THE TROJAN MONEY SPINNER

Mika Ståhlberg
F-Secure Corporation, Tammasaarenkatu 7, PL24, 00181 Helsinki, Finland

Tel +358 9 2520 0700
Email mika.stahlberg@f-secure.com

ABSTRACT

It is obvious that as more and more money moves online, criminals who want to steal that money are moving online as well. Since banks no longer have large sums of money in their vaults and bank robbery has several inherent risks, criminals have found a lucrative and a much lower-risk business in online crime. Email-based phishing has been the first echelon of this change, but the situation is already changing again.

Online banks have begun to improve their security and authentication methods. This will very much reduce the effectiveness of phishing that is based on emails and fraudulent sites. There is a clear demand for better solutions in the world of crime. The second echelon of online bank fraud is banking trojans. These trojans infect the computer of an online bank customer. The trojan has visibility to everything the customer does and can use his authenticated banking session to steal his money. Also, a key difference from email-based phishing is that the victim is doing nothing wrong; he is just going to his bank and doing his business, as he should.

These attackers are making a lot of money. Relatively few of them are caught, so the problem is only going to get worse. To better understand this problem and its size, we have implemented a new tool for analysing banking trojans. We have run this tool on thousands of recent malware samples to get an idea of how common these banking trojans are, the current trends, the geographical distribution of this problem, and what the targets are. This paper presents our findings.

WHAT IS A BANKING TROJAN?

In this paper when we refer to a 'banking trojan' we are talking about a piece of malware that targets the money from the account of an online bank. Certain other financial services such as online stock brokerage services are also considered 'online banks' in this context. Some papers have used the term 'phishing trojan' for almost the same thing.

Recently the term 'crimeware' has become commonly used to refer to banking trojans. In this paper we consider banking trojans to be a subcategory of crimeware. Crimeware refers to a more general group of malware that are designed to bring financial gains to their writer or distributor [1]. Crimeware therefore includes clickers, spam proxies, ransomware, and other malicious programs that are not interested in online banking *per se*.

HOW DO BANKING TROJANS WORK?

Filtering data

Trojans specifically designed to harvest banking information began to appear in mid-2004. Phishing gangs had used malware before that, but earlier it was mainly spam proxy and backdoor type of use – not harvesting banking credentials from compromised hosts. In 2004 these malware, or banking trojans if you will, also started to filter out keylogging data that was not related to the banking session. Traditional keylogging and data harvesting produces a lot of data and mining that data requires a lot of effort. By filtering out as much as possible the operation of the 'bank robbers' becomes more efficient. Typically the filtering is done based on the URLs the user accesses. [2]

In order to focus on specific sites banking trojans typically contain, or download from a control server, a list of filter strings. These filters are banking strings such as parts of bank URLs (e.g. 'www.citibank.com' or '/TAN/') or dialog title strings (e.g. 'Welcome to Citi'). The trojan monitors activity on the system and jumps into action only when a filter string is detected.

Some banking trojans have a huge list of banks. For example, Bancos.NL [3] includes 2,764 different bank URLs from over 100 countries. However, when looking at the list of banks we can easily see sites that are not really online banks (e.g. Bank of Finland, which is not a customer service bank) and banks that already at the time of the release of the trojan did not use single factor authentication – authentication that could be subverted with the techniques employed by Bancos.NL. Bank account balance and other sensitive information would be compromised, yes, but that was hardly the goal of the attackers.

How do they know when the user has gone to a site?

As said, banking trojans filter out useless data – or more precisely, they only capture interesting data from banking activity. This means that the trojan has to know when the user is banking online. It is very common for the trojan only to monitor what the web browser is doing and where it is going. Banking trojans today use the following means of determining where the user is surfing:

- Hooking (e.g. inline hooks on WinInet API functions)
- BHO (Browser Helper Object) interface [4]
- Window title enumeration (e.g. FindWindow() [5])
- DDE [6]
- Other COM (Component Object Model) / OLE (Object Linking and Embedding) interfaces
- *Firefox* browser extensions
- LSP (Layered Service Provider) interface [7]

As a fairly conventional example, Banker.ark [8] steals logon credentials related to some Brazilian banks by logging keystrokes when the internet browser title bar contains a string that is on its filter list.

How do trojans spy on the data?

After the trojan has determined that the user is accessing a banking site, it tries to capture the user's credentials or his authenticated banking session. Trojans use the following techniques:

- Form grabbing
- Screenshots and video capture
- Keylogging

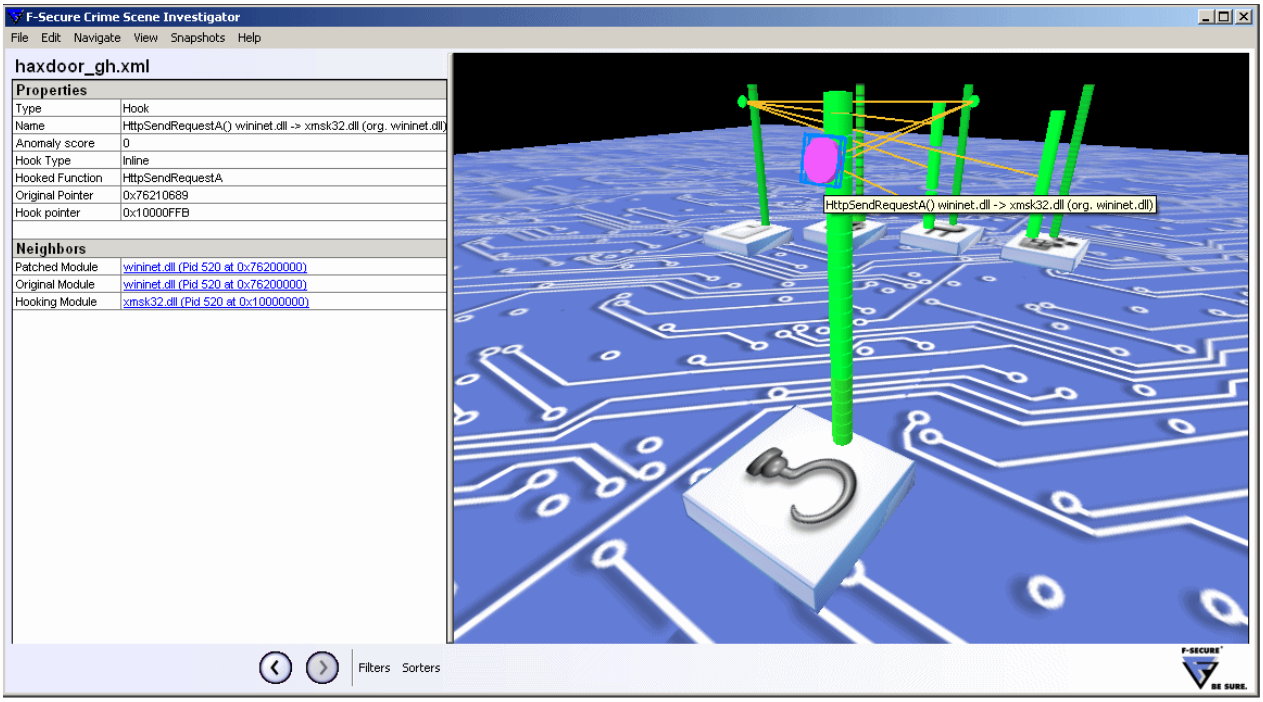

Figure 1: An analysis tool showing that Haxdoor.gh (xmsk32.dll) has hooked HttpSendRequestA() in IE process. The trojan does this in order to spy and redirect online banking connections. The relations in the view also show that xmsk32.dll has a registry launchpoint (in this case a Winlogon notify routine).

- Injection of fraudulent pages or form fields
- Pharming
- Man-in-the-middle attacks

As an example of the HTML injection techniques, some banking trojans monitor the sites a user accesses and then display fraudulent web pages when they see that the user has entered an interesting site. One such trojan is Sinowal.cp [9], discovered in March 2007. When Sinowal is activated on a compromised system, it contacts a control server controlled by the attacker. The server provides a list of banking sites the trojan then starts monitoring. When a monitored site is hit, the trojan displays fraudulent web pages delivered from the control server instead of the real bank pages.

Traditional man-in-the-middle (MitM) attacks against online banking are based on a fraudulent website that modifies and relays traffic between the user and the server. Sometimes man-in-the-middle attacks that take place between the user interface and the security layer (e.g. encryption) of a browser are called 'man-in-the-browser' (MitB) attacks. Trojans can perform MitB attacks either by showing the user fraudulent content, modifying content received from the server, or by modifying data the user enters to a form before it is sent to the server. [10]

How does the money get stolen?

Haxdoor.ki was spammed with German and Swedish emails in August 2006 [11]; obviously the targeted banks are in German and Swedish-speaking areas. The case became famous in the media in January 2007 since the trojan caused major financial losses [12]. It collected usernames, passwords, and PINs. A trojan like this typically displays an error message after the user has entered his password. The trojan then sends the information to the attackers and they can use the authentication credentials again since the bank has never actually seen them being used.

Many banking trojans steal usernames, passwords, transaction numbers (TAN), or one-time-passwords (OTP) and send them to a server managed by the attacker. The attacker can then log into the online bank and place a transaction to send money to an account belonging to himself or more likely to a hired money mule. Banks can prevent these kinds of attack by using passwords from the password list in random order, monitoring for anomalous web access, etc.

As more and more banks are starting to use multi-factor authentication, attackers must either concentrate on the lowest hanging fruit, i.e. banks that do not yet have the latest and greatest security mechanisms in place, or they will have to come up with attacks that go beyond just stealing passwords. On the other hand, many banks e.g. in the US are still not

001	~~2455~~	021	2455	041	6210
002	~~4389~~	022	4389	042	3981
003	~~8953~~	023	8953	043	6292
004	~~0583~~	024	0583	044	0459
005	~~3281~~	025	3281	045	2027
006	~~1049~~	026	1049	046	4338
007	~~7281~~	027	7281	047	3221
008	~~2988~~	028	2988	048	1059
009	~~9723~~	029	9723	049	3758
010	~~2589~~	030	2589	050	2332
011	7043	031	7043	051	3355
012	2801	032	2801	052	2424
013	1974	033	1974	053	9383
014	5543	034	5543	054	1022

Figure 2: A typical OTP (one-time password) scheme used by European banks. The customer gets a list of passwords. Each password is used only once.

using one-time-passwords or other stronger authentication mechanisms. This makes them vulnerable even to conventional keyloggers and email-based phishing.

There is an ongoing arms race between banks and trojans. Some banks have deployed new security mechanisms such as virtual keyboards. Trojans have responded. Many banking trojans perform screen or video capture to bypass virtual keyboards [5, 6]. Some banking trojans, like Nuklus.a [13] and Sinowal.cp [9] collect certificates from the system certificate storage. The most likely aim for this behaviour is to bypass the authentication of banks using client-side certificates [14].

What are the consequences for the customer of an online bank if money is stolen from his account? He might get his lost money back from the bank. However, he can lose a lot of personal data as well and that loss cannot be undone. Therefore, this kind of online crime is a very concrete threat to all computer users. Banks have reached the threshold where online banking is the norm. This is good for the banks because it reduces costs. However, this also means that not all online banking users are early adopters any more – many online banking users are not very computer savvy. The people who are at the greatest risk of getting infected by a banking trojan are also the people who will have the biggest problems learning how to use multi-factor authentication or any of the other new security measures deployed to keep them out of harm's way.

Local session riding

The world of banking trojans is moving from stealing credentials into stealing authenticated sessions [15]. If a trojan gets administrator level privileges on a system, even a two-factor authentication system will not protect against the trojan using an authenticated session to post or modify transactions [16]. The term 'local session riding' has been coined for this sort of attack [14]; the term 'session hijacking' is also commonly used for the same thing.

The problem essentially boils down to the fact that a browser within the personal computer of a customer is in fact a banking terminal. The user cannot tell whether or not the terminal shows him everything that is happening and the bank cannot really tell if everything they receive actually came from the user. The problem is actually very similar to what has been recently discussed around the security of electronic voting and what would happen if a voting terminal is compromised [17].

In session riding the malware can either replace transactions (e.g. '$200 to John Doe' changed to '$999 to D.B. Cooper') or add completely new transactions. Once the transaction is in place, the attacker can walk into a bank and withdraw the cash. Of course, criminals are not using their own identities or bank accounts to collect stolen money. Catching them once the money has been withdrawn can be a daunting task.

How does form grabbing work?

Keylogging is not a very effective way of collecting online banking data. If the malware logged everything the user typed, the attacker would end up with a whole lot of useless data without any proper structure. For this reason, from the beginning of 2003 form grabbing has been the method of choice for collecting banking data [2]. Form grabbing refers to the trojan only capturing data that is submitted out of the system when filling out a web form. After all, sensitive details the user types into an online banking session end up in a form field.

Common form-grabbing techniques include Browser Helper Objects (BHO) [18], COM interfaces (e.g. IWebBrowser2) [19, 20] and API hooking. The problem with these of techniques is that the trojan can access the data before it is encrypted using SSL. While most of these form-grabbing methods only work against *Microsoft Internet Explorer*, the problem is not strictly limited to *IE* users. We have also seen the first malware to use *Firefox* browser extensions for form grabbing [13, 14, 20] and e.g. Haxdoor.gh can also grab data from browsers by hooking the generic GetDlgItemTextA function.

Haxdoor is a good example of a banking trojan that uses API hooking for form-grabbing purposes. We first analysed Haxdoor samples during our *BlackLight* rootkit detection research [21]. Haxdoor is a rather advanced 'malware as a service' type of kernel-mode rootkit that uses SSDT hooks in order to hide. We were puzzled by the fact that it injects code from the kernel to user-mode and hooks functions there. It did not seem to make sense since the kernel is all-powerful in itself. Things started to add up when *Secure Science* published a paper [22] explaining how, in this way, Haxdoor gets to eavesdrop and modify data before it is encrypted using SSL.

The same techniques that are used for grabbing data can also be used for replacing data. Many trojans (e.g. Sinowal) show fraudulent web pages made to look like the real bank site. After the user has filled in the fake form with his credentials the trojan will show an error dialog and send the data to the attackers. This technique has become very common in Brazil lately [23]. A Banker variant (Banker.cjm) we analysed included 132 jpg images of forms, fields, virtual keyboards, buttons, and dialogs of Brazilian banking sites.

Some banking trojans extend the standard form-grabbing technique by modifying pages on the fly. For example, for skimming ATM cards criminals may want to know the ATM PIN of the user. However, normal bank sites do not contain an input box for that piece of information. Some trojans add this input box dynamically to the actual banking page when the user enters the site. For example, Sters (a.k.a. Briz) trojans allow the criminal to collect social security numbers and other personally identifiable information (PII) in this way [24].

Pharming

Some banking trojans redirect the user logging onto an online bank to a malicious website. This kind of an attack is called pharming. The malicious website can either pretend to be the bank site or it can act as a man in the middle, modifying and relaying traffic between the bank site and the user's browser. Pharming can be accomplished using a number of different techniques.

For example, the trojan can add bank site names to the hosts file with an IP address pointing to a malicious site – Qhost.je is a good example of such a trojan [25]. Another common technique is to hook wininet.dll functions in the *Internet Explorer* process. Some Haxdoor variants (e.g. Haxdoor.gh from January 2006) have this functionality, but not all. Apparently pharming is an add-on feature in the Haxdoor generator and not all 'customers' have chosen to buy or activate it – for example Haxdoor.ki from August 2006 does

not have this functionality enabled.

While most users would probably just ignore the SSL certificate warning when connecting to a fraudulent banking site, the malware authors can work around these warnings. A banking trojan that does pharming by hooking wininet.dll functions in a browser is also quite capable of bypassing or suppressing any warning dialogs [22]. Also, a trojan modifying the hosts file or doing something else to the system could also install its own root certificate, thus preventing any warnings about untrusted sites [14].

MSTRINGS: A TOOL FOR ANALYSING BANKING TROJANS

So, that is how they do it. How can we fight this threat then? How can banking trojans be analysed? How can we categorize them and find which banks are being targeted?

We studied banking trojans and ended up with the following facts:

1. Trojans must use filter strings in order to reduce the amount of data they collect (this is explained well in [2]).
2. Filter strings are banking strings – typically bank URLs.
3. Malware that is not interested in banks does not include banking strings.
4. Banking trojans typically encrypt or obfuscate their filter strings within the file image, but decrypt them into memory.

This led to the idea that we could run collections of malware, running samples in a test system and search the memory of the system for banking strings. If the memory contains banking strings we would collect them in a database and analyse them for trends and other statistical purposes. The same technique could also be used for locating banking trojans from incoming samples in lab automation.

We created an analysis tool called 'Mstrings' for this purpose. Mstrings is an *F-Secure* internal research tool that currently has the following set of features:

- Has a database of search strings (currently contains 1,400 search strings).
- Can search through user-mode and kernel-mode memory.
- Can bypass basic forms of string encryption automatically.
- Has a whitelist for false positive strings.
- Is rather fast. With the current database, it goes through all required areas in memory in 10–30 seconds.

Figure 3: Test arrangement. Trojans were installed one-by-one on a test machine and Mstrings was run. The results were stored in a database.

RESULTS OF THE MSTRINGS RUNS

We chose a malware collection and took a set of PE (.dll, .exe, .sys) malware samples from October 2006 to December 2006. The set we used did not include spyware samples, scripts, etc. The samples were in no way handpicked, thus the ratio of banking trojans to other types of malware should be fairly realistic for that period.

We ran all of these files through the analysis system (Figure 3). Only sample files that were successfully run on the system were included. We ended up including 5,244 samples in the results. Out of this sample set, Mstrings tagged the samples listed in Table 1 to be targeting banks.

Interestingly, three online game trojan families, Magania, Nilage and OnlineGames, combined ended up having 1,029 sample files in the set, while Bzub, Banbra, Banker, Bancos, Haxdoor, Sters, and Sinowal together had 180 files. This speaks volumes about the rise of malware targeting online gaming. On the other hand, we could think of virtual commodities and currencies as being just another form of banking. Stealing virtual money or a troll-slaying axe in the virtual world and converting that to real-world money does not differ that much from stealing money directly from the player's bank account.

Family	Samples
Banker	50
Bzub	21
Banbra	4
Bancos	3
Delf	3
Qhost	2
GrayBird	1
Haxdoor	1
PcClient	1
Sinowal	1
VB	1

Table 1: Number of samples targeting banks tagged in the sample set. As can be seen Banker was by far the largest family of banking trojans.

We did an analysis of which banking establishments were being targeted by malware and compared that to brands being targeted by email-based phishing. *PIRT* top 20 from July 2006 [26] was used as the comparison data of brands targeted by email-based phishing. This comparison showed that while email-based phishing in 2006 had its sights on *PayPal*, *eBay* and US banks, the target selection of trojans is somewhat different. Top targets for trojans from late 2006 were Brazilian banks, *e-gold*, and Western European banks.

Figures 4, 5 and 6 present further results of the analysis runs.

Since the sample set contained very few samples of the typical trojan families targeting European banks, we also took 414 Haxdoor executables (from 2004 to 2007) and ran those on the system as well. Figure 7 shows the geographical target distribution of these Haxdoors. Out of the 414 samples, 321 were targeting banks, while the rest were just plain backdoors. Haxdoors that targeted banks were on average targeting 34.7 banks. From the results it was also apparent that there was a dramatic drop in the number of new Haxdoor variants in October 2006 and that the number of new variants has remained low ever since.

ACCURACY OF THE RESULTS

There are a number of factors that will affect the accuracy of the results:

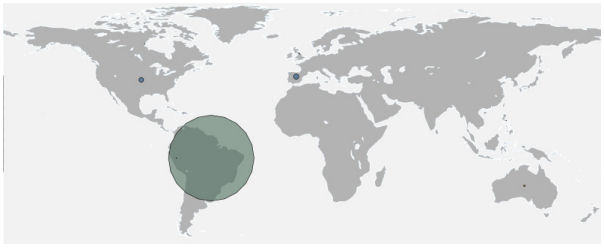

Figure 4: Geographical target distribution for trojans of the Banker family. It is fairly apparent from the map that the Banker family targets Brazilian banks. As Banker was also the largest banking trojan family found in the sample collection, this result has also implications on the overall global distribution of these attacks. (Coordinate information source: CIA World Factbook.)

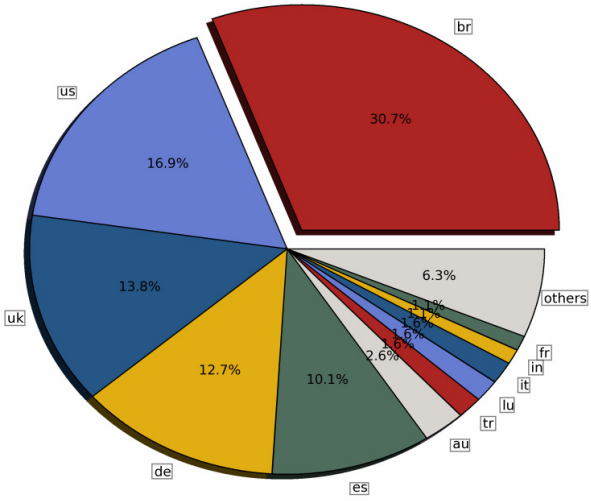

Figure 5: Geographical distribution of the banks targeted by banking trojans in the analysed sample set. Almost a third of banks targeted by banking trojans are from Brazil.

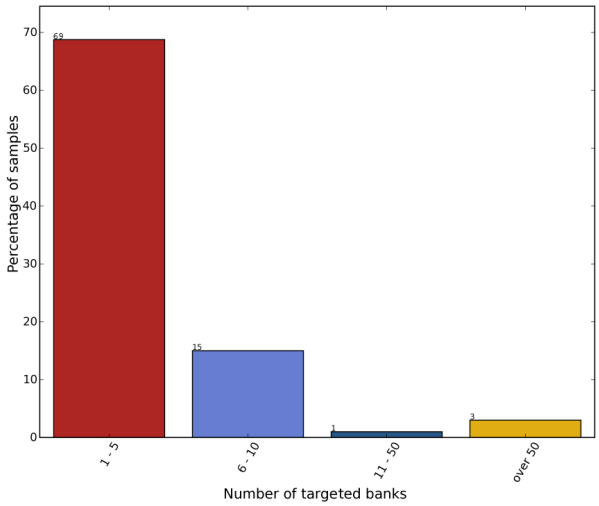

Figure 6: Most banking trojans seem to have a fairly focused set of targets. They are not really interested in more than a few banks and the customers of those banks. In particular, banking trojans targeting Brazilian banks fell into the leftmost category.

Filter strings downloaded from a control centre

Not all banking trojans contain banking strings in the binary itself. This seems to be a growing trend as many of them download filter strings or binaries containing these strings from servers on the internet. One example is Sinowal.cp [9], which contains only part of the strings in the binary – the rest is downloaded from a website. Our test environment was not connected to the internet so we have missed some relevant banking strings. In order to be effective in these cases Mstrings would have to be run on a machine that has an internet connection and while the control server is still up.

Banking strings that are not filter strings

Some malware might not be directed against a bank, despite containing bank names. Our initial configuration had some false positives. Even though we improved the configuration and logic significantly, some false positives might still remain – this should have only a very marginal effect on the results, though.

Strong encryption

While most banking trojans do not encrypt banking strings in memory and Mstrings does have the capability of handling some basic encryption methods, it could be that some strings have been missed due to encryption.

Targeted branch office listed under head office

Some banks are global. For example, if a malicious program is interested in the string 'Santander', it is very difficult to directly tell if it is the head bank or a local branch that actually is being targeted. Of course, if the trojan targets five Brazilian banks and 'Santander' it is fairly obvious that it is actually 'Santander Banespa' from Brazil that is being targeted and not the Spanish head bank.

Malware run was not set up properly

While the run was performed against 5,244 PE samples, these included many dlls, drivers, and others that were not standalone malware components. We did try, for example, to run all DLL samples using rundll32.exe, but in many cases the sample will not produce the correct results. We would

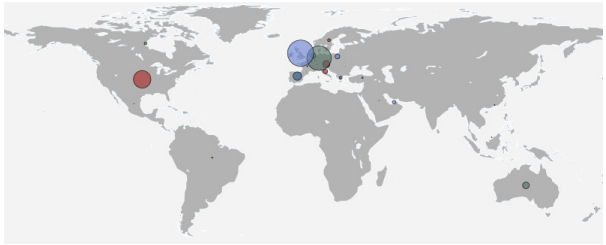

Figure 7: As can be seen from the diagram, the target distribution of Haxdoor family is very much different to Bankers (see Figure 4). We calculated how many Haxdoors targeted a bank. Individual banking establishments from a particular country were then added together. This resulted in 2,340 hits for the United Kingdom and 2,183 hits for Germany, for example. Haxdoor target distribution is quite scattered and even Finland got three hits. (Coordinate information source: CIA World Factbook.)

have needed to collect all files that belonged to a particular malware and run them together. Due to how sample acquisition and collections work, it was not feasible to do so in this magnitude. Also, it is possible that some of the samples we ran did not run correctly due to the environment. However, we did make every effort to prevent malware from detecting that it was not running on a normal host.

While it is clear that the results have a relatively big margin of error for the reasons presented above, the sheer number of samples should guarantee some value for the results. The results are statistical and should show pretty well the direction that banking trojans have taken.

CONCLUSIONS

Basically there are two kinds of banking trojans: Brazilian ones and the rest. In late 2006 banking trojans seem to be a pretty Brazilian phenomenon. 30.7 per cent of banks targeted by banking trojans were Brazilian banks. Most of the trojans targeting Brazil belonged to the Banker and Bancos families.

Typically trojans targeting Brazilian banks target only five or fewer banks. Trojans that target Europe or USA usually target both and tend to have many more than five targets. In the collection we analysed there were very few banking trojans targeting Asia or Africa. Australia did get some hits.

It is interesting to note that Brazil was the most targeted country by the number of banks even though a typical Banker or Bancos variant targets only three to four banks. This means that the focus on Brazil is even tighter than shown in Figure 1. There were 88 samples tagged as banking trojans out of the total of 5,244 sample files in the sample set. The Brazilian-focused Banker family alone accounted for 50 samples.

On the other hand, trojans of the Banker and Bancos families are malware that include their filter string inside the main executable. Haxdoor (a.k.a. A-311 Death), Sinowal (a.k.a. Torpig, a.k.a. Anserin), Nuklus (a.k.a. Apophis), Bzub (a.k.a. Metafisher), Snatch, and Sters (a.k.a. Briz, a.k.a. VisualBreeze) are mainly targeted against European, Australian and North American banks. This could change, of course, since these trojans are typically customizable 'malware as a service'. Some of these trojans download their filter strings or filtering components from the web. Since our test system did not have access to the internet, the results are skewed towards Banker-style trojans. However, there were only four Sters sample files in the non-selectively chosen sample set, for example.

Banking trojans targeting Brazilian banks typically do not use hooks or Browser Helper Objects. They seem to rely on *Windows* APIs (e.g. FindWindows()) and DDE in spying on *Internet Explorer* use. One probable reason for this is that Brazilian banks tend to use Java applet based virtual keyboards. Screenshots, video capture, and injected web pages are therefore the attack methods of choice for these trojans. Trojan families that have a European focus (e.g. Haxdoor and Sinowal) very commonly use wininet.dll hooks. There were no banking trojan samples using LSP in the sample set.

Currently it seems that, while US banks are very much being targeted by email-based phishing, Brazilian and some other banks are being targeted more by malware than the more conventional phishing attacks. This is supported by the fact that CERT.br reports [27] that, while email-based phishing was very common in Brazil in 2002 and 2003, it is nowadays very rarely seen and online fraud is based on malware.

Why are banking trojans so common in Brazil? Actually, malware in general is a big problem in Brazil – not just banking trojans. Brazil has a large population of which an ever-growing part is now going online. As there is a constant flow of new computer users, mass social engineering attacks are very successful in compromising users' machines. [23]

The APWG report from April 2007 [28] shows that only 2.33% of banking trojan sites are in Brazil. According to CERT.br's report [29], while Banker and Bancos trojans take the lion's share (50.77%) of their malware notifications, only 7.58% of IP addresses hosting these trojans in 2006 were in Brazil. This means that Brazil does not really stand out as a target if we only consider the download sites hosting malware – we also need to look at where the targets are.

Banking trojans targeting Brazilian banks are typically not targeting any banks outside the country. This is fairly natural, since the gangs making and distributing these trojans are local, they do not seem to have any connections to international criminals, and they usually come from a very poor background. This means that crime, for them, is a way to make an income and they do not really know that much about the international banking system. Even if these gangs would get their hands on overseas banking credentials they would not know how to use that information. [23]

There is one consideration that needs to be kept in mind when interpreting the results: the fact that a bank is being targeted does not mean the attack is successful. Several trojans target hundreds of banks and it is fairly apparent that sometimes the attackers are just trying their luck at banks they do not really know to be vulnerable to their methods. It may be that the attackers target a huge list of banks in order to see which customer group they manage to infect and then update their trojan or their configuration to perform a targeted attack against those particular banking systems.

The Mstrings approach to banking trojan analysis and detection seems feasible for the moment. Most current banking trojans can be detected solely based on the fact that they include filter strings. Especially if the analysis system has access to the internet, this approach can be used to analyse incoming malware samples. An alert can be sent to targeted banks and this can be done automatically.

REFERENCES

[1] The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond. A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October 2006. http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[2] Lance, J. Phishing Exposed. Syngress. 2005.

[3] Bancos.NL a.k.a. agent.aa. Malware description. http://www.f-secure.com/v-descs/agent_aa.shtml.

[4] Trojan-Spy.Win32.BZub.bl. Malware description. http://www.f-secure.com/v-descs/bzub_bl.shtml.

[5] New technique against virtual keyboards. Hispasec / VirusTotal. 26 September 2006.

http://www.hispasec.com/laboratorio/New_technique_against_virtual_keyboards.pdf.

[6] Banking trojan Captures User's Screen in Video Clip. Hispasec / VirusTotal. 05 September 2006. http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf.

[7] Gozi Trojan. SecureWorks. 20 March 2007. http://www.secureworks.com/research/threats/gozi/?threat=gozi.

[8] Banker.ARK. Malware description. http://www.f-secure.com/v-descs/banker_ark.shtml.

[9] Trojan-PSW:W32/Sinowal.CP. Malware description. http://www.f-secure.com/v-descs/trojan-psw_w32_sinowal_cp.shtml.

[10] Gühring, Philipp: Concepts against Man-in-the-Browser Attacks. 16 June 2006. http://www.it-observer.com/pdf/dl/concepts_against_mitb_attacks.pdf.

[11] Haxdoor.KI Being Spammed. F-Secure weblog. 17 August 2006. http://www.f-secure.com/weblog/archives/archive-082006.html#00000951.

[12] Swedish bank hit by 'biggest ever' online heist. ZdNet. 19 January 2007. http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm.

[13] Trojan-Spy:W32/Nuklus.A. Malware description. http://www.f-secure.com/v-descs/trojan-spy_w32_nuklus_a.shtml.

[14] Wüest, C.: Advances in phishing malware 'the enemies within'. In proceedings of the 16th Virus Bulletin International Conference 2006.

[15] Information Security Situation Report 2/2006. 03 July 2007. CERT-FI. http://www.cert.fi/attachments/5mfKbZPac/5mW6gPJ6O/Files/CurrentFile/CERT-FI_situation_report_2-2006.pdf.

[16] Schneier, B. Two-Factor Authentication: Too Little, Too Late. April 2005. http://www.schneier.com/essay-083.html.

[17] Hursti, H. Diebold TSx Evaluation. A Black Box Voting Project. 11 May 2006. http://www.blackboxvoting.org/BBVtsxstudy.pdf.

[18] How Internet Explorer could drain your bank account. CNET Reviews. 02 Jul 2004. http://reviews.cnet.com/4520-3513_7-5142439-1.html.

[19] Win32.Grams E-Gold Account Siphoner Analysis. LURHQ Threat Intelligence Group. 04 November 2004. http://www.lurhq.com/grams.html.

[20] Hayashi K. A fortune fox hunter. Virus Bulletin. November 2006.

[21] Kasslin, K.; Ståhlberg, M.; Larvala, S.; Tikkanen, A. Hide'n Seek Revisited – Full Stealth is Back. In Proceedings of the 15th Virus Bulletin International Conference 2005.

[22] Emerging Threat Center Malware Analysis Report v1.1. Secure Science Corporation. 02 February 2006. http://ip.securescience.net/advisories/SSC_MSAT_FEB_02_2006-public.pdf.

[23] Montanaro, D. Email interview. 22 May 2007.

[24] Alperovitch, D.; Judge, P. Phishing trojan creation toolkits: an analysis of the technical capabilities and the criminal organization behind them. In Proceedings of the 16th Virus Bulletin International Conference 2006.

[25] Trojan:W32/Qhost.JE. Malware description. http://www.f-secure.com/v-descs/trojan_w32_qhost_je.shtml.

[26] PIRT Top 20+ July Phished Brands. CastleCops. 03 August 2006. http://www.castlecops.com/a6628-PIRT_Top_20_July_Phished_Brands.html.

[27] Hoepers, C.; Steding-Jessen, K. Financial Fraud Response in Brazil – Challenges and Evolution. CERT.br. Collaboration Meeting for CSIRTs with National Responsibility. July 2006. http://www.cert.br/docs/palestras/certbr-fraud-national-csirts-meeting2006.pdf.

[28] Phishing Activity Trends report. Anti-Phishing Working Group. April 2007. http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[29] Hoepers, C. Crimeware Related to Brazilian Frauds. CERT.br. APWG 2006 General Meeting. November 2006. http://www.cert.br/docs/palestras/certbr-apwg2006.pdf.