G DATA

TRUST IN
GERMAN
SICHERHEIT

G DATA
SECURITYLABS
MALWARE REPORT

HALF-YEAR REPORT
JANUARY – JUNE 2014

CONTENTS

AT A GLANCE

- The number of new malware types remains at the same level as previously: the first half of the year saw the appearance of 1,848,617 new signature variants.
- Since 2006, G DATA SecurityLabs has recorded 15,197,308 new malware types.
- Statistically, a new malware type is discovered every 8.6 seconds.

- The number of new malware variants in the adware category continued to increase steeply. Attackers use tactics such as unsolicited display advertising to earn a lot of money for little effort.
- In the evaluation of attacks recorded on PC users, malware in the adware category is at the forefront as well. The SwiftBrowse family is prominent here for the wrong reasons, its 34 variants being responsible for almost two thirds of all MII reports in the half year.
- On the other hand, the number of new rootkits dropped. This sustained trend is due, among other things, to improved defence mechanisms in 64-bit systems.

- Since the beginning of March, a newcomer in the banking sector called Vawtrak has held the top spot among the most frequently detected banking Trojans.
- Malware in the Cridex family has also been conspicuously active during the past half year, with a derivative called Swatbanker.
- In May 2014, a new all-time high was recorded in the detection figures for banking Trojans.
- According to a G DATA survey, Bank of America was the most frequent target for attacks by banking Trojans, followed by PayPal and Citibank.
- At least 825 different targets were attacked by banking Trojans in total.
- The banking Trojans were principally targeting banks and payment service providers in English-speaking countries. Of the 25 most frequently attacked targets, 48% came from the USA, 24% from the United Kingdom and 16% from Canada.
- 40% of the 25 most common targets were susceptible to conventional keyloggers using the target's obligatory security measures; 80% were susceptible to banking Trojans that are able to manipulate transactions without the user knowing.

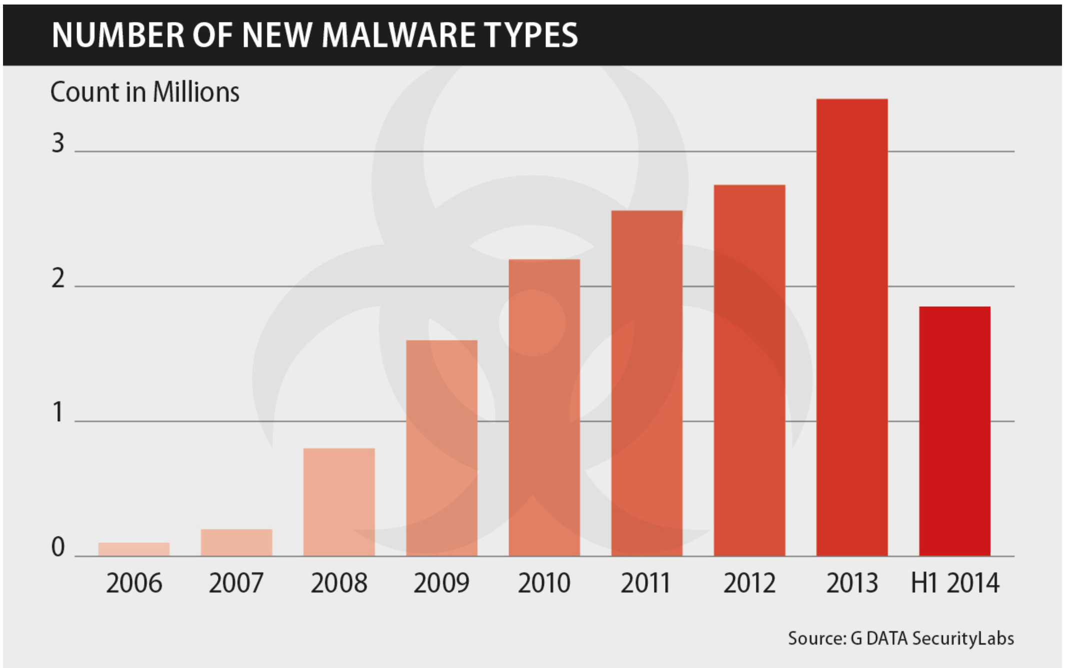
Forecasts and trends

- The signs continue to point towards growth. By the end of 2014, the 3.5 million mark for new types of malware in a single year will have been exceeded.
- The adware sector has become very established among attackers, and its malware will continue to pester computer users with unwanted display adverts in the future.
- Banking Trojans are a very lucrative business and have become a fixed factor in the underground economy. Hence the development of banking Trojans will continue to be very dynamic in the second half of the year.

MALWARE PROGRAM STATISTICS

During the first six months of 2014, G DATA SecurityLabs recorded 1,848,617 new malware types[1]. This means that the value is almost the same as for the previous half year (1,874,141), with a minimal drop of 1.38%. However, in spite of this, there was a significant increase overall in the potential for attacks on computer users of course.

A review of the figures since 2006 shows that more than 15 million new types of malware have appeared during the last 8.5 years. In purely statistical terms, this means that, throughout this entire period, a new malware variant was recorded every 20 seconds! However, the rate has increased significantly, as the following illustration shows. In the first half of 2014 alone, the statistical number for new discoveries dropped to just 8.6 seconds. That means over 10,000 new malware types per day (10,327)!



Source: G DATA SecurityLabs

Categories

Malware programs are classified on the basis of the malicious actions that they execute in an infected system. A look at these categories enables an assessment to be made on the attack methods cyber criminals are currently focusing on. The most important categories are shown in the figure on page 4. However, it should be noted in principle that a high number of new malware types does not necessarily imply high risk or quality, as demonstrated by **adware** for example. Equally, a low number of new signature variants does not indicate low quality or an absence of risk, as can be seen with **rootkits** and **exploits**. The number of new signature variants for **rootkits** and **exploits** dropped to less than 1,000 during the past half year.

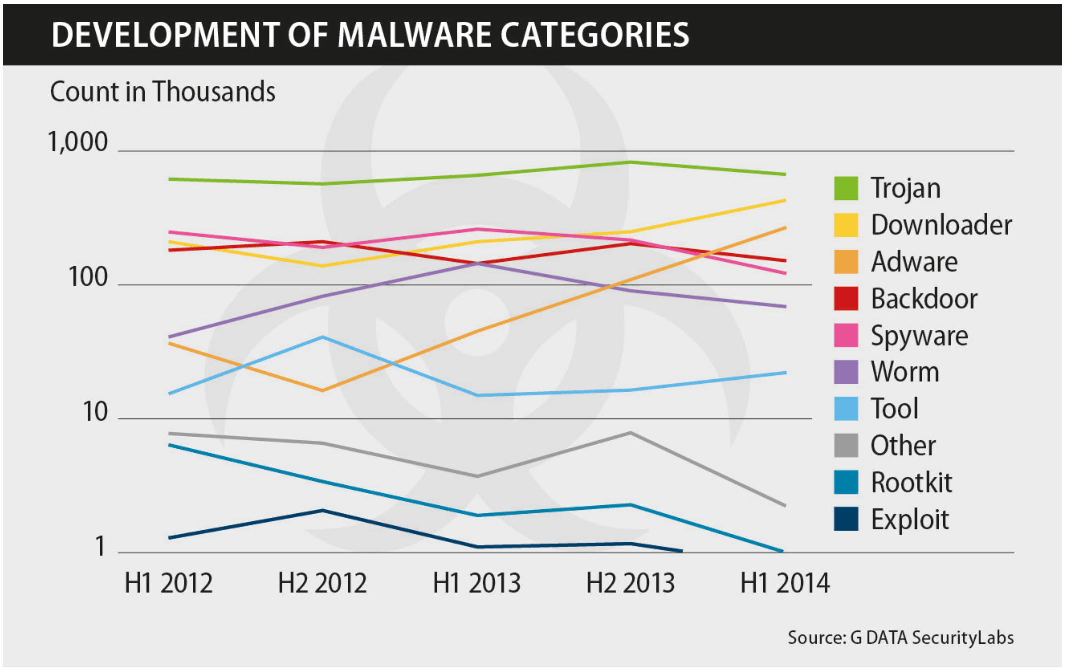
The use of **rootkits** in particular has changed significantly during the past year, as attacks have become significantly more difficult for these masters of disguise following the conversion to 64-bit operating systems. One of the protection measures introduced with the new Windows OS generations is kernel patch protection.[2] Circumventing this has long been difficult, even for malware authors. One example for removing precisely this

[1] The figures in this report are based on the detection of malware using virus signatures. They are based on similarities in the code of harmful files. Much malware code is similar and is gathered together into families, in which minor deviations are referred to as variants. Fundamentally different files form the foundation for their own families. The count is based on new signature variants, also called malware types, created in the first half of 2014.

[2] http://technet.microsoft.com/en-us/library/cc759759%28v=ws.10%29.aspx

type of protection[3] was discovered in the course of analysing the **Uroburos rootkit**[4], a highly complex type of spyware. There is almost no doubt that the number of new **rootkits** will start to increase again at some point.

In complete contrast to this, the **adware** category is continuing to fly high. Since the second half of 2012, the number of new malware types in this category has increased rapidly, by a factor of 16. 14% of all new signature variants currently fall into the **adware** category. As in the previous half year, this massive increase is also reflected in the attacks fended off by G DATA products, as is assessed in the RISK MONITOR section.



Source: G DATA SecurityLabs

Platforms – .NET developments on the rise

Once again, a significant increase in the proportion of .NET developments (MSIL) was recorded. The proportion has risen to 8.5%. During the past half year again, nothing has changed in the dominance of malware types targeting Windows – the percentage is still in excess of 99.9%.

						Difference	Difference
						#2014 H1	#2014 H1
	Platform	**#2014 H1**	**Share**	**#2013 H2**	**Share**	**#2013 H2**	**#2013 H1**
1	Win	1.688.719	91.4%	1.774.287	94.7%	-4.82%	+15.47%
2	MSIL	158.127	8.5%	97.686	5.2%	+61.87%	+240.44%
3	WebScripts	598	<0.1%	720	<0.1%	-16.95%	+10.70%
4	Scripts[5]	551	<0.1%	642	<0.1%	-14.26%	+277.19%
5	NSIS	399	<0.1%	252	<0.1%	+58.44%	+1561.91%

Table 1: Top 5 platforms in the last two six-month periods

[3] https://blog.gdatasoftware.com/blog/article/uroburos-deeper-travel-into-kernel-protection-mitigation.html
[4] https://blog.gdatasoftware.com/nc/blog/article/uroburos-highly-complex-espionage-software-with-russian-roots.html
[5] Scripts are batch or shell scripts or programs that have been written in scripting languages such as VB, Perl, Python or Ruby.

RISK MONITOR

The risk monitor shows the Top 10 defeated attacks against computer users[6] involving G DATA security solutions[7] and active user feedback[8]. The most frequently averted attacks in the first half of 2014 are shown below. A permanently updated list for individual months can be found on the G DATA SecurityLabs website[9].

Rank	Name	Percent
1	Gen:Variant.Adware.SwiftBrowse.1	55.8%
2	Adware.SwiftBrowse.B	4.0%
3	Adware.SwiftBrowse.P	2.5%
4	Adware.Relevant.CC	2.4%
5	Script.Application.Plush.D	2.2%
6	Script.Application.ResultsAlpha.D	1.8%
7	Win32.Application.Linkury.A	1.3%
8	Script.Application.JSLoadBrowserAddon.A	1.0%
9	Gen:Variant.Adware.Graftor.125313	0.5%
10	Win32.Application.SearchProtect.O	0.3%

Table 2: The Top 10 attacks registered by MII in H1 2014

The observed trend – the rapid increase in **adware detections** – continued in H1 2014. The top positions overall in the evaluation lie firmly in the hands of malware in the **adware** category that belongs to the group called **"Potentially Unwanted Programs" (PUPs)**. From a statistical point of view, almost 3/4 of overall detections belong to the list of Top 10 malware variants (71.8%).

However, the new top protagonists are no longer malware variants in the **Bprotect** family, but those in the **SwiftBrowse** family. This family has occupied three places in the Top 10 for the last six months, having reached these positions by being singly responsible for 62.4% of all attacks in this half year period. Adding together all 34 of the **SwiftBrowse variants** that occurred in H1 brings their share to almost 65%.

Malware variants in the **SwiftBrowse** family are highly variable, which is another reason for the high number of detections. The pest uses over 80 different campaign aliases, such as WebGet, BetterBrowse, EnhanceTonic, etc. It injects JavaScript into the browser to display potentially unwanted additional advertising, banners, coupon promotions, comparison offers from other online shops and the like. The adverts are generally obtrusive and annoying.

The extremely high detection figures have partly resulted because the installation of **SwiftBrowse** is controlled from the server-side. This means that every time the browser is opened, the browser plug-in tries to connect to the server associated with the campaign and to download malicious code from there. This attempt is detected by the scanners and blocked.

Each **SwiftBrowse campaign** has its own website and its own associated domain. However, all are designed in the same way and all are registered on Yontoo LLC, founded in 2011. Yontoo LLC is one of multiple subsidiary

[6] The way of counting in this section differs from the preceding section, because the number of actual attacks is evaluated rather than the number of new malware types. A single malware program can have a massive effect when the attacks are counted, even if the family has produced few (new) variants.

[7] Since January 2014, these statistics relate exclusively to the G DATA CloseGap and Bitdefender scanner combination.

[8] The Malware Information Initiative (MII) relies on the power of the online community; any customer that purchases a G DATA security solution can take part in this initiative. The prerequisite for this is that customers must activate this function in their G DATA security solution. If a computer malware attack is fended off, a completely anonymous report of this event is sent to G DATA SecurityLabs. G DATA SecurityLabs then collects and statistically assesses data on the malware.

[9] https://www.gdatasoftware.co.uk/securitylabs/top10-malware.html

companies owned by Sambreel Holdings. In the past there have been negative reports about Sambreel, when it illegally captured advertisements on Google, Facebook, the New York Times website and the like and even set the wheels of law in motion by doing so.[10] The video service YouTube and its users have also been troubled by Sambreel using "malvertising".[11] Hence the masterminds behind these observed massive campaigns are far from unknown, and no end to this inconvenience can be foreseen as things stand.

The massive occurrence of **PUP malware** raises more and more questions among customers. Technical forums are filled with complaints regarding **"Potentially Unwanted Programs"**. Users complain that "a virus has infected their browser" or "a toolbar has hacked into the PC" and they justifiably feel extremely aggrieved by this. However, this does not involve malware in the traditional sense, and the majority of such "infections" can actually be avoided. Experts at G DATA SecurityLabs have therefore specifically set up a blog entry on this subject to help clarify it.[12]

In most cases, **PUPs** are programs that change browser settings, display advertising and show unsolicited offers – in this way they annoy users and make money for the distributors. Such programs do not generally get onto the computer by exploiting security holes, for example, but are frequently installed as an unwanted extra without the user noticing. Attackers tend to package these up with popular freeware programs and distribute them on the Internet. Hence it is advisable to only download software directly from manufacturers' sites or get it from trustworthy third party providers. Furthermore the installation dialogue should be read carefully and every option field checked when doing so – especially those with a checkbox already marked.

[10] http://online.wsj.com/news/articles/SB10001424052970203413304577086463731021828
https://gigaom.com/2012/10/19/notorious-ad-hijacker-spreads-to-more-media-retail-sites/
http://www.thewire.com/technology/2012/10/meet-company-hijacking-new-york-times-ad-revenue/58147/

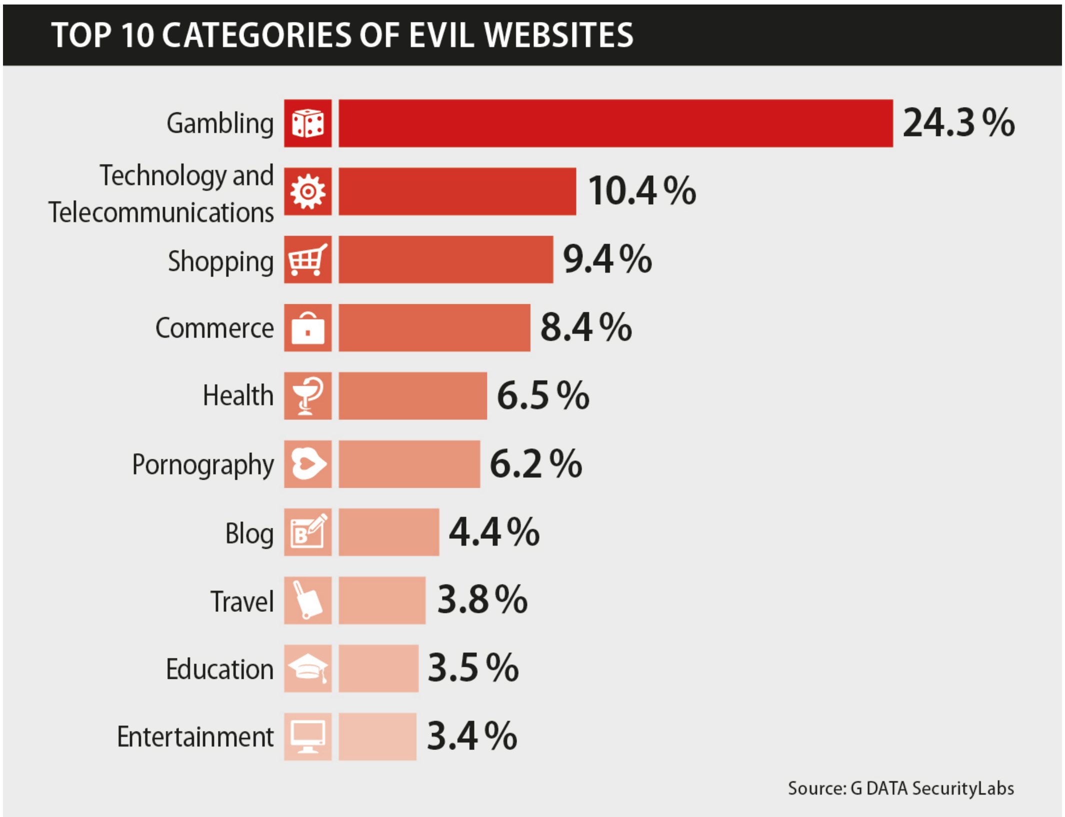
[11] http://www.spider.io/blog/2013/08/sambreel-is-still-injecting-ads-video-advertisers-beware/

[12] https://blog.gdatasoftware.com/blog/article/potentially-unwanted-programs-much-more-than-just-annoying.html

WEBSITE ANALYSES

Categorisation by topic

The following graphic shows how websites ranked as vicious[13] were categorised by subject in the first half of 2014. Overall the Top 10 make up a share of 80.3% of all classified websites, which is a significant 8.3% more than even in the previous half year. The Top 5 alone are responsible for 59.0%.



Source: G DATA SecurityLabs

One re-entry in the first half of this year is the **education** category – in H2 2013 it did not just make it into the Top 10, however it has now climbed back up to rank number 9 with 3.5%, displacing the **games** category. In the second half of 2013, the **gambling** category appeared as a new subject in 9th place. In the evaluation of H1 2014, it has now reached no less than 1st place. Accordingly one in every four vicious websites came under the title of **gambling**. According to research, the compromised gambling websites primarily involved small, less popular sites. Attackers illegally gain access to casinos' webspace and, for example, set up phishing sites for popular payment service providers, banks, webmailers and much more. They then distribute the links to these phishing websites via spam email, for example, and lure victims onto the sites on the pretext of imminent account suspension or similar scenarios.

Where malware is deposited on the compromised websites, this frequently involves exploit kits. Scripts check the computer for vulnerabilities and, where possible, subsequently launch a suitable attack on the computer. Computers are then infected with things such as banking Trojans, spyware or malware that turns them into zombie computers.

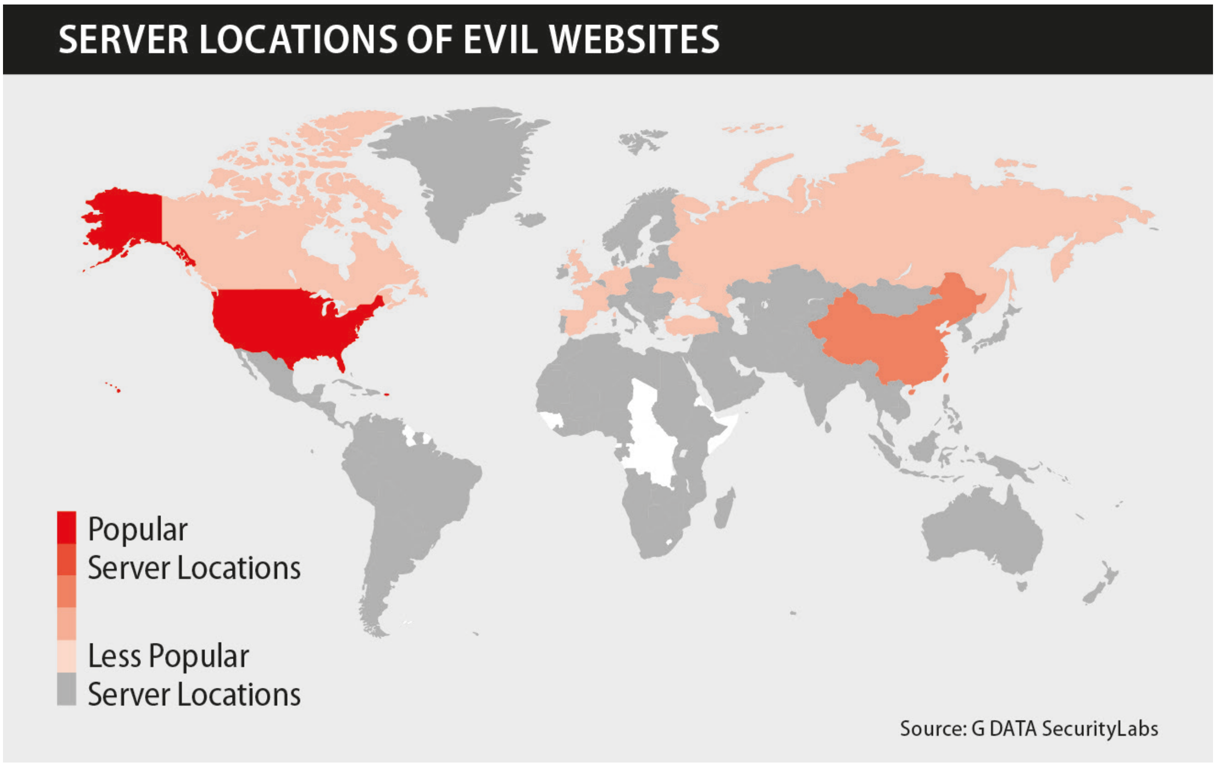
The gambling market is booming on the Internet, and numerous new providers are forcing their way into it. Attackers see an opportunity of increasing their hit rate for attacks by following such trends. Because their sights

[13] In this context, vicious websites include phishing sites as well as malware sites. The count also does not distinguish between domains set up specifically for this purpose and legitimate sites that have been manipulated.

are set on making a quick profit, the quality of the websites set up by the providers, and hence the level of security, all too often suffer. Attackers take advantage of this. They can find a large number of sites that can potentially be attacked and a large number of potential victims visiting these sites.

Categorisation by server location

Vicious websites are categorised by location under this evaluation. Whether it is a phishing website or a website compromised by malware, all are checked for their server location. The following world map shows which countries are particularly popular among attackers.



SERVER LOCATIONS OF EVIL WEBSITES

Source: G DATA SecurityLabs

It is notable that there are no longer any significant differences in the popularity of the server locations in **Europe**. Where **Germany** had an even higher share of vicious websites in previous half years, European countries now all lie on the same level. The number of sites set up on **Russian servers** has also dropped.

In contrast to this, however, **Canada** is now classed as the second most popular location, although still behind the **USA**.

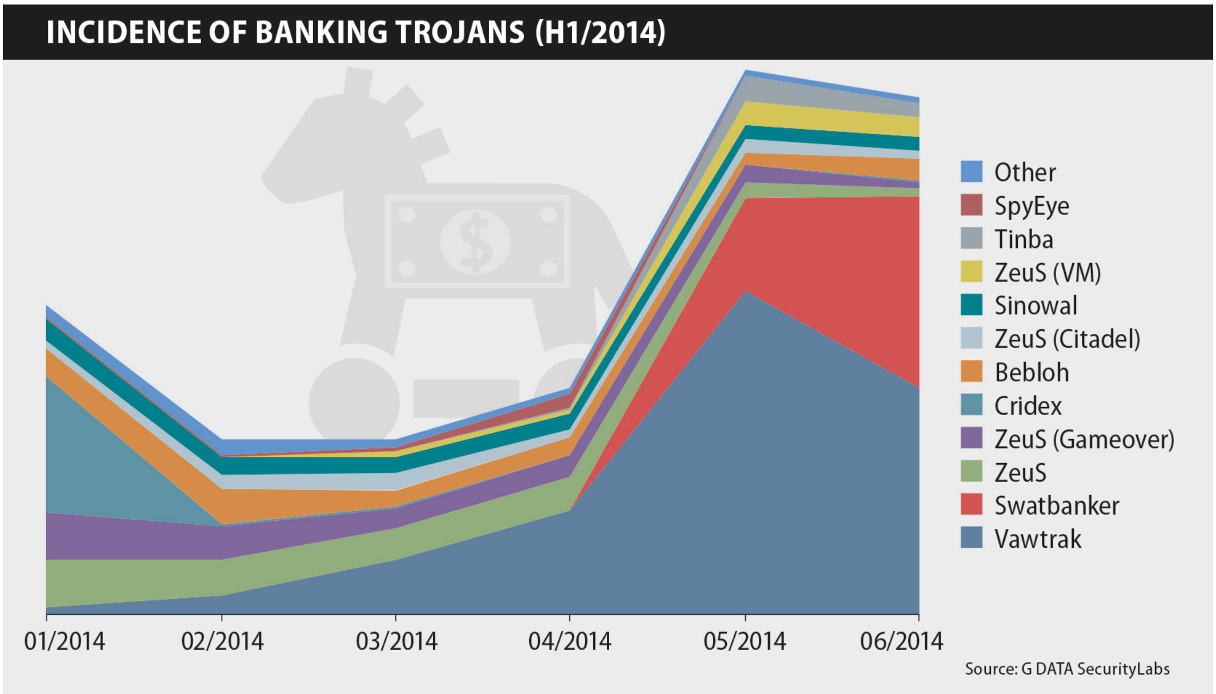
The white specks in **Africa**, which are countries in which, according to our knowledge, no vicious websites were set up in the last half year, have increased again slightly, but have not changed significantly. **Central Africa** is and remains a region with less than ideal conditions for cyber attacks.

BANKING

Trends in the Trojan market

The picture of the market for banking Trojans has changed greatly in the first half of 2014. Previously dominant malware has been displaced by newer malware, and previously apparently small or even completely new families of Trojans have taken the places of established old ones, sometimes driving detection figures to record levels.

The attack vectors have changed in 2014 as well, and are alarmingly successful, according to the detection figures. On the one hand, exploit kits have been as active as ever. On the other, however, the criminals behind the banking Trojans have also been infecting large numbers of computers recently, using massive waves of spam as their starting point.
At the beginning of the year, it was determined from such a wave that a slightly modified variant of the previously rather inconspicuous banking Trojan **Cridex**, also known as **Feodo**, was being mass-distributed. It was hidden behind hyperlinks in emails that supposedly pointed to invoices.[14] This wave of attack levelled out significantly in February and ebbed away entirely a short time later. After a two-month gap, presumably the same attackers returned with the same scam. In this wave, malware from the **Swatbanker**/**Geodo** family, a previously unknown banking Trojan presumably programmed specifically for these attacks, was mass-distributed. In some respects, this showed clear parallels with **Cridex** and can therefore be considered as its successor.[15]



Source: G DATA SecurityLabs

Another malware strain established itself at the same time as **Cridex** and **Swatbanker**, and within a few months its detection numbers exceeded every banking Trojan known in recent years. **Vawtrak**, which first appeared barely a year ago[16], remained resolutely under the radar throughout 2013. However, in the first half of 2014, its detection levels rose upwards steeply as a result of its distribution both in exploit kits and via spam. Since early March **Vawtrak** has held the top spot among the most frequently detected banking Trojans.

[14] https://blog.gdatasoftware.com/blog/article/cridex-banking-trojan-on-the-rise.html
[15] https://blog.gdatasoftware.com/blog/article/massive-spam-campaign-returns-cridex-successor-swatbanker-is-spread.html
[16] http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/Vawtrak.A

The parallel increase of **Cridex**/**Swatbanker** and **Vawtrak** saw the infection figures in February and March, which were relatively low overall, increase more than threefold in May and hence reach a new all-time high, only dropping back slightly by the end of the first half of the year.

The heavy drop-off in the figures recorded for the **ZeuS family**, which yielded the variants **Citadel**, **Gameover** and **VM**, can only be partially explained. There were two major events for **Gameover** during the course of the six month period. Firstly, the **kernel mode rootkit Necurs** started being co-distributed in March by a new variant of **Gameover**.[17] The sole purpose of this rootkit was to prevent the removal of **Gameover**, or at least make it more difficult. That the plan misfired can be seen in the large reduction in detection figures in the following months. The explanation for this seems relatively obvious: whereas the attackers behind **Gameover** went to a lot of effort to hide the executable file in **Gameover** from antivirus software, the rootkit **Necurs** is relatively old and can be reliably detected by the majority of AV products. The combination of the two files therefore led to higher detection rates, which in turn reduced the infection figures.
Gameover also suffered a serious setback in June when the entire botnet was taken over by the US authorities and thus incapacitated.[18]

On the other hand, the **ZeuS variant VM**, also known as **KINS**, made significant gains. It barely occurred in previous years, but since February a new version has been causing numerous infections, reaching a high in May.

Another development predicted in the last six months of last year was confirmed. The detection figures for the Trojan families **Tatanga** and **Bankpatch** declined rapidly and are barely visible any more. **Sinowal** continued to show a strong downwards trend and, in case the situation will remain unchanged, these families will disappear from the picture almost completely in the coming months.

The banking Trojan **Tinba** underwent a small resurgence, which has increased significantly again since May. This may be due to the sale and improvement of the source code.[19]

The banking Trojans sector remains the most lucrative in the underground economy. A great deal of money is earned there, and is invested in things such as the improvement of existing banking Trojans and the development of new ones. We expect a great deal of movement in the banking Trojans sector once again in the second half of 2014.

[17] http://stopmalvertising.com/rootkits/analysis-of-zeus-gameover-with-necurs.html
[18] http://blogs.microsoft.com/blog/2014/06/02/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup/
[19] https://www.csis.dk/en/csis/news/4303/

The targets of banking Trojans

Besides the distribution of banking Trojan families, it is also interesting to look at which targets are being attacked by these Trojans. Depending on the type of malware, a particular focus of the attackers is banking and financial services providers.

Methods of attack

In principle, two formats need to be distinguished in attacks by banking Trojans: there are invisible attacks, and attacks from the **social engineering** sector.

With invisible attacks, the user for example logs on with his bank, perhaps carries out a transaction, and has money stolen from him, without him having noticed anything.

Attacks via **social engineering** require the malware to interact with the attacker, with the customer ultimately taking the attacker to be his bank. In this way, for example, pop-ups can be displayed on online banking portals suggesting to the user that he needs to carry out a test transaction, supposedly for security reasons. However, this is actually a genuine transaction.

Attacks via social engineering have been very difficult to detect thus far for both banks and users. Primarily, the proverbial common sense of the user can provide protection: here too, the chances of detection depend on the quality of the attack and the user's knowledge of the respective protocols. A request to carry out a test transaction that contains numerous linguistic errors and has no plausible reasons might lead to suspicion among many users. However, if the message is linguistically correct and there are a number of plausible reasons, such as supposed synchronisation of the TAN generator, detection becomes very difficult for non-technical users.

In technical terms, banking Trojans carry out their attacks using so-called **web injects**. These involve snippets of code that a banking Trojan can insert in websites when an infected PC opens a target site. **Web injects** can be used for things such as smuggling code during an online banking session. This possibly manipulates the list of transfers or the status of the account, preventing the user from noticing that fraudulent transactions are being carried out on his account during the online banking session. This is intended to prevent the victim contacting his bank and enabling it to block the fraudulent transaction.

Security measures

Banks try to counter attacks with internally implemented measures. A fundamental distinction must be made between whether the measures are obligatory (compulsory for the customers) or optional. Several frequently occurring security measures need to be set out in brief here. As all security measures are developed with significant differences by the various banks, the evaluation set out below quantifies only the relative attack frequency, and says nothing about whether these attacks were actually successful.

Single-use passwords

The most frequently used security measures are single-use passwords. As the name implies, these only work for a single process. Sometimes a process here means a login session, and sometimes an individual financial transaction. In the context of a transaction, a password is often referred to as a TAN, which is short for Transaction Number.

Single-use passwords ensure that an attacker cannot gain access simply by knowing the single-use password, as the password will have already been used by the victim. Attacks using simple **keyloggers** are effectively prevented using this method.

There are various procedures for generating single-use passwords.
A common way is to use lists of passwords that are checked off, called TAN lists. However, transaction numbers are often also sent to customers via a second channel – either via the mobile network (mTAN or smsTAN), or via another, separate device (e.g. chipTAN). If the transaction data can be checked once again on the second channel, e.g. by displaying the target account and the amount on the mobile phone display when receiving the smsTAN, furtive changes to the transaction can be prevented. Such changes to transactions might otherwise be carried out by online banking Trojans.
For example: the victim wants to transfer €100 to a specific target account. Unbeknownst to the victim, the banking Trojan changes the target account number to one that it controls, and changes the amount to €1,000. If the TAN that is entered has just been checked off a list, the victim does not notice the manipulation on his computer, or at least not until it is too late. However, if the transaction data is displayed once again in an SMS on a mobile phone using smsTAN prior to being executed, for example, the victim can detect the manipulation in good time and cancel the transaction.

Multiple-use passwords and personal questions

An intermediate method between single-use passwords and permanent passwords is often used. For example, there might be a nine-character password, of which three characters selected at random by the system must be entered during each login. Or, on the first login, the user is asked to answer a number of security questions, e.g. his mother's maiden name, his favourite colour, his first car, etc. Some services also permit entirely customised questions to be set up, along with the associated answers. Thereafter, one or more of these questions will be asked during each login process.

What these processes have in common is that they provide a certain level of protection against **keyloggers**. An attacker can only log in using the recorded login data. However, as not all of the security questions are asked, it is uncertain whether the attacker will be asked the security questions that he has been able to record from the victim. Of course, the actual implementation of the process on the part of the bank plays a role here, i.e. is the attacker asked another question during a second login attempt that, unlike the first question, he might have already recorded?

However, it must be noted that the effectiveness of the protection of this security measure is limited; nevertheless, where such measures have been implemented, protection against **keyloggers** is assumed in the following evaluation.

Plausibility check

Some banks apply further, more invisible security measures. These frequently involve techniques often referred to as a kind of fingerprint of the registered user's computer, and plausibility checks.

For example: according to his usual profile, a user always logs on in Great Britain and only carries out inland transactions. A few minutes after logging off the service, from Great Britain as usual, he apparently logs on again from a PC located in Russia and carries out a transfer to Russia. It is obvious that this transaction is not plausible. In this case the bank could therefore block the transaction or only execute it on the customer's explicit confirmation. In principle, such checks can be visualised as an adaptation of human common sense, turned into an automatic check on the part of the bank. As the way in which such checks work is not generally made apparent for security reasons, they can only be considered in the following evaluation if there are explicitly known security measures, e.g. if a transfer to a previously unknown recipient triggers further security measures.

Phishing protection via personalisation

Another security measure often used is personalisation of the login process. In the most common cases, a personalised image can be selected. This is selected at will by the customer during his first login on the bank's website. This image is displayed to the customer prior to the last step in the login process. If the image that the customer has chosen himself is not displayed, he can assume that he has become the target of a **phishing attack** and should cancel the login process immediately. As only the operator of the website and the customer know of the image, the attacker cannot fully falsify the website.

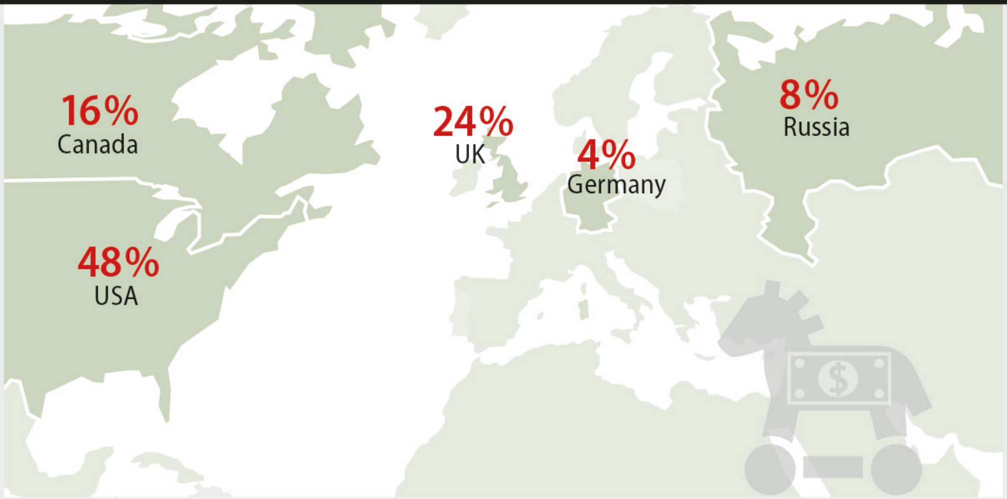
However, the personalised image is merely protection against **phishing.** Attacks by banking Trojans are not affected by this, as they operate in the context of the bank's legitimate site. Hence the interface appears legitimate to the user. Measures of this type are not generally taken into further consideration in the following evaluation.

Results

A tabular evaluation of the results is given on page 15. In total, 825 different targets were attacked by the banking Trojans investigated. According to the research, the most common target was the Bank of America under "bankofamerica.com", which was embedded in 12.98% of the banking Trojan configurations investigated.

On average, the Top 25 targets determined were attacked by 8.68% of the banking Trojans investigated; the Top 100 targets were attacked by 4.69% on average, and all 825 targets by 0.83%. Hence there is no uniform distribution; rather, the criminals behind the attacks evidently prefer specific banks. It can be presumed that the attackers focus on the anticipated success rate when selecting their targets. Factors such as the number of customers, the average anticipated profit, and the security measures of the bank play a fundamental role here. Of the Top 25 targets of attack, twelve come from the **USA**, six from the **United Kingdom** and four from **Canada**. Hence 88% of the targets of attack were located in English-speaking countries. Two payment service providers came from **Russia**. Just one bank in the top list came from **Germany**.

COUNTRIES TARGETED BY TOP 25 BANKING TROJANS (H1/2014)



Worldwide allocation of Top 25 targets, based on 3,521 analysed ZeuS (including Citadel) and Spyeye banking Trojans

Source: G DATA SecurityLabs

The most valuable banks in the world in 2013, as indicated by Broad Finance Plc, are also among the Top 25 investigated, and all have their head office in English-speaking countries[20].

Almost half (40%) of the Top 25 targets were susceptible to conventional **keyloggers** when using the obligatory security measures. Where all optional security measures were used by customers, this was just 12%.
If the customer only uses the obligatory security measures, four out of five targets (80%) were susceptible to banking Trojans capable of manipulating transactions without the user noticing. When using additional security measures, this was still more than three quarters (76%).

Both banks and other operators of the websites being attacked are relatively powerless against banking Trojans that use technology from the **social engineering** sector. Only client-side protection systems help here. One such client-side protection system offering protection against any attacks by online banking Trojans is G DATA BankGuard. Keylogger Protection is also included as a new feature in the new 2015 product generation, which prevents attacks by **keyloggers**.

[20] Market value according to http://www.brandfinance.com/images/upload/the_banker_brand_finance_banking_500_full_results.pdf

TOP 25 TARGETS OF BANKING TROJANS (H1/2014)

	Country	Rating	Protection against silent banking Trojans		Protection against Keylogger		Attack Frequency
		Brand value via Brand Finance	obligatory	optional	obligatory	optional	Relative attack frequency, based on 3,521 analysed ZeuS (including Citadel) and Spyeye banking Trojans
Bank of America bankofamerica.com	🇺🇸	**4**	✗	✗	✓	✓	🟩 12.98 %
PayPal paypal.com	🇺🇸	–	✗	✗	✗	✓	🟦 12.92 %
Citi citibank.com	🇺🇸	**5**	✗	✗	✓	✓	🟩 12.78 %
Lloyds lloydstsb.co.uk	🇬🇧	60	✓	✓	✓	✓	🟩 10.91 %
TSB Bank tsb.co.uk	🇬🇧	60	✓	✓	✓	✓	🟩 10.91 %
HSBC hsbc.co.uk	🇬🇧	**3**	✓	✓	✓	✓	🟩 10.88 %
USAA usaa.com	🇺🇸	–	✗	✗	✗	✓	🟩 10.25 %
Barclays barclays.co.uk	🇬🇧	17	✓	✓	✓	✓	🟩 10.11 %
Wells Fargo wellsfargo.com	🇺🇸	**1**	✗	✗	✓	✓	🟩 8.92 %
SunTrust suntrust.com	🇺🇸	79	✗	✗	✓	✓	🟩 8.26 %
US Bancorp usbank.com	🇺🇸	35	✗	✗	✗	✗	🟩 8.09 %
Chase chase.com	🇺🇸	**2**	✗	✗	✗	✗	🟩 8.01 %
Royal Bank of Canada royalbank.com	🇨🇦	21	✗	✗	✗	✓	🟩 7.87 %
Canadian Imperial Bank of Commerce cibc.com	🇨🇦	47	✗	✗	✓	✓	🟩 7.75 %
TD Bank tdbank.com	🇺🇸	20	✗	✗	✓	✓	🟩 7.36 %
eBay ebay.com	🇺🇸	–	✗	✗	✗	✓	🟧 7.10 %
Postbank postbank.de	🇩🇪	92	✓	✓	✓	✓	🟩 6.84 %
PNC Financial Services pnc.com	🇺🇸	50	✗	✗	✓	✓	🟩 6.79 %
Halifax halifax-online.co.uk	🇬🇧	78	✗	✗	✓	✓	🟩 6.76 %
Bank of Montreal bmo.com	🇨🇦	36	✗	✗	✗	✗	🟩 6.59 %
Yandex yandex.ru	🇷🇺	–	✗	✗	✗	✓	🟦 6.59 %
Skrill moneybookers.com	🇬🇧	–	✗	✗	✗	✓	🟦 6.56 %
WebMoney webmoney.ru	🇷🇺	–	✗	✓	✗	✓	🟦 6.53 %
Capital One capitalone.com	🇺🇸	27	✗	✗	✓	✓	🟩 6.50 %
TDBG td.com	🇨🇦	20	✗	✗	✓	✓	🟩 6.33 %

Category: 🟩 = Bank 🟦 = E-Payment 🟧 = Auction

Source: G DATA SecurityLabs

Methodology

In total, 3,521 configuration files were extracted from samples of banking Trojans in the families **ZeuS**, including its clone **Citadel,** and, **SpyEye**. These malware variants can traditionally be used to form a good cross-section of the banking Trojan landscape. The configuration files contain a list of target sites (websites for banks, payment service providers, etc.) that are attacked using **web injects**.

The domains were extracted from the target sites for this current evaluation, and the DNS entries for the domains checked for their validity. Finally, there was a count of which domains occur in how many samples. In this way the relative attack frequency on domains could be determined, and so the domains are ultimately designated as targets of attack.

Countries of origin were also allocated to the Top 25 domains, for which the companies' own information on the relevant sites was used. Furthermore, the site security measures were evaluated for the domains. As far as the security measures are concerned, the information accessible on the public website at the time of the investigation was used as a basis, so no guarantee for the actual correctness can be accepted.

In addition, the type of attack carried out by the most common **web injects** was analysed.

Security measures for the Top 25 individually

As **social engineering attacks** via banking Trojans (e.g. test transfers) on banks can only be detected by heuristics on the part of the banks that cannot be considered further here, susceptibility to such attacks is implicitly assumed for each bank.
The way in which such checks work is not generally transparent for security reasons, so these are only taken into further consideration in the following evaluation where there are known patterns (e.g. if a transfer to a previously unknown recipient triggers further security measures).

1st place: Bank of America (bankofamerica.com)

The bank that heads up the analysis results referred to above uses two security measures called SiteKey and SafePass.

SiteKey is the name of an obligatory security measure. This involves the display of an image during the login process that is selected by the user when he first logs in. In addition, three questions also selected by the user at the outset must be answered if he tries to log in from a device previously unknown to the bank. This system can only offer protection against conventional phishing (primarily via spam email) and keyloggers, not banking Trojans.

SafePass involves single-use transaction passwords that are displayed to the user via a mobile phone or another device in card form. However, this is an optional security process. SafePass only needs to be used to carry out transactions above a certain limit. Furthermore, no transaction details are shown for verification purposes, which makes manipulations possible.

Sources: https://www.bankofamerica.com/privacy/online-mobile-gfbanking-privacy/safepass.go
https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/sitekey.go

2nd place: PayPal (paypal.com)

The well-known payment service provider PayPal is the highest-placed target of attack in this list that does not form part of the traditional banking business. In the standard configuration, there is no protection on PayPal against keyloggers or banking Trojans. However, PayPal has an optional protection system called Security Key that uses single-use login passwords via mobile phone or another device in card format. The protection system can be used for logging on to eBay as well. The transaction data (target account, amount) is not transmitted to the user, so this cannot be checked. Hence an attacker can use a banking Trojan to substitute the amount and target account during a transaction without the user being notified; social engineering is not required.

Source: https://www.paypal.com/securitykey

3rd place: Citibank (citibank.com)

In late 2013, Citibank introduced obligatory single-use transaction passwords via mobile phone. However, the information sent to the mobile phone for this does not contain any transaction data, so it cannot be verified. Therefore this offers protection against keyloggers, but not online banking Trojans.

Source: https://online.citibank.com/JRS/pands/detail.do?ID=SecurityCenter

4th place: Lloyds (lloydstsb.co.uk)

Lloyds Bank appears in the Top 25 list under two domains, in 4th place and 5th place. During each login, the customer must enter three random characters from a longer password. In principle this is a single-use password, albeit with a very limited number of options. Furthermore, this methodology is very susceptible to social engineering attacks, as one only needs to suggest to the customer that the complete password must be entered for security reasons.

However, with previously unknown payment recipients, there is also an automated callback via telephone, during the course of which the user needs to identify himself and verify the current transaction. Hence the transaction is authorised via a second channel.

As a result, this offers protection against keyloggers and online banking Trojans that are not attacking via social engineering. An exception here might be the worst case scenario in which an attacker tries to transfer money to an account that is already known. However, this does not correspond to the usual attack patterns of cyber criminals.

Source: http://www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp

5th place: Lloyds (tsb.co.uk)

The protection methods used by Lloyds Bank are described in the evaluation for 4th place. The measures for the two domains do not differ from one another.

Source: http://www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp

6th place: HSBC (hsbc.co.uk)

The Hong Kong & Shanghai Banking Corporation (HSBC) has been using a protection system involving an additional device for several years. Every login and every transaction involving an unknown recipient must be confirmed via a single-use password. This system not only provides protection against keyloggers. Transaction details are verified on the device by using parts of the recipient's account number to generate a Secure Key PIN. Therefore in principle this offers protection against online banking Trojans that modify transaction data without being noticed. As with Lloyds Bank, the worst case scenario here is that the attacker tries to transfer money to an account that is already known, which is not a standard attack pattern for attackers. Furthermore, the risk of social engineering attacks is particularly high, as the transaction is not explicitly displayed on the security key device, nor does it have to be confirmed; rather, the target account is only implicitly verified, by entering the last four characters of the account number.

Source: https://www.hsbc.co.uk/1/2/customer-support/online-banking-security/secure-key

7th place: USAA Bank (usaa.com)

USAA Bank uses an optional process of single-use passwords via a mobile phone for logging in, offering protection against keyloggers. However, transactions are not authenticated, leaving customers susceptible to online banking Trojans that can substitute the amount and target account of a transaction without being noticed.

Source: https://www.usaa.com/inet/pages/security_token_logon_options

8th place: Barclays (barclays.co.uk)

Barclays has the PINsentry protection system that uses single-use passwords to secure both logins and transactions. These can be generated via mobile phone or an additional device. Without protection via PINsentry, only transfers to recipients already saved or to specific recipients verified by the bank (esp. companies) can be carried out. In this case, a passcode and a memorable word suffice as legitimation. Nevertheless, details about the transaction are shown for verification purposes on the mobile device or the additional device, but only for payments to new payees. Therefore, a manipulation by banking Trojans cannot be excluded as there is a chance of a scenario in which someone fraudulently attempts to transfer money to a known recipient or one verified by the bank.

Sources: http://ask.barclays.co.uk/help/online_banking/register
http://www.barclays.co.uk/Helpsupport/HowtousePINsentry/P1242560253457
http://ask.barclays.co.uk/help/online_banking/memorable_word_passcode
Barclays PINsentry User Guide Leaflet (Item reference: 9907259)

9th place: Wells Fargo (wellsfargo.com)

Customers who use the Direct Pay or Foreign Exchange Online services receive a single-use password generated per additional device when logging in. Other customers must correctly answer one of three predefined security questions. However, as only the login and not the transaction is secured, the amount and target account of a transaction can be changed by banking Trojans without being noticed.

Sources: https://www.wellsfargo.com/privacy-security/online/protect/
https://www.wellsfargo.com/biz/jump/securid

10th place: Suntrust (suntrust.com)

Besides the conventional login via user ID and password, Suntrust uses security questions for protection against keyloggers. However, this is still susceptible to online banking Trojans.

Source: https://www.suntrust.com/FraudAndSecurity/FraudProtection/HowWeProtectYou

11th place: U.S. Bank (usbank.com)

No information on security systems could be found beyond a simple password. Consequently there is a very high probability of susceptibility to keyloggers and online banking Trojans.

Source: https://www.usbank.com/online-security/index.html

12th place: Chase (chase.com)

No information on security systems could be found beyond a simple password. Consequently there is a very high probability of susceptibility to keyloggers and online banking Trojans.

Source: https://www.chase.com/resources/privacy-security

13th place: Royal Bank of Canada (royalbank.com)

In addition to the user ID and password, Royal Bank of Canada secures the login to its Sign-In Protection feature and the request for new passwords via one of three predefined personal questions, which means protection against keyloggers. This only offers protection for the login, not individual transactions, so banking Trojans are able to change the amount and target account of a transaction without being noticed.

Source: https://www.rbcroyalbank.com/onlinebanking/bankingusertips/security/features.html#1

14th place: Canadian Imperial Bank of Commerce (cibc.com)

In the first half of 2014, the Canadian Imperial Bank of Commerce was using personal questions to protect its customers, as well as a conventional login using a card number and password. Therefore there is protection against keyloggers, but not online banking Trojans. Since July 2014 there has been a change in progress, after which transactions will also be secured via single-use passwords. This migration, which lies outside of the period of this report, is not taken into further consideration in the evaluation.

Sources: https://www.cibc.com/ca/legal/identity-fraud.html
https://www.cibc.com/ca/features/banking-enhancements.html?WT.mc_id-Int-ANCH-NGA-ComingSoon-E

15th place: TD Group (tdbank.com)

Toronto Dominion Bank is represented under two domains in the Top 25. The same security functions apply to both. When logging in with a new device, the user must answer one of five predefined security questions. Hence the login is merely protected against keyloggers. However, there is no additional protection for individual transactions, which implies susceptibility to online banking Trojans.

Sources: http://www.tdbank.com/bank/securitycommitment.html
http://www.td.com/privacy-and-security/privacy-and-security/how-we-protect-you/online-security/idplus.jsp

16th place: eBay (ebay.com)

eBay has an optional protection system via single-use login passwords via mobile phone or an additional device in card format. The protection system can be used for logging on to PayPal as well. In principle, the problem is that, again, only the login and not the transaction (here primarily the sale) is checked. Conventional online banking Trojans can change the target of the transaction without the user noticing.

Source: http://pages.ebay.com/securitykey/faq.html

17th place: Postbank (postbank.de)

According to the current analysis, Deutsche Postbank is the most attacked target based outside of the English-speaking territories. There are numerous processes for authenticating transactions via mobile phone and other devices, offering protection against keyloggers and online banking Trojans that do not attack via social engineering.

Source: https://www.postbank.de/privatkunden/pk_sicherheit_tanverfahren.html

18th place: PNC Financial Services (pnc.com)

Under the obligatory security measures, personalised images are displayed for protection against phishing. Furthermore, personal questions are asked when logging in from unknown end devices, offering protection against keyloggers. With customers who use the PINACLE portal for corporate customers, a single-use password generator is used instead. However, this only secures the login and not transactions. Hence there is no protection at all against online banking Trojans.

Source: https://www.pnc.com/webapp/unsec/ProductsAndService.do?siteArea=/pnccorp/PNC/PNC+Security+Center/Enhanced+Authentication+Landing+Page

19th place: Halifax (Halifax-online.co.uk)

In the Halifax Bank online bank portal, protection against keyloggers is inbuilt based on the need to select three characters from a predefined private word during login, in addition to the user name and password. However, there is no additional protection for individual transactions, meaning that banking Trojans can change the amount and target account of a transaction without being noticed.

Source: http://www.halifax.co.uk/aboutonline/security/protecting-you/

20th place: Bank of Montreal (bmo.com)

No information on security systems could be found beyond a simple password. Consequently there is most probably susceptibility to keyloggers and online banking Trojans.

Source: http://www.bmo.com/home/about/banking/privacy-security/how-we-protect-you

21st place: Yandex (yandex.ru)

Yandex provides an offering similar to Google, focused on the Russian market. The target of the attacks in every case investigated was the Yandex Money service, a payment service comparable to PayPal. Yandex offers optional single-use passwords via a cross-off list and via SMS for securing transactions. With single-use passwords via SMS, there is no indication that the text messages enable authentication of the transaction target. In this regard it can be assumed that only the login and not the transactions are secured. Therefore this offers protection against keyloggers, but not online banking Trojans. Without single-use passwords there is also no protection against keyloggers.

Source: https://money.yandex.ru/doc.xml?id=524852

22nd place: Skrill (skrill.com)

Since 2009, payment service provider Skrill, then still operating under the name moneybookers, has issued optional additional devices for generating single-use passwords for the purposes of login security. This process provides protection against keyloggers, but not against online banking Trojans.
In 2011 a rebranding process from moneybookers to Skrill was implemented. In the last quarter of 2013, skrill.com became the main site, whereas moneybookers.com is just for redirecting. In spite of this, all of the samples investigated target moneybookers.com and not skrill.com, meaning that the web injects found at the time of the investigation do not function. This indicates a certain indolence in this market.

Sources: https://www.skrill.com/en/personal/security/
https://www.skrill.com/en/vip/moneybackguarantee/

23rd place: Webmoney (webmoney.com)

The proprietary client software WM Keeper WinPro (Classic) or login in a browser via WM Keeper WebPro (Light) can be used when logging on to payment service provider Webmoney. Logging in via the browser is possible via three different ways: a client certificate or single-use passwords via mobile phone (E-num) or classic log-in and password approach. Hence protection against keyloggers is provided when using optional security features. The web injects analyse solely attack WM Keeper WebPro (Light). The user can chose from a variety of verification methods for transactions and can, with the right choice, arrange protection against manipulation by banking Trojans.

Sources: https://wiki.wmtransfer.com/projects/webmoney/wiki/Transaction_confirmation_in_WM_Keeper_WebPro
https://wiki.wmtransfer.com/projects/webmoney/wiki/WM_Keeper_WebPro
http://security.wmtransfer.com
http://www.e-num.com

24th place: Capital One (capitalone.com)

Capital One secures the online banking login with one of five preselected security questions. This method offers protection against keyloggers. There is no additional verification for individual transactions, meaning that banking Trojans can change the amount and target account of a transaction without being noticed.

Source: http://www.capitalone.com/online-banking-faq/?Log=1&EventType=Link&ComponentType=T&LOB=MTS%3A%3ALCTMJBE8Z&PageName=Contact+Us+FAQ&PortletLocation=4%3B4-12-col%3B2-2-3-1-1&ComponentName=FAQ+olb+small+business+home+LOANs%3B18&ContentElement=1%3BCredit+Cards&TargetLob=MTS%3A%3ALCTMJBE8Z&TargetPageName=Online+Banking+FAQ

25th place: TD Group (td.com)

The protection measures for the TD Group are described in detail in the evaluation of 15th place. The measures for the two domains do not differ from one another.

Sources: http://www.tdbank.com/bank/securitycommitment.html
http://www.td.com/privacy-and-security/privacy-and-security/how-we-protect-you/online-security/idplus.jsp