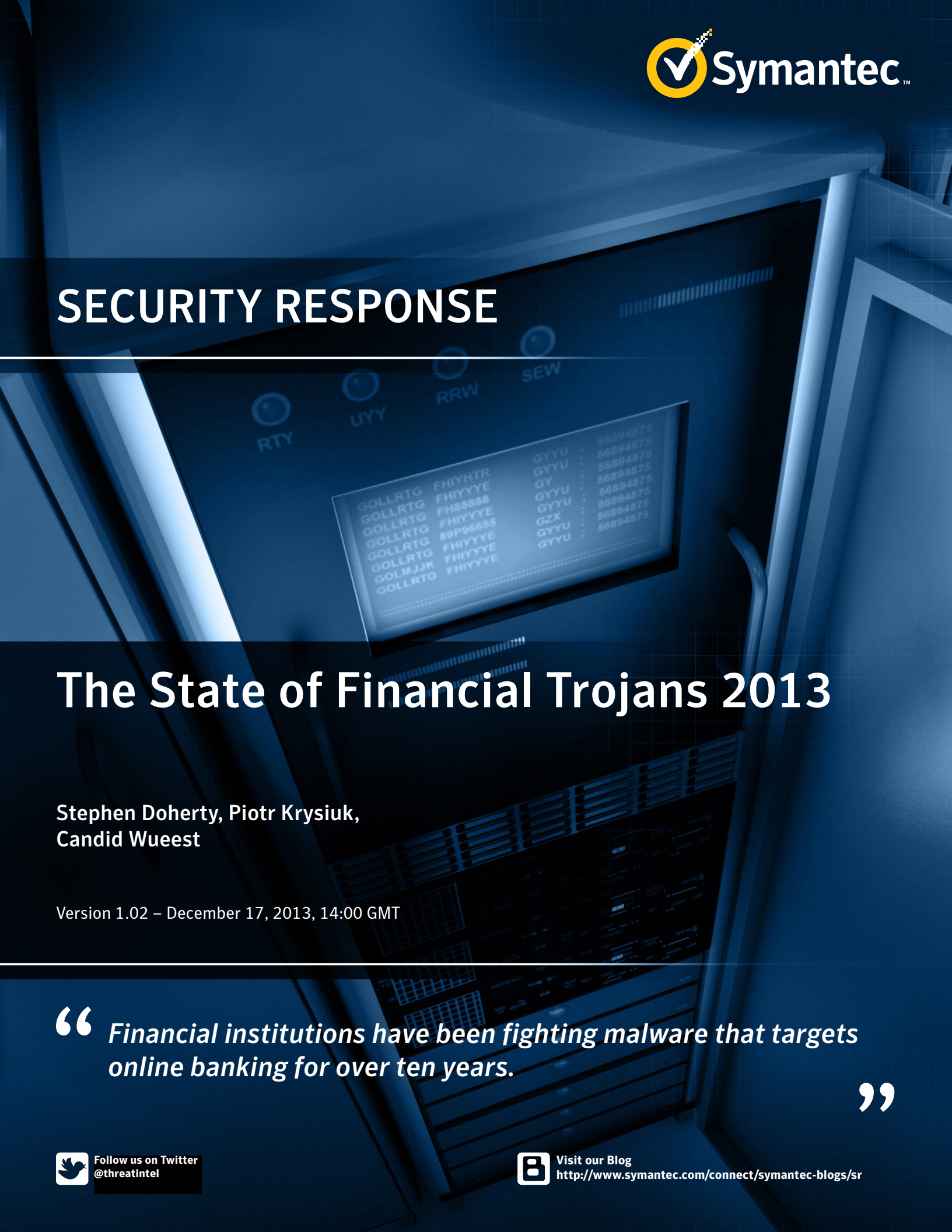


Symantec

SECURITY RESPONSE

The State of Financial Trojans 2013

Stephen Doherty, Piotr Krysiuk,
Candid Wueest

Version 1.02 – December 17, 2013, 14:00 GMT

“Financial institutions have been fighting malware that targets online banking for over ten years.”

Follow us on Twitter
@threatintel

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

CONTENTS

OVERVIEW 3
Key findings 4
Introduction 4
Targeted institutions 7
Modern banking Trojans 8
- Man-in-the-browser attacks 10
- The underground economy 10
- Trojan capabilities 11
- Strategies 11

Other ways to attack financial targets 16
- Online banking and mobile 16
- Attacks outside of online banking 16
- Bitcoin 16

Conclusion 18
Appendix 20
- Notable Trojans 20

Resources 23
Glossary 24

OVERVIEW

Financial institutions have been fighting malware that targets online banking for over ten years. During that timeframe, banks have had to evolve their security measures to protect online transactions from fraud. Attackers adapted to these countermeasures and sophisticated banking Trojans began to emerge. In many situations, financial institutions adopted custom security solutions. However, many of these security implementations are ineffective at protecting against the modern banking Trojan. Cybercriminals who are motivated by financial reward are using these advanced Trojans to commit large scale financial fraud, targeting institutions across the globe.

This report is an update on the financial Trojan threat landscape for 2013. It examines eight of the most common and sophisticated financial Trojans in circulation today. The Trojans have been targeted at over 1,400 financial institutions and compromised millions of computers around the globe. When targeting these institutions, many attackers either opt for a focused attack or a broad strokes approach. Exact details of the techniques used against specific financial institutions are withheld, but are available to the financial institution on request.

Key findings

- Over 1,400 financial institutions are targeted by attackers using financial Trojans
- The top 15 targeted financial institutions were targeted by more than 50 percent of the Trojans
- The most targeted bank is in the US and was attacked by 71.5 percent of all analyzed Trojans
- Two dominant attack strategies are identified: “focused attack” and “broader strokes”
- Institutions in 88 countries have been targeted
- Continued expansion into the Middle East, Africa and Asia
- New institution types are being targeted outside of traditional online banking
- Existing techniques are being streamlined for automation and precision
- In the first three quarters of 2013, the number of financial Trojans has grown by three times

Introduction

In 1994, financial institutions started providing online banking services to their customers. Using a Web browser, clients could log into their bank’s secure website to view statements, add new accounts and make financial transactions. Since then, online banking has grown in popularity and today, most major financial institutions facilitate the service and are evolving it further to reach mobile devices. In that same time period, attacker motivations have changed dramatically. No longer searching for notoriety and fame, cybercriminals have turned their attention to financial gain. Initially, attacks against user accounts involved simple keylogging Trojans and phishing emails. These attacks were capable of defeating simpler security measures. By May 2003,

Figure 1. Weak authentication and authorization (OTP tokens, iTAN)

around 20 distinct banking Trojans existed. As financial institutions bolstered security and fraud detection capabilities, cybercriminals adapted. Since then, many new banking Trojans have emerged. Modern day attacks involve sophisticated Trojans capable of circumventing complex security mechanisms.

The European Network and Information Security Agency (ENISA) currently advises financial institutions to adopt security measures that assumes that user devices are compromised. Some institutions are now beginning to adopt strong security measures such as transaction authentication numbers (TAN) with transaction verification. These out-of-band challenge response mechanisms, which contain a transaction verification step, greatly enhance the security of online transactions. A strong security measure is likely to prevent an unsuspecting user from proceeding with a

Figure 2. Strong authentication and authorization (chipTan transaction verification)

fraudulent transaction on a computer that has been compromised with an advanced financial Trojan.

Unfortunately, the adoption rate of strong technologies is slow and attackers are exploiting existing weak security measures. Over the years, the sophistication of Trojans targeting these weak security measures has increased dramatically and financial Trojans have become one of the most prevalent threats today. In the first three quarters of 2013, the number of financial Trojans has grown by three times.

The banking Trojans selected for this research are listed in the following table. These Trojans were highly prevalent threats this year, collectively compromising millions of computers around the world.

Table 1. The prevalence of banking Trojans in 2013

Threat	Compromised computers	Availability
Zbot + Gameover	>2,000,000	Public and custom
Cridex	>125,000	Private
Shylock	>33,000	Custom
Spyeye	~26,000	Public
Bebloh	~21,000	Custom
Mebroot	~9,000	Custom
Tilon (Tiylon)	~2,000	Custom

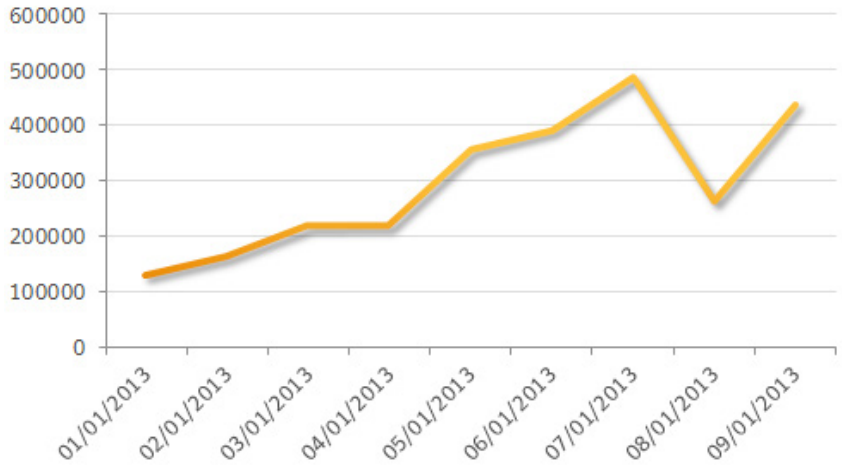


Figure 3. Number of computers compromised by banking Trojans in 2013

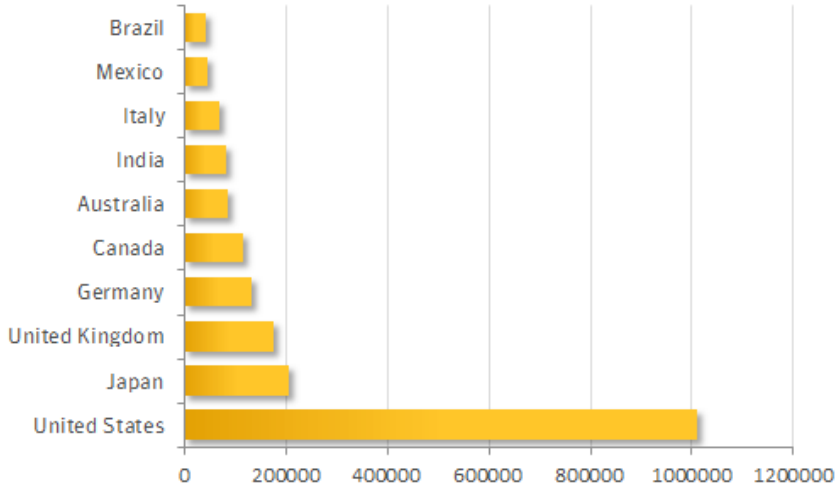


Figure 4. Number of computers compromised by banking Trojans by country in 2013

Symantec

TARGETED INSTITUTIONS

> “In nearly 95 percent of cases, financial sector institutions were targeted.”

Targeted institutions

Today's banking Trojans typically utilize an updatable and encrypted configuration file, which is stored in the file system, the registry or is actually embedded in the Trojan itself. The configuration file contains a list of target URLs along with rules to be applied to these Web pages.

In this analysis, 1,086 configuration files were examined. Over 2,000 domains belonging to more than 1,400 distinct institutions were identified in these configurations. In nearly 95 percent of cases, financial sector institutions were targeted. The remaining five percent were traditional online services like social media, employment websites, auction houses and webmail.

Table 2 is a list of the types of institutions being targeted:

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

Table 3 lists banks ranked by how frequently attacker configuration files target them. Specific institution identities are not provided here but are available to financial institutions by request.

Table 2. Targeted institutions

Online banking	Related financial	Third-party finance	Other
Commercial banks	Payroll systems	Private corporate finance	Health
Private banks	Stock trading	Private corporate credit cards	Travel
Automated Clearing House (ACH)	Commodities		Employment
Investment banks	ePayments		Auctions
Merchant banks			Web services
Building societies			Social networking
Cooperative banks			Entertainment
Credit unions			Dating
Banking platforms			

Table 3. Top 25 institutions targeted in configuration files

Rank	Institutions	Locations	% of Trojans targeting firm
1	Bank 1	United States	71.54
2	Bank 2	United States	65.54
3	Bank 3	United Kingdom	62.62
4	Bank 4	United Kingdom	62.43
5	Bank 5	Colombia, Spain, United Kingdom	61.33
6	Bank 6	United Kingdom	60.82
7	Online payments	United States	57.05
8	Bank 7	Italy	56.75
9	Bank 8	United States	56.36
10	Bank 9	United States	56.36
11	Bank 10	United States	55.77
12	Bank 11	Germany	54.44
13	Bank 12	United Kingdom	51.28
14	Bank 13	Germany	50.71
15	Bank 14	France	50.62
16	Bank 15	Canada	50.24
17	Bank 16	Australia	49.98
18	Bank 17	United States	49.91
19	Bank 18	United Kingdom	49.80
20	Bank 19	Spain	49.14
21	Bank 20	United States	48.51
22	Bank 21	France	48.12
23	Bank 22	United States	45.60
24	Bank 23	United States	45.47
25	Bank 24	United Kingdom	45.10

Attackers prefer to target institutions in developed countries with sizeable populations and wealthy residents. This makes sense as there is a large potential base of individuals to compromise with a high potential return. Different global factors can influence attackers' decisions, such as spoken languages and countries where international transactions are more difficult and require local steps to launder the money.

Today's banking Trojans are a major step forward since 2003. Many of the modern banking Trojans seen today are heavily influenced by two threats that appeared between 2007 and 2009.

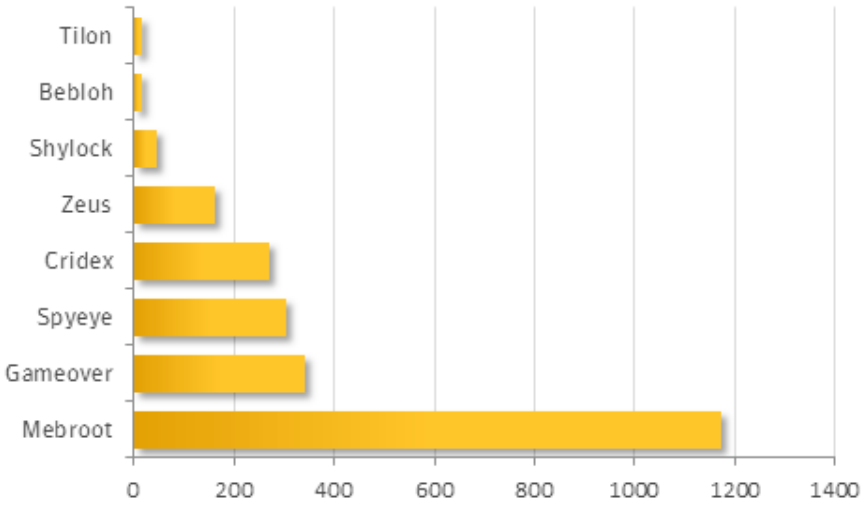


Figure 5. Number of institutions targeted by each Trojan

Modern banking Trojans

In 2007, an advanced financial fraud Trojan emerged called Zbot (Zeus). This kit, created by a Russian malware author called Slavik/Monstr, sold on the underground for thousands of dollars. Two years later in 2009, a competing Trojan called Spyeye, authored by Gribodemon, hit the market and sold for the more affordable price of US$700. The underground financial Trojan marketplace was thriving.

The market has changed considerably since then. The Zeus source code was stolen and leaked to the underground community in May 2011. The price of this kit crashed instantly as Zeus became freely available. Forks of Zeus began to emerge, including the enhanced kits Ice IX and Citadel, which competed for market share. Cybercriminal gangs also built custom

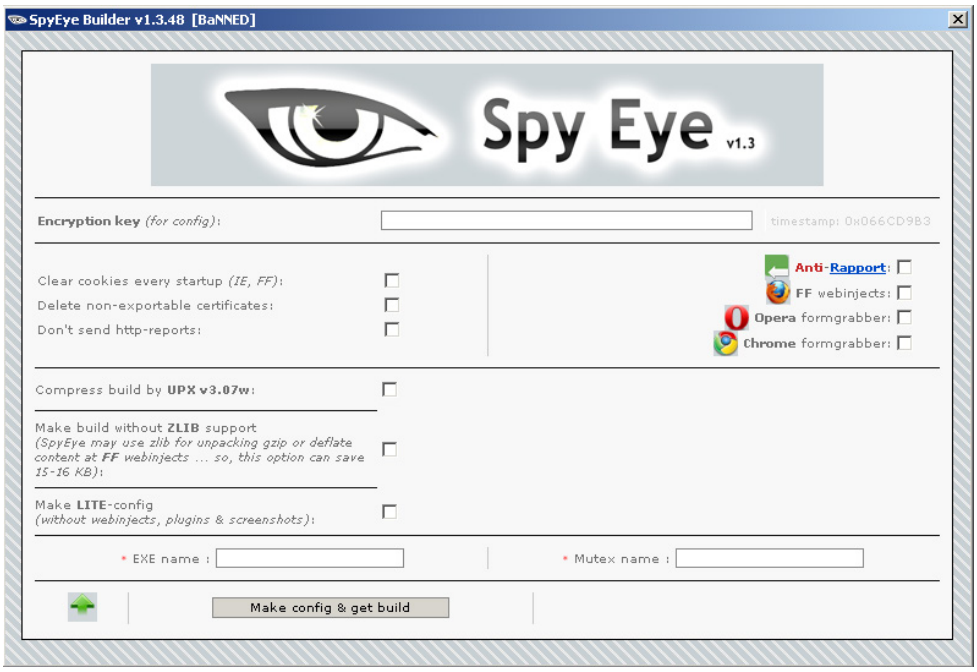


Figure 6. Leaked version of Spyeye builder

versions of Zeus for personal use, such as the notorious “Gameover,” which appeared in July 2011. One month after Zeus’ source code leaked, an individual who goes by the moniker of Xylibox cracked the builder protection for Spyeye. It suffered from a similar price crash to Zeus. Currently, neither Trojan is being actively developed by their original authors in the public domain. Many modern financial Trojans have copied the techniques and architecture of Spyeye and Zeus.

Modern-day banking Trojan kits typically contain of the following components:

Builder application: This is used to configure and generate the Trojan payload

Backend scripts: These scripts include a control panel on a command-and-control (C&C) server to direct compromised computers. Backend scripts can be a weak point for the attacker if they are identified, which could help law enforcement, CERTs or Internet service providers shut down the C&C server. Attackers are using bulletproof hosting, hacked proxy servers, cloud services, domain generator algorithms (DGAs), hidden Tor services and peer-to-peer (P2P) infrastructure to protect the C&C server against identification and takedown. Newer versions of backend scripts include CAPTCHAs and SQL injection mitigations in order to protect against other cybercriminals brute-forcing the login page to access the backend script.

Configuration file: This file contains target URLs along with rules and modifications to be applied to these targeted Web pages. This information is used for an attack technique called man-in-the-browser (MITB).

```
<url domain=[redacted] request="/commercial/planning/g2/security-advice-centre*" />

<data>
<begin mask="*">
</begin>
<inject>
[redacted]<span style="display:none;">
</inject>
<end mask="*">
[redacted]
</end>
</data>
<data>
<begin mask="*">
[redacted]
</begin>
<inject>
</span>
</inject>
<end mask="*">
</end>
</data>
```

Figure 7. Shylock configuration alters phone numbers displayed on a UK banking website

Man-in-the-browser attacks

This idea was first presented by Agusto Paes de Barros in 2005 and by 2007, financial fraud Trojans were using this attack technique. Man-in-the-browser (also known as Web-injects) is an attack technique that involves an application hooking into the browser and manipulating data before it is displayed. A simple man-in-the-browser attack is described below:

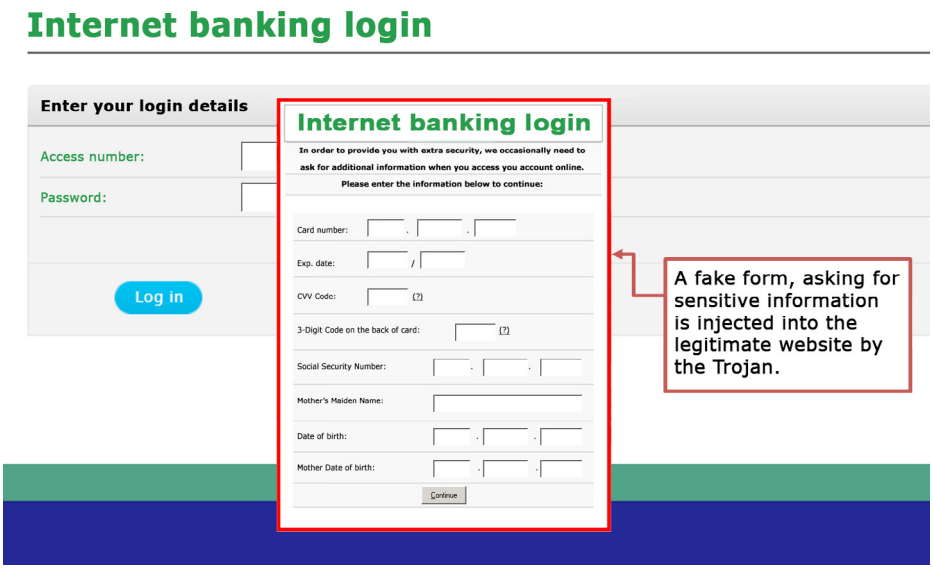


Figure 8. Man-in-the-browser attack

- User attempts to log into a website
- Trojan intercepts the request
- Trojan injects a form in the browser, which requests sensitive information to proceed
- User unknowingly submits information to the attacker

A man-in-the-browser 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 attacker requests and can end up fooling the user. This is a simple example of how Web-injection works. More complex Web-inject scripts are capable of dynamically loading important data to avoid attention. The more sophisticated scripts can automatically execute transactions in the background.

Since most major financial institutions facilitate online banking through a Web browser, it is not surprising to see that modern banking Trojans have adopted this technique. It's an appealing feature for attackers who are looking for an effective financial Trojan on underground marketplaces.

The underground economy

Attackers of all skill levels can enter the arena of financial fraud, as the underground marketplace is a service industry that provides an abundance of resources. Those who lack expertise can simply purchase what they need. The Trojans and services available to attackers vary depending on the experience and financial resources available. Entry-level attackers have a limited selection of financial Trojans, while more experienced or trusted attackers will have access to private Trojans. Experienced attackers may even decide to develop their own custom Trojan.

For as little as $100, an attacker can avail of a leaked Zeus or Spyeye equipped with Web-injects. These bots are unintelligent and require configuration updates. A state-of-the-art Zeus fork, like Citadel, costs around $3,000 to an outsider and includes regular updates. Custom Web-injects can be purchased for between $30 and $100. Third-party spam services, location-aware exploit kits and traffic direction services can then be used to deliver the payload. Those services may come with explanatory videos or even free chat support during installation.

Key factors in determining the success of a campaign are:

- Trojan selection – Reliable, stable, low detection rate
- Web-inject configuration – Intelligent, up to date
- Distribution – The target user must be a customer of financial institutions specified in the Trojan's

configuration data
- Money laundering – Reliable source of money mule bank accounts

Trojan capabilities

The modern financial Trojan is extremely flexible, supporting a range of functionality designed to facilitate fraudulent transactions across a variety of services. Modern financial Trojans share many characteristics. MITB is a technique common to all of the financial Trojans selected for this research. The security implementations of a given institution will determine the level of sophistication required. For example, advanced functionality like Virtual Network Computing (VNC), which provides direct access to the compromised computer, is limited to a subset of Trojans analyzed. Direct access to a compromised computer is not necessarily a requirement. The choice of Trojan depends on the financial resources of the attacker and the level of security an institution adopts.

Table 4 contains a feature list of these analyzed financial Trojans. Some of these features are plugins that can be added to the Trojan. Some groups developed their own private plugins which might not be listed below.

Financial Trojans facilitate fraudulent transactions. The MITB component gathers and manipulates required fields on the Web page in order execute these transactions. The combination of these techniques and capabilities determines the success rate of a fraudulent transaction.

*Table 4. Features in modern financial Trojan (*Citadel enhancement **additional plug-in)*

Feature	Zeus	Gameover	Spyeye	Bebloh	Shylock	Tilon	Mebroot	Cridex
MITB	X	X	X	X	X	X	X	X
Redirect	X		X			X	X	X
Screen shots	X	X	X	X				
Video	X*				X		X	
Certificates	X	X	X		X		X	X
Credit cards			X			X	X	
Notifier			X					
Proxy	X	X	X		X	X	X	X
Back connect	VNC	VNC	RDP**		VNC		X	

These Trojans rely heavily on intelligent configurations for MITB to work.

Strategies

After choosing, their Trojans, the attackers must then consider the strategy needed to attack their targets. Every cybercriminal has a preferred method of operation. The following table highlights some of the current tactics observed involving the Trojans analyzed.

Attackers do not limit themselves to one approach over another.

Table 5. Financial Trojans, including price and other information

Threat	Availability	Maintenance	Price	Targeted Institutions	Prevalence
Zeus	Public	Low	Free - $1000s	Focused/Broad	High
Spyeye	Public	Low	Free – $700	Focused/Broad	Medium
Cridex	Private	Low	N/A	Broad	High
Mebroot	Custom	High	Priceless	Broad	Medium
Tilon	Private/ Custom	High	N/A	Focused	Low-Medium
Gameover	Custom	High	Priceless	Broad	High
Shylock	Custom	High	Priceless	Focused	Low
Bebloh	Custom	High	Priceless	Focused	Medium

They will use multiple banking Trojan families, if necessary, and adapt their methods to suit their circumstances. Attackers might abandon the use of one Trojan in favor of another if the first one is under intense focus of security researchers and law enforcement operatives. Two distinct approaches are, however, most typical: the focused attack and the broad strokes approach.

Focused attack

With the advent of location-aware exploit packs and traffic direction services, localized attacks are easy to launch. This approach suits attackers with limited resources but also scales well to larger operations. If the distribution is accurate and the target institution has a sizeable client base, a focused attack can provide an adequate supply of targets. Shylock, Bebloh and Tilon all use this approach exclusively.

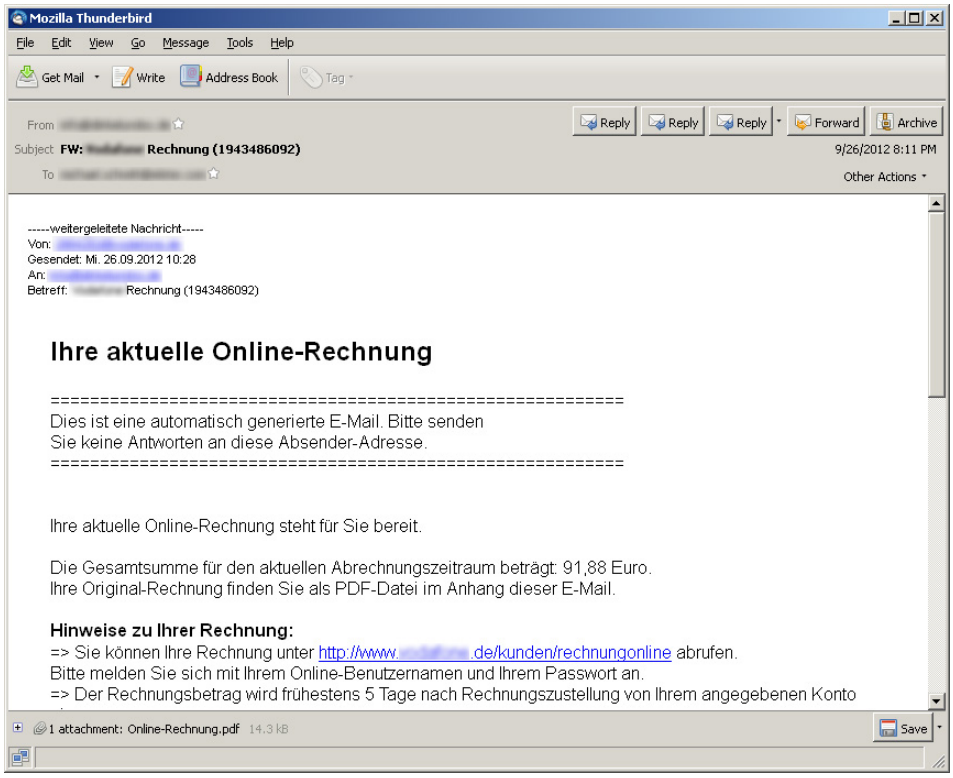


Figure 9. Trojan.Bebloh (URLZone) targeted attack email

Focused attacks have two main characteristics:

- Focused target list
- Localized distribution

Choosing a focused list of financial institutions has its advantages. There is a lower maintenance cost, fewer rules require modifications when institutions update their websites, and it's relatively simple to target consumers by using location-aware exploits or targeted attack emails.

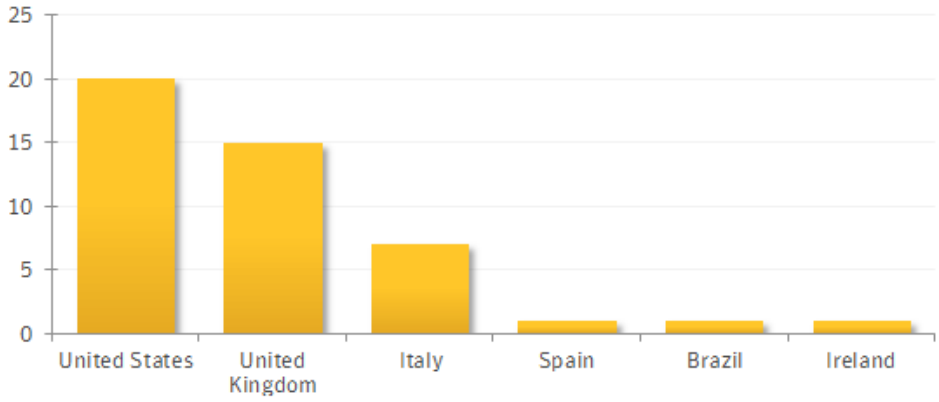


Figure 10. Trojan.Shylock, targets per country in 2013

Trojan.Bebloh was used against three German institutions exclusively since 2009, compromising computers through targeted attack emails. In 2013, the Trojan was targeted at seven financial institutions — one in France and several Internet service providers in Germany and the US. Trojan.Shylock, on the other hand, was predominantly targeted

at UK institutions in 2012 and is distributed through location-aware exploit kits. In 2013, Shylock expanded to include targets in the US.

This is a prime example of attackers actively exploring new markets in order to search for additional profit. This expansion may serve as an indication that UK institutions are adopting stronger technologies or that the attackers have free resources that they want to invest.

Although Trojan.Spyeye does not exclusively fit into the category of focused attack, Spyeye users also tend to adopt a focused approach. The majority of the examined Spyeye configurations target just one or two institutions.

On average, a typical Spyeye configuration may target around 19 institutions but one Spyeye configuration actually targeted up to 155 institutions in a broad strokes approach, the highest number of targeted institutions seen in a Spyeye configuration.

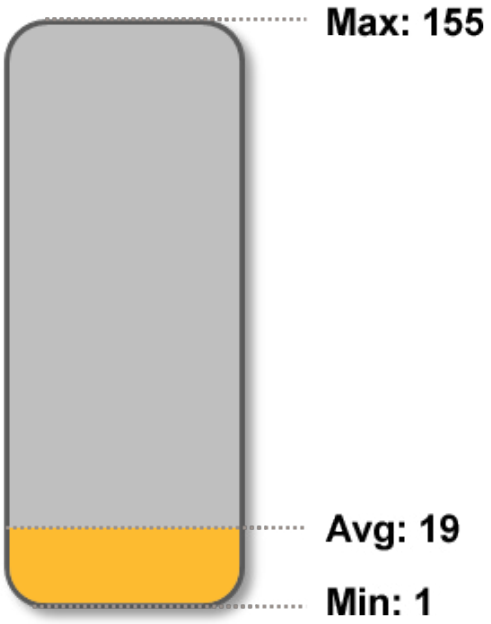


Figure 11. Number of institutions targeted in Trojan.Spyeye configurations

Attackers attempted to keep a low profile this year using Trojan. Hesperbot against banks in Turkey and the Czech Republic. The attackers sent out emails with a link to an alleged invoice from the local bank. When the user followed the link, they ended up on a clean website that asked them to solve a CAPTCHA. When the user entered the CAPTCHA correctly, they were redirected to the malware binary and were prompted to save or open it. This additional step by the attacker ensures that any automated security service that scans URLs in emails will end up at a benign-looking site with no exploit and no evident malware. If the user visited the same site with a mobile device, the script asked the user to access the site through a computer. This is because the malware was not able to infect mobile devices at the time.

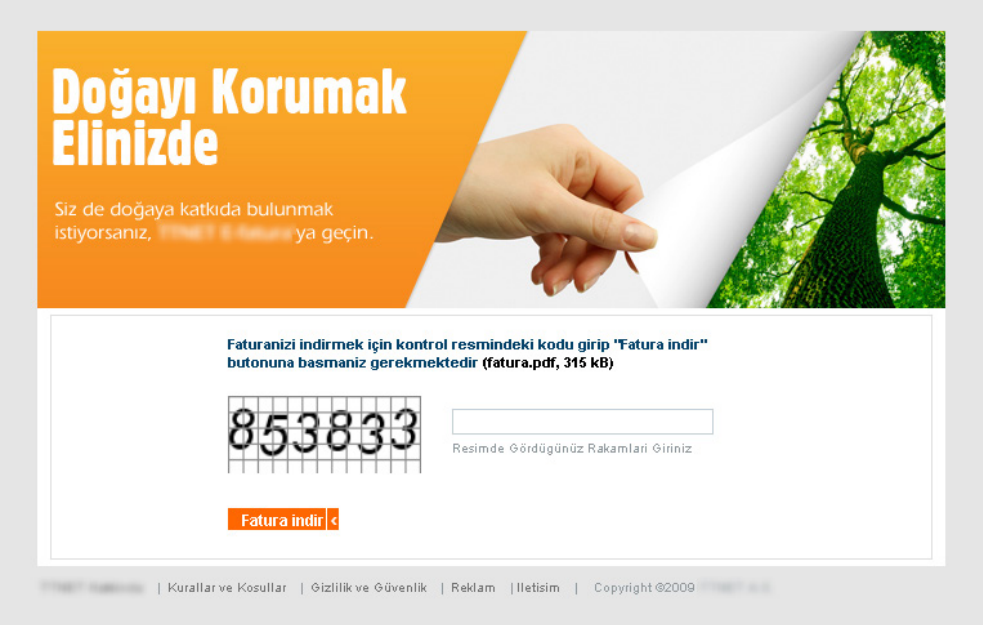


Figure 12. Phishing with CAPTCHA

Broad strokes

In this attack strategy, Trojans are set to target large numbers of institutions. Tilon, Cridex, and Gameover adopt these tactics and Zeus also uses this approach in its default configuration. Maintaining rules to circumvent protections at every institution requires a lot of work, however. In many cases, attackers rely on intelligent configurations from third-party developers. This service is typically included as part of the package when buying a kit. Alternatively, the attacker can use third-party services. Automated transaction services (ATS) are now being used in some of the more sophisticated attacks.

Targeting a large number of institutions concurrently suits large-scale distribution campaigns. Attackers who adopt this approach typically mass-distribute the Trojans through drive-by-downloads, iframe injection attacks, spam

runs or blackhat search engine optimization. Targeting a large array of institutions also works for reconnaissance, allowing attackers to monitor user interactions at specific institutions before deciding if it is a suitable target. Distribution does not need to be accurate.

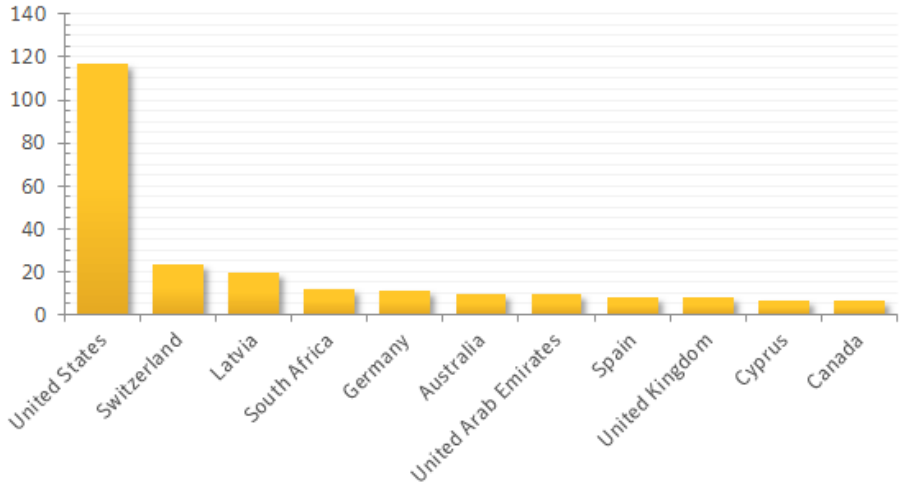


Figure 13. Cridex, targets per country

Typically, configuration files are self-contained, possessing all the functionality required to engineer a fraudulent transaction. In certain broad strokes attacks, remote Web-inject components have been observed. The logic to circumvent bank security implementations are retrieved from remote sites. These scripts are independent from specific Trojan configurations, opening up the potential for dedicated services supplying intelligent Web-injects that work across multiple Trojan families.

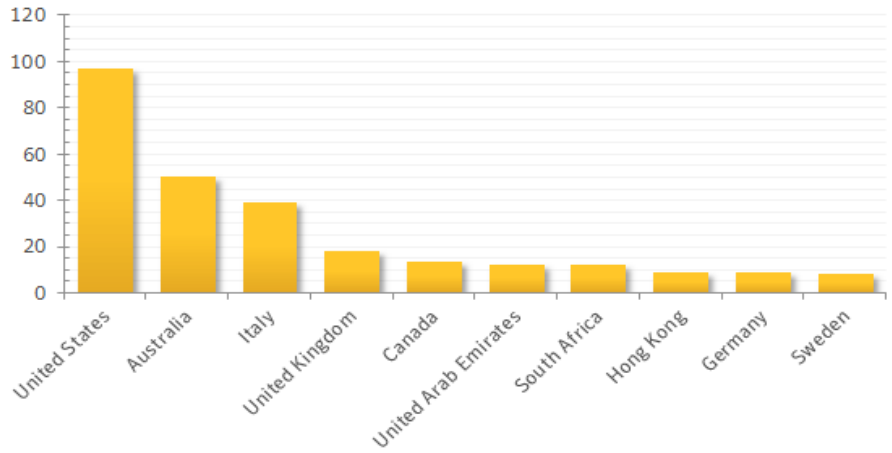


Figure 14. Gameover, targets per country

The Zeus fork, Gameover, combines a broad strokes approach with innovative techniques. The Trojan employs a P2P infrastructure, which is resilient to takedown. It also has significant capabilities in terms of distributed denial-of-service (DDoS) attacks and uses remote Web-injects to facilitate automated transaction services. The traditional Zeus Trojans have generally targeted a large number of institutions. In our investigation, the average number of targeted institutions is 68, but a maximum of 115 institutions has been observed.

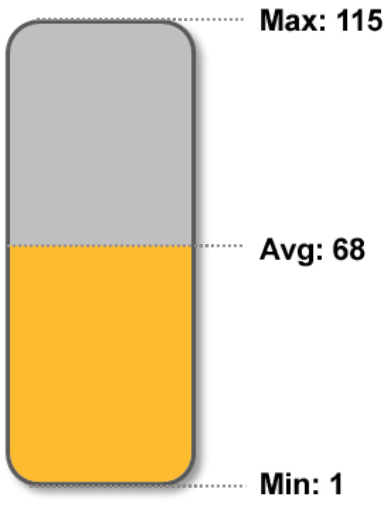


Figure 15. Number of institutions targeted in Zeus configurations

Both focused and broad approaches have their advantages and the attackers' chosen strategy is influenced by preference, experience and resources. The advent of third-party services offering customized and remote Web-injects allows attackers to intelligently target institutions more reliably and on a larger scale. These services will enable attackers with adequate financial resources to adopt either approach. The idea of mass-distributed Trojans targeting large numbers of institutions concurrently and also leveraging third-party services dedicated to circumventing security measures is concerning.

Symantec™

OTHER WAYS TO ATTACK FINANCIAL TARGETS

> “Attackers have also targeted new emerging cryptocurrencies, the most prominent of which is Bitcoin.”

Other ways to attack financial targets

There are several ways that attackers can take advantage of financial institutions' newer banking services, such as mobile banking, for financial gain. They can target financial institutions with misdirection to undertake unnoticed malicious activities. Attackers have also targeted new emerging cryptocurrencies, the most prominent of which is Bitcoin.

Online banking and mobile

Many financial institutions have started to use mobile devices like smartphones as an authentication token for the user. The use of mobile TAN (mTAN) has become very popular for banks. With mTAN, the bank sends a text message to the customer's registered phone number. The message contains an authorization code and often mentions some of the transaction details for verification purpose. 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. Other organizations distribute a one-time password generator application on the mobile device, which can be used for two factor authentication (2FA). As a result, when the user executes a transaction on the mobile phone and receives the verification code on the same device, the out-of-band channel is lost.

In order to circumvent the 2FA protection measure, malware authors have started to add mobile plugins for their Trojans. Through social engineering, attackers can trick the user into installing the Trojan on their mobile device. Once installed, the Trojan can forward any transaction code received by the device to the attacker. The text message is suppressed so that the user never sees the message. Some attackers have posted fraudulent one-time password generator applications for mobile devices on third-party app markets. Once the malicious app is installed, the user is prompted to input their account password. This act gives the attackers the information they need to defraud the victim.

In Europe, the misuse of multiple SIM cards has become another successful method for fraud. Telecos often allow their customers to order a secondary SIM card, which is often used in tablets. Unfortunately, attackers have taken advantage of this service to persuade telecom employees to send a secondary SIM card to an address of the attackers' choice. Other attackers used personal information gained through compromised computers to report the victims' original SIM card as stolen, letting the attackers order a new one. Once the attackers possess the new SIM card, they can issue fraudulent transactions through a Trojan on the victims' computer and then authorize the transaction using the cloned SIM card. This attack does not scale for broad stroke attacks, but is very effective for focused attacks.

Attacks outside of online banking

Cybercriminals also target financial institutions outside of online banking services. In the first half of 2013, financial institutions were the third most attacked sector by targeted attacks. Attackers have targeted some financial organizations with DDoS attacks as a distraction from other malicious activities. While the institutions' emergency response team is busy mitigating the low-volume DDoS attack, the attackers launch the real attack unnoticed. This could let attackers use stolen passwords to gain direct access to the institutions' back end server in order to conduct fraudulent transactions.

Bitcoin

The interest in Bitcoin — the decentralized digital currency — has grown substantially in 2013, particularly since the exchange rate for one Bitcoin rose to over $1000 in November 2013. But as any established method of payment, this cryptocurrency also sparked the interest of scammers. Over the last few years, malware authors have developed Trojans that steal from Bitcoin wallets. Many attackers have focused on stealing the local stored files of the offline wallet. Since quite a few people are using online wallets or accounts with online traders to store their Bitcoins, those services have become a target as well. Some attackers have started to use financial Trojans to steal passwords to access online Bitcoin wallets. There are also reports of a few direct attacks against Bitcoin trading platforms where the attackers successfully stole Bitcoins worth millions of dollars. We expect that attackers' interest in this digital currency will grow further, especially as Bitcoin's value is currently increasing and while the security of the online platforms stay at a weaker level compared to traditional online banking.

Symantec

CONCLUSION

> “As long as institutions persist with weak security measures, large-scale financial fraud will continue to be a lucrative enterprise for attackers.”

Conclusion

The world of financial Trojans is a thriving industry. In ten years, the state of online security has undergone significant changes to counteract these threats. Unfortunately, in many situations, security implementations adopted by financial institutions are inadequate to defend against the modern financial Trojan. 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 exploited by attackers. Strong security measures will deter attackers from pursuing these institutions in favor of vulnerable institutions where existing techniques are successful. As long as institutions persist with weak security measures, large-scale financial fraud will continue to be a lucrative enterprise for attackers.

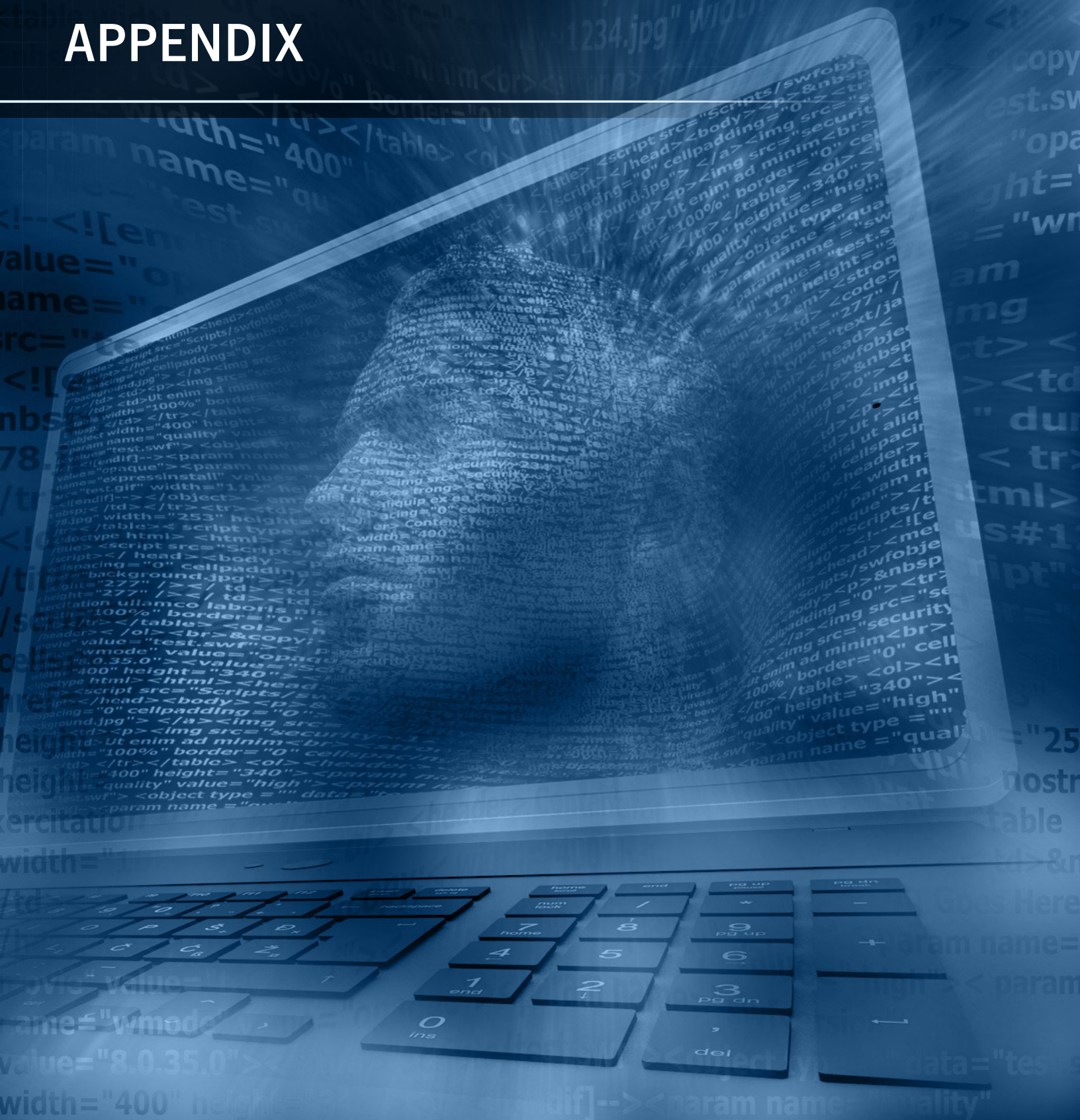
The financial fraud marketplace is also increasingly organized. It is a service industry where a wide variety of financial Trojans, Web-injects and distribution channels are bought and sold. Services on offer are dedicated to each aspect of a financial fraud campaign. These offerings will improve the effectiveness of established techniques. Location-aware distribution services will deliver payloads with precision, while third-party remote Web-injects are available to help circumvent security countermeasures. As a service, these remote injects enable the attackers to target a large array of financial institutions concurrently and intelligently. In a mix of focused attacks and broad strokes, attackers will continue to streamline their campaigns to maximize return on their efforts.

Attackers are also entering new markets, expanding operations and seeking out new targets where existing techniques can be applied. Regions such as the Middle East, Africa and Asia are being increasingly targeted. Areas with sizeable populations and wealthy residents are more tempting for attackers, such as Saudi Arabia, UAE, Hong Kong and Japan have recently come under attack. Cybercriminals are also exploring fresh institution types. In search of maximum return, attackers are now targeting high volume and high value transaction services: ACH in the US and, more recently, Single Euro Payments Area (SEPA) credit transfers in Europe. Proactive measures need to be taken to ensure that adequate security mechanisms are in place. Strong measures will deter attackers from targeting these institutions.

Ultimately, the end user is the eventual source of weakness during an online transaction. Even the strongest technologies are susceptible to social engineering attacks. Institutions need to be open about the risks and should continue to educate their customers about the security issues that they encounter. As more users adopt online banking to replace conventional in-branch or over-the-phone banking, banks must ensure that the user feels secure. 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 annually.

Symantec™

APPENDIX



Appendix

Notable Trojans

Tilon

This Trojan entered the scene in 2011 as a further development of a financial Trojan called Silon. In the summer of 2012, larger campaigns were seen using this Trojan. Tilon is a classic financial Trojan that uses MITB techniques on all major browsers to defraud victims. The Web-inject format is the same as the one used by the Zeus Trojan.

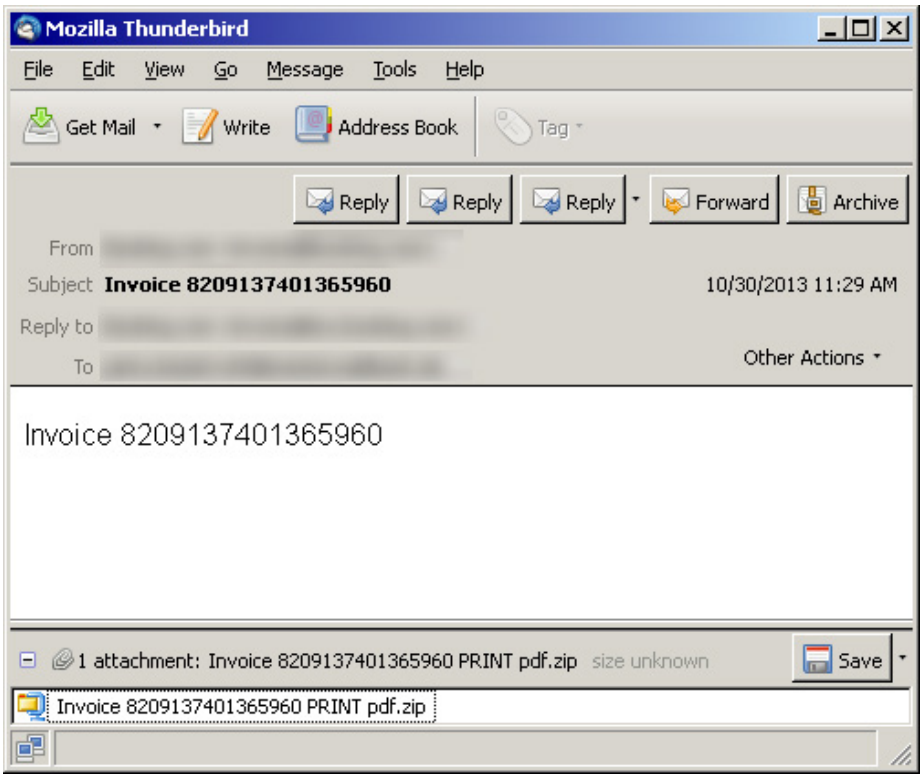


Figure 16. Spam email used to distribute Tilon

Tilon uses a focused approach, attacking only a few countries and institutions. The primary target is the UK, but it also focuses on Italy, the US, Australia and Canada. The Trojan is usually distributed through infected websites or spam emails. The attackers used spam emails with Downloader. Dromedan in multiple campaigns, with various social engineering techniques to trick users into clicking on the attachments. This downloader, which is shared among different groups, then downloads the Tilon Trojan on to the computer. More recently, the attackers started to spam out the Tilon Trojan directly without the use of a downloader.

Tilon uses various anti-sandbox and anti-reverse engineering techniques to slow down analysis. The samples contain between one and three hardcoded C&C server addresses and store some configuration data that is RC4 encrypted in the registry.

One of the latest campaigns, which was observed in October 2013, targeted Germany and used an invoice template in spam emails to distribute the Trojan.

Mebroot

The Mebroot family consists of a combination of different Trojans:

- Mebroot or Sinowal is the rootkit part of the Trojan, which was phased out in 2013.
- Litagody/Sinowal is the downloader component of the Trojan.
- Anserin/Torpig is the main user mode financial Trojan component.

For simplification purposes, we will refer to any sample of this family as Mebroot.

Mebroot is a very modular Trojan with typical MITB techniques for financial fraud. Configuration files are encrypted with RC4 or, in later versions, obfuscated with XOR. Mebroot was one of the first financial Trojans to make use of DGA in order to protect the attackers' C&C servers.

The first significant usage of Mebroot was in 2005, making it one of the older financial Trojans. Some early versions made use of a sophisticated rootkit, enabling it to infect the Master Boot Record and remain hard to remove. This rootkit functionality made the Trojan very stealthy once the threat was installed on a computer. With the widespread adoption of Windows Vista and Windows 7, the attackers decided to return to user mode components in 2011 in order to remain effective against newer computers. This move highlights the constant development of this Trojan and shows the level of sophistication of its authors.

The attackers distribute the malware through infected websites and spam emails. They often focus on a single country for a few weeks and then move on to different countries. Once a computer is infected, a smart network of proxy servers is used to distribute the matching payloads to the victim.

Gameover

Gameover is one of the most capable forks of Zeus. It appeared in July 2011, shortly after the leak of the official Zeus source code. It adopts the broad strokes approach and is typically distributed through high-volume spear-phishing campaigns that redirect to the Blackhole Exploit toolkit.

Once a computer is compromised, the Trojan waits until the user browses to a preconfigured URL. A typical user experience during a fraudulent transaction attempt is illustrated in the following image. In this example, an Italian bank was chosen, but the actual user experience will differ according to the institution targeted.

- A user visits a banking website whose URL is included in the Gameover configuration.
- Detailed host configuration data (including browser and hardware settings) is sent to the attacker.
- The login information is intercepted and form details, such as the user name, PIN and one-time password, are sent to the attacker while the user is presented with a "please wait" message.
- The attacker uses these details to log into the banking website.
- As the bank asks for additional questions, the attacker relays them to the victim.

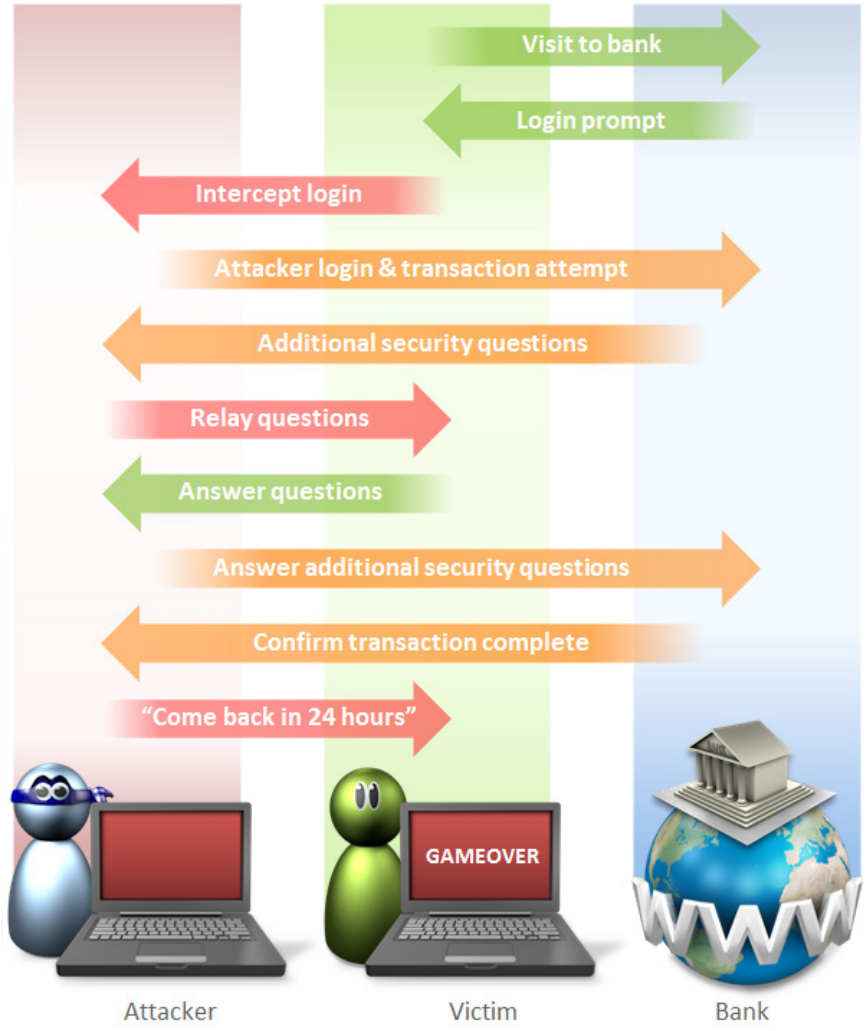


Figure 17. Typical user experience during a fraudulent transaction attempt

- The previous step is repeated until the attacker has enough information to complete the fraudulent transaction.
- Once the fraudulent transaction is complete, the user is shown an error message that asks them to return in 24 hours.

In this attack, detailed host configuration data is sent to the attacker to ensure that the attacker's setup is identical to the host computer. The attacker then proxies the connection through the user's compromised computer during the fraudulent transaction attempt. This serves to hide the attacker's IP address and may circumvent some anti-fraud detection measures that identify mismatched host configurations and suspicious IP addresses.

This example illustrates how modern banking Trojans have advanced capabilities for committing online bank fraud and how attackers are well aware of the security precautions behind online banking websites.

In November 2013, Symantec analyzed the Gameover P2P botnet distribution in more detail. By enumerating the peer list, we were able to identify computers infected with Gameover. The complete botnet is believed to be made up of hundreds of thousands of active bots.

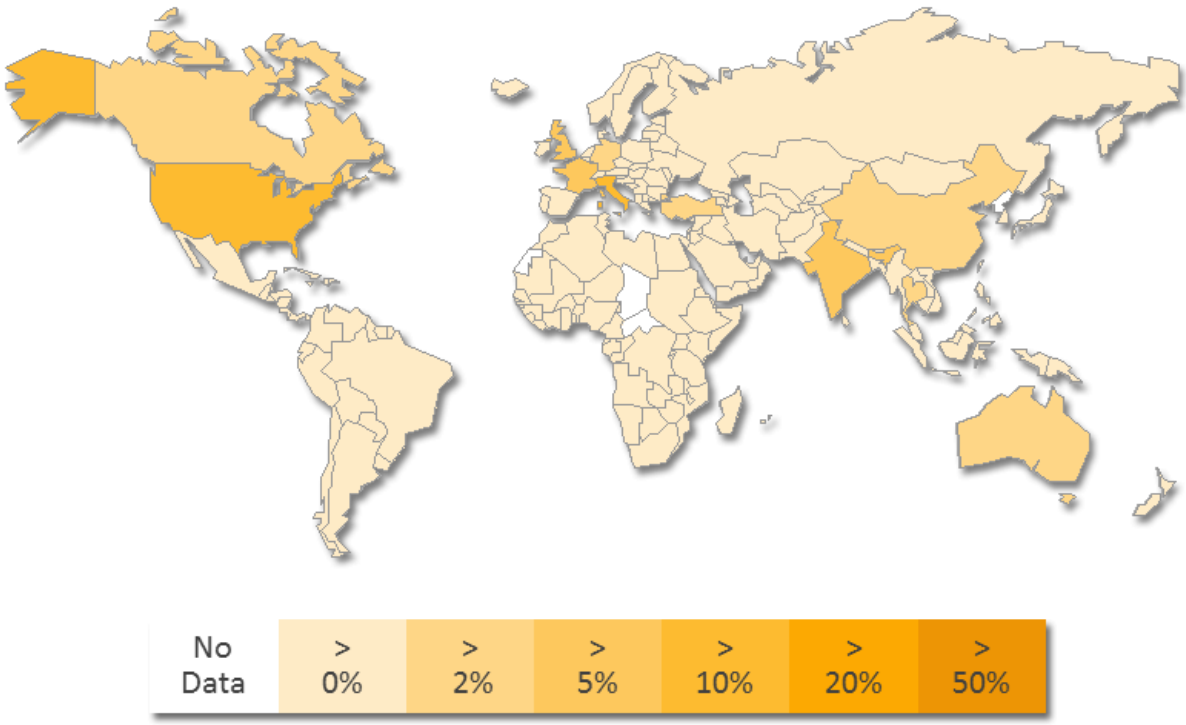


Figure 18. Worldmap of Gameover infected computers

Resources

"High Roller" Online Bank Robberies Reveal Security Gaps
http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

Members of the Largest Criminal Group Engaged in Online Banking Fraud are Detained
http://group-ib.com/index.php/o-kompanii/176-news/?view=article&id=627

Tatanga Attack Exposes chipTAN Weaknesses
http://www.trusteer.com/blog/tatanga-attack-exposes-chiptan-weaknesses

Threats to Online Banking
http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf

The World Distribution of Household Wealth, December 2006
http://www.wider.unu.edu/events/past-events/2006-events/en_GB/05-12-2006/

Trojan.Bebloh
http://www.symantec.com/security_response/writeup.jsp?docid=2011-041411-0912-99

Trojan.Carberp
http://www.symantec.com/security_response/writeup.jsp?docid=2010-101313-5632-99

Trojan.Shylock
http://www.symantec.com/security_response/writeup.jsp?docid=2011-092916-1617-99

Trojan.Spyeye
http://www.symantec.com/security_response/writeup.jsp?docid=2010-020216-0135-99

Trojan.Tatanarg
http://www.symantec.com/security_response/writeup.jsp?docid=2011-030106-5323-99

Trojan.Mebroot
http://www.symantec.com/security_response/writeup.jsp?docid=2008-010718-3448-99

Trojan.Tilon
http://www.symantec.com/security_response/writeup.jsp?docid=2012-111612-5925-99

Trojan.Hesperbot
http://www.symantec.com/security_response/writeup.jsp?docid=2013-090617-0331-99

Trojan.Zbot
http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

Zeusbot/Spyeye P2P Updated, Fortifying the Botnet
http://www.symantec.com/connect/blogs/zeusbotspyeye-p2p-updated-fortifying-botnet

W32.Cridex
http://www.symantec.com/security_response/writeup.jsp?docid=2012-012103-0840-99

Glossary

CAPTCHA: A CAPTCHA is a test that a human can pass but bots can't. They are used to prevent bots from registering or accessing accounts and posting spam.

Domain generation algorithm (DGA): Various families of malware often use algorithms to generate a large number of domains for the attacker. This makes it difficult for law enforcement agents to shut down botnets, as infected computers may only contact some of these domain names each day to receive updates or commands.

Drive-by-download: A drive-by-download happens when a malicious file or software is downloaded to a users' computer without their knowledge or consent. Often, attackers will compromise websites to host this malware, which could download onto the victim's computer in the background without their knowledge. This is often achieved using exploits for various software such as browsers and browser plugins.

Man-in-the-browser attackers (MITB)/Web-injects: MITB or Web-inject is an attack technique that involves an application hooking into the browser and manipulating data before it is displayed. The attacker takes advantage of functionality in the Web browser to insert additional forms fields onto the Web page. This allows the attacker to trick users into entering information that they would not normally be asked for such as the ATM card PIN when logging onto a bank website.

One-time password (OTP): OTPs are passwords that are valid for just one login session or transaction. OTPs can be generated in several ways, such as through hardware tokens or mobile apps.

Peer-to-peer (P2P): A peer-to-peer network is a decentralized network that relies on individuals nodes on the network, rather than a central server, to share resources.

Transaction authentication numbers (TAN): A TAN is used as a form of one-time password to authorize financial transactions. They act as a second layer of authentication, along with the user's password. There are a few different forms of TANs:

- **iTAN:** The user is asked to input a specific TAN as identified by an index that's randomly chosen by the bank. However, iTANs are susceptible to MITB attacks.
- **chipTAN:** This is a device that involves the use of a TAN generator that only works if the user's bank card is inserted into the chipTAN device.
- **mobileTAN (mTAN):** When a user attempts to conduct a transaction, the bank generates a TAN and sends it to the user's mobile device by SMS. The message may also include transaction data to allow the user to verify the nature of the transaction.

Two factor authentication (2FA): Two factor authentication requires the user to have two forms of authentication in order to log into their online accounts. Typically, the user must first input a password to attempt to login. The service provider will then send the user an authentication code as an SMS message, an email or to the user's app, which can be used as the second layer of authentication.

If you are unfamiliar with any other term this report uses, please visit the SecurityFocus glossary at http://www.securityfocus.com/glossary for more details on information security terminology.

Authors

Stephen Doherty
Senior Threat Intelligence Analyst

Piotr Krysiuk
Principal Software Engineer

Candid Wueest
Principal Software Engineer

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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.