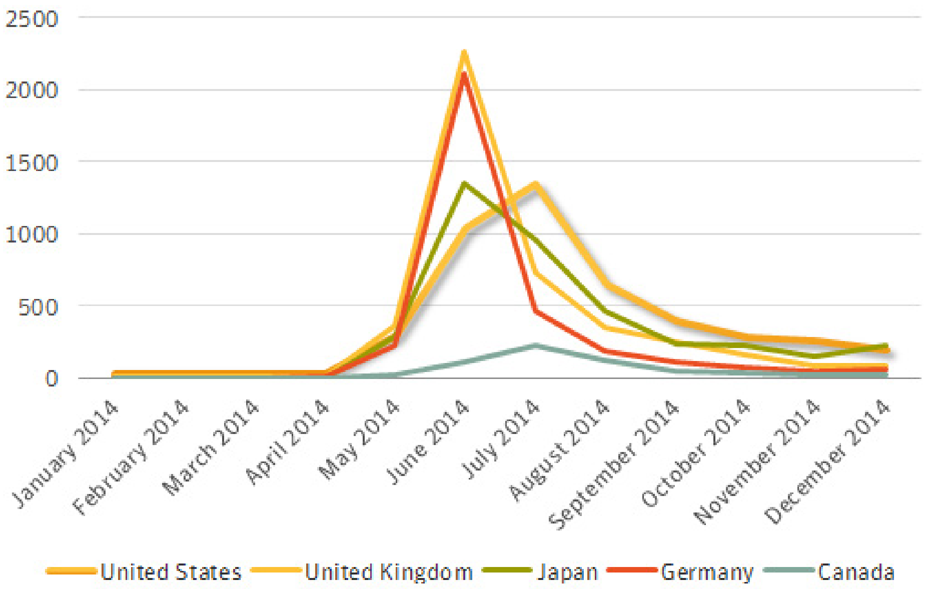
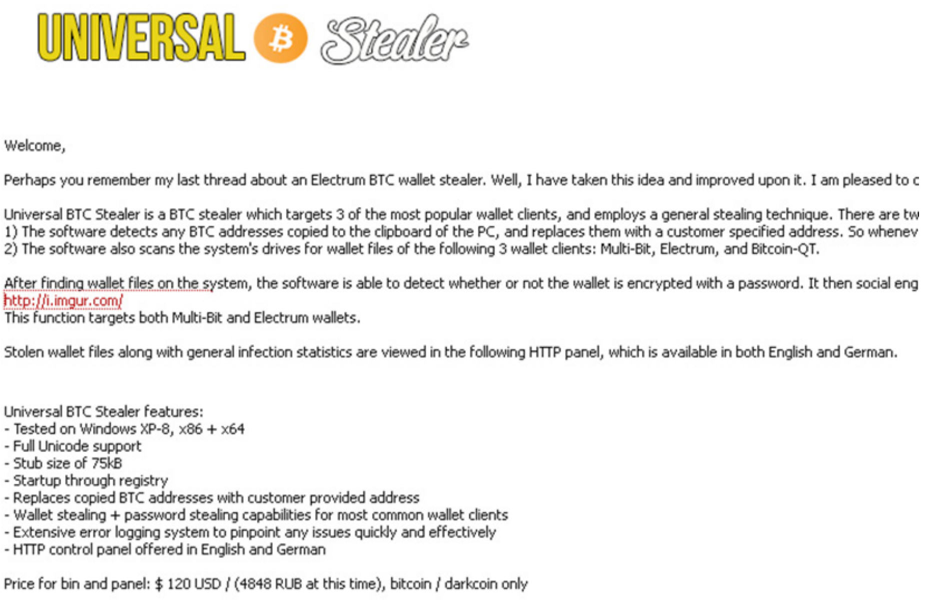


Figure 9. Top five Trojan.Snifula detections by country in 2014

Other financial Trojans increased their list of targeted institutions. Trojan.Snifula, which had a spike of activity in June 2014, grew its list of targets over the summer from targeting 8 to 37 different financial institutions in Japan, including 12 smaller regional banks in Japan. Japan had the third most Trojan.Snifula detections in 2014, following the US and UK.

Attacks outside of online banking

There are a few more financial-related attacks worth mentioning, which do not directly involve the classic online banking and financial Trojan.



Welcome,

Perhaps you remember my last thread about an Electrum BTC wallet stealer. Well, I have taken this idea and improved upon it. I am pleased to c

Universal BTC Stealer is a BTC stealer which targets 3 of the most popular wallet clients, and employs a general stealing technique. There are tw
1) The software detects any BTC addresses copied to the clipboard of the PC, and replaces them with a customer specified address. So whenev
2) The software also scans the system's drives for wallet files of the following 3 wallet clients: Multi-Bit, Electrum, and Bitcoin-QT.

After finding wallet files on the system, the software is able to detect whether or not the wallet is encrypted with a password. It then social eng
http://i.imgur.com/
This function targets both Multi-Bit and Electrum wallets.

Stolen wallet files along with general infection statistics are viewed in the following HTTP panel, which is available in both English and German.

Universal BTC Stealer features:
- Tested on Windows XP-8, x86 + x64
- Full Unicode support
- Stub size of 75kB
- Startup through registry
- Replaces copied BTC addresses with customer provided address
- Wallet stealing + password stealing capabilities for most common wallet clients
- Extensive error logging system to pinpoint any issues quickly and effectively
- HTTP control panel offered in English and German

Price for bin and panel: $ 120 USD / (4848 RUB at this time), bitcoin / darkcoin only

Figure 10. Advertisement for a Bitcoin stealer malware

Bitcoins

As the prices of Bitcoins have decreased by around 60 percent over the year 2014, it seems that attackers' interest in this cryptocurrency has dropped as well. Only a few of the information-stealers and financial Trojans have updated their configuration files to go after online Bitcoin wallet providers. We have also seen malware stealing offline wallets for cryptocurrencies like Bitcoin or replacing Bitcoin addresses in memory when a transaction is locally executed.

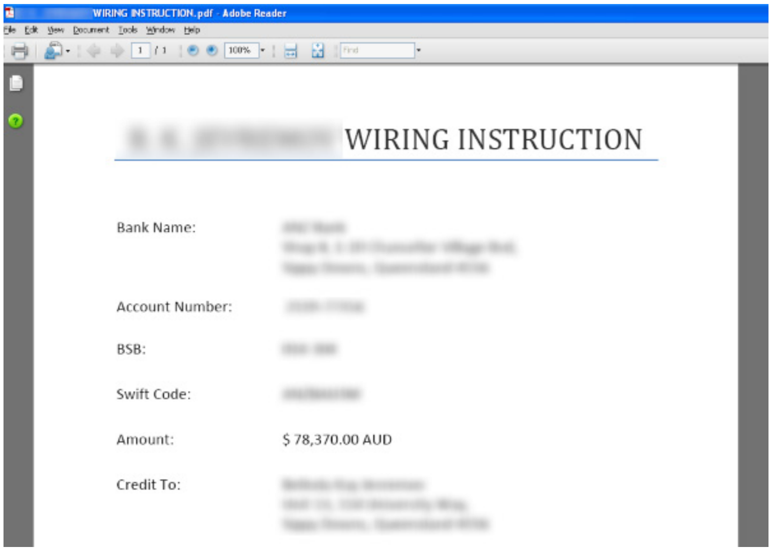
There have also been a few direct attacks against larger Bitcoin sites with online wallets, most notably the attack against Bitstamp at the beginning of 2015, but these campaigns usually do not involve the use of malware on users' computers.

We can only speculate on the reasons why the attackers did not adapt more to target cryptocurrencies. Perhaps cryptocurrency's usage is still too low to be attractive for the scammers or the attackers are still making enough profits with their other targets and don't want to change their plans to include cryptocurrencies yet.

Fake wire transfers

One type of financial scam that experienced a huge boom in 2014 is fake wire transfers. This kind of scam involves an attacker sending a convincing wire transfer instruction by email to the financial department of the targeted company. The fraudsters often pose as company executives planning an acquisition or a large deal. This cover story is then used to ensure that the victim does not talk with others about this transaction and to build up some urgency to issue the transaction right away.

We have seen such attacks before and the FBI warned about them in 2014. However, with the amount of information available in social networks along with use of online payments to carry out larger transactions, these scams have become much easier for attackers to conduct than ever before.



[redacted] WIRING INSTRUCTION.pdf - Adobe Reader

[redacted] WIRING INSTRUCTION

Bank Name: [redacted]

Account Number: [redacted]

BSB: [redacted]

Swift Code: [redacted]

Amount: $ 78,370.00 AUD

Credit To: [redacted]

Figure 11. Example of fake wire transfer instructions

In one instance, attackers successfully compromised the mail server of a construction material supply company. After observing the email traffic for several weeks, the attackers started to use old invoices as a template and created modified versions with new beneficiary account details. These fraudulent invoices were then sent to victims with a note asking them to update the banking details. This simple trick convinced a few of the victims to issue very large transactions to the scammers' account.

Similar variants of the scam have been observed, where the attackers registered a domain name resembling their victim's and used this to send convincing invoice emails. Other attackers even compromised the VOIP telephone system in order to catch anyone who might be making transactions by phone.

This scam usually does not involve malware and relies heavily on social engineering. For the bank, this transaction is harder to spot as well, since it is conducted from the legitimate account with non-stolen credentials. Even if the bank representative calls the issuer of the transaction for more details, the issuer will confirm the payment due to the social engineering cover story.

Takedowns

Increased collaboration among different law enforcement entities and private sector companies has resulted in a number of takedown operations against larger botnets, including financial Trojan botnets, and arrests of malware authors.

In July 2014, a joint takedown operation, led by the UK National Crime Agency (NCA) and European Cybercrime Centre (EC3) at Europol, resulted in the seizure of C&C servers and domains used for Trojan.Shylock's communications between infected computers. This banking Trojan mainly targeted financial institutions in the UK and US. The damage caused by Trojan.Shylock is estimated to cost several million US dollars.

The main source of Shylock infections in 2014 was through exploit kits. Shylock has been observed being distributed by at least five different exploit kits over the past year: Blackhole, Cool, Magnitude, Nuclear, and Styx. After the takedown, the number of Shylock infections fell by more than half.

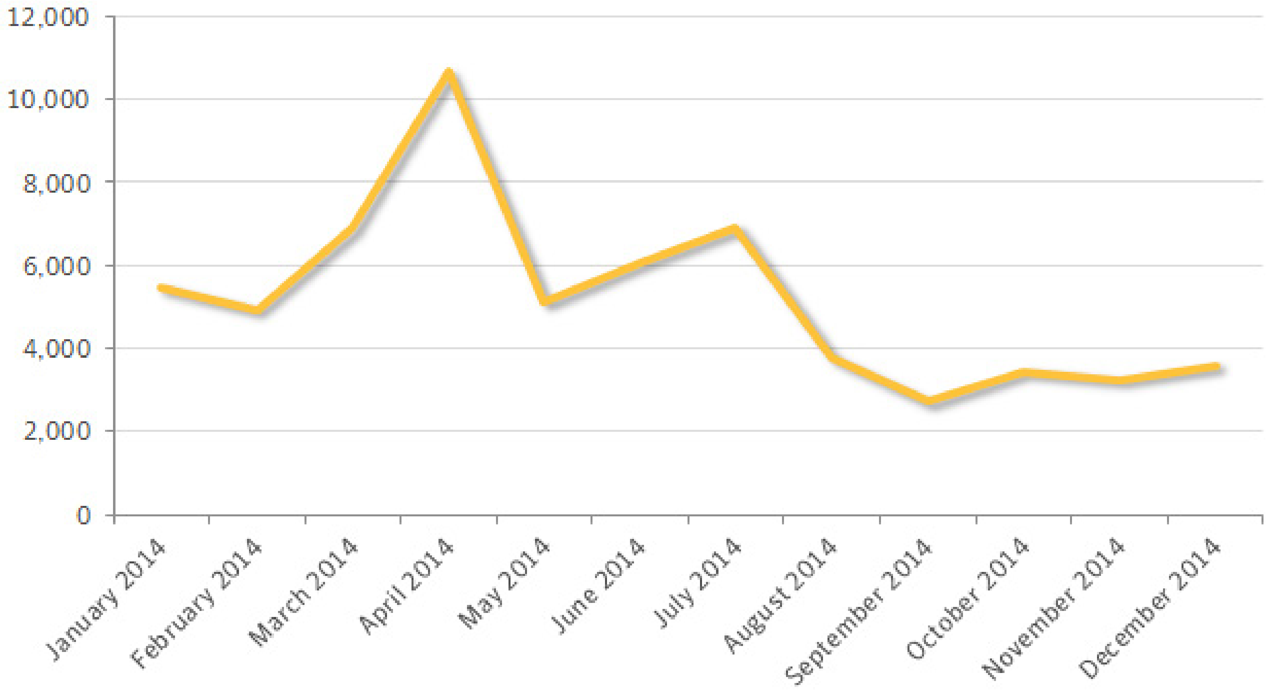


Figure 12. Trojan.Shylock detections per month in 2014

About one month earlier, a similar operation by the FBI, NCA, and other law enforcement agencies and security companies took out much of the Gameover Zeus botnet. The variants in question used a P2P infrastructure for C&C communication and a DGA as fall back method, making the C&C operations more difficult to completely disrupt.

The Gameover Zeus group has maintained a relatively steady network of hundreds of thousands of infected computers around the world, with the most infections located in the US. Gameover Zeus has survived at least two previous attempts to disrupt the botnet, in the spring and autumn of 2012. The Gameover Zeus team closely monitors suspicious activity to protect the existing network of compromised computers. This is a highly profitable enterprise worth protecting and the group is known to identify weaknesses within the network and rebuild when necessary.

Whenever there are takedown operations or major arrests, there are also discussions on how successful and wise these moves really are. Fighting botnets is by no means an easy task. It is difficult to completely eradicate botnets and often, the criminals will build a new botnet if they have not been arrested. Even the arrest of the author of Spyeye in 2013 did not make this botnet disappear completely. Arguably, the attackers could learn from the takedown and come back with an even stronger new version of the threat.

However, law enforcement can't allow this argument to stop them from carrying out takedown operations in the future. Ultimately, the operations do have a positive effect and hinder the cybercriminals. We believe that even if takedowns operations do not permanently stop cybercriminals, they at least make it harder for the cybercriminals, who have to spend time and resources to rebuild their campaigns. The arrests, which are often made in parallel to the C&C infrastructure seizures, send a clear message to cybercriminals. Every little helps in order to make the internet a safer place for tomorrow.

Symantec recently signed a memorandum of understanding (MoU) with Europol to continue this coordinated effort. Although this was a positive step in keeping consumers and business protected, the reality is that cybercrime won't disappear overnight. Both private industry and law enforcement will continue such collaborative efforts in 2015 in order to have a long-lasting impact against cybercrime and stop attackers in their tracks.

Protection

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

- Antivirus and IPS detections are in place for each of the discussed threat families
- Browser protection can protect against exploits
- Norton Safeweb blocks users from visiting compromised websites
- Insight can proactively block files associated with financial Trojans and detect them as WS.Reputation.1
- Behavior-based detection blocks suspicious processes using the Bloodhound.SONAR series of detections
- Symantec MessageLabs Email Security.cloud can block emails associated with these attacks

In addition, users should adhere to the following advice to prevent these attacks from compromising their computers:

- Exercise caution when receiving unsolicited, unexpected, or suspicious emails.
- Keep antivirus software and operating systems up to date.
- Enable advanced account security features, like 2FA, if available
- Use strong passwords for all your accounts
- Always log out of your session when finished
- 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

Symantec

CONCLUSION

> “In a mix of broad strokes and focused attacks, attackers will continue to streamline their campaigns to maximize return on their efforts.”

Conclusion

The world of financial Trojans is a thriving and profitable one for the cybercriminals. The financial fraud marketplace is a well-organized service industry where a wide variety of financial Trojans, web injects, and distribution channels are traded. These offerings help to improve the effectiveness of established attack techniques. Location-aware distribution services deliver payloads with precision, while web injects which are remotely updated by third parties are available to help circumvent security countermeasures. The tools are offered on a software-as-a-service basis and allow anyone to conduct a large array of intelligent attacks against different financial institutions.

By mixing various strategies and techniques, attackers will continue to streamline their campaigns to maximize return on their efforts. In 2014, we did not see much innovation in fraud techniques. Most attackers relied heavily on man-in-the-browser attacks through web injects. They perfected and automated proven techniques, expanded to newer regions like Asia, and went after specialties in local markets like the Boleto Bancário payment system in Brazil. We have also seen more attackers using banking Trojans against non-financial services, including stealing master passwords for password safes.

Despite the criminals' best efforts, the number of financial Trojan infections decreased by 35 percent in 2014. This can be partially attributed to a few takedown and arrest operations conducted by different law enforcement agencies in cooperation with the security industry. It is clear that these operations have had some success but cybercrime won't disappear overnight. Both private industry and law enforcement must continue such collaborative efforts in 2015 in order to have a long-lasting impact against cybercrime.

Aside from this, some financial institutions are starting to adopt strong security measures like chipTAN, but the adoption rate is slow. Institutions that persist with weaker security measures will continue to be targeted by attackers. Strong security measures will deter attackers from pursuing these institutions in favor of vulnerable institutions where existing attack techniques are successful. As long as institutions continue to use weak security measures, large-scale financial fraud will continue to be a lucrative enterprise for attackers.

Unfortunately, the end user is often the weakest link in the chain during an online transaction. Because of this, even the strongest technologies are susceptible to social engineering attacks. Institutions need to be open about the risks and continue to educate their customers about the security issues they encounter. Many banks have internal anti-fraud monitoring systems that can detect and block suspicious transactions. It will take time for adequate protections to be put in place, and until then, cybercriminals will continue to defraud institutions and their customers of millions of dollars each year.

Authors

Candid Wueest
Princ Software Engineer

Follow us on Twitter
@threatintel

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

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 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

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

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

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.