TRUST IN
GERMAN
SICHERHEIT

G DATA SECURITYLABS MALWARE REPORT

HALF-YEAR REPORT
JULY – DECEMBER 2014

CONTENTS

AT A GLANCE

- The number of new malware strains increased enormously in the second half of the year (H2); 4,150,068 were counted. There were 1,848,617 instances in the first half of 2014, meaning that the experts recorded an increase of around 125%.
- Consequently, a total of 5,998,685 new malware strains appeared in 2014 as a whole. That is 77 percent more than the total number in 2013.
- Statistically, a new malware type was discovered every 3.75 seconds in H2 2014.

- The adware category once again displayed the highest rates of growth. The proportion of new adware signature variants was 31.4 percent in H2. Hence, almost one in three new detections came from this sector.
- The absolute figures for new adware strains have actually surpassed the downloader category and now lie in second place.
- The Malware Information Initiative (MII) provides an insight into averted attacks on computer users. Here too adware poses the greatest threat. Malware in the Browsefox/Browserfox family is particularly prominent here.
- The number of new signature variants for rootkits increased again. These are frequently used by attackers to integrate zombie PCs into their botnets so that malware components can remain hidden on the PC.

- The Vawtrak banking Trojan has been much in evidence since spring 2014 and continues to be a very active malware strain.
- The barriers for cyber criminals have been raised even higher through new security measures by banks and payment services, and the risk of being caught by criminal prosecution services is increasing.
- Few innovations in the banking Trojans sector were recorded in H2 2014; however, the risk from these is not considered any the less for this. The number of averted attacks rose by 44.5 percent! This indicates a consolidation in the market for banking malware.
- The latest investigation into the most common targets of attack by banking Trojans in the second half of the year showed seven new targets in the Top 25, including a bank in France in this six-month period.
- Service providers in the English-speaking countries continue to be the focal point here. 36 percent of the targets come from the USA, 24% from the United Kingdom and 12% from Canada.

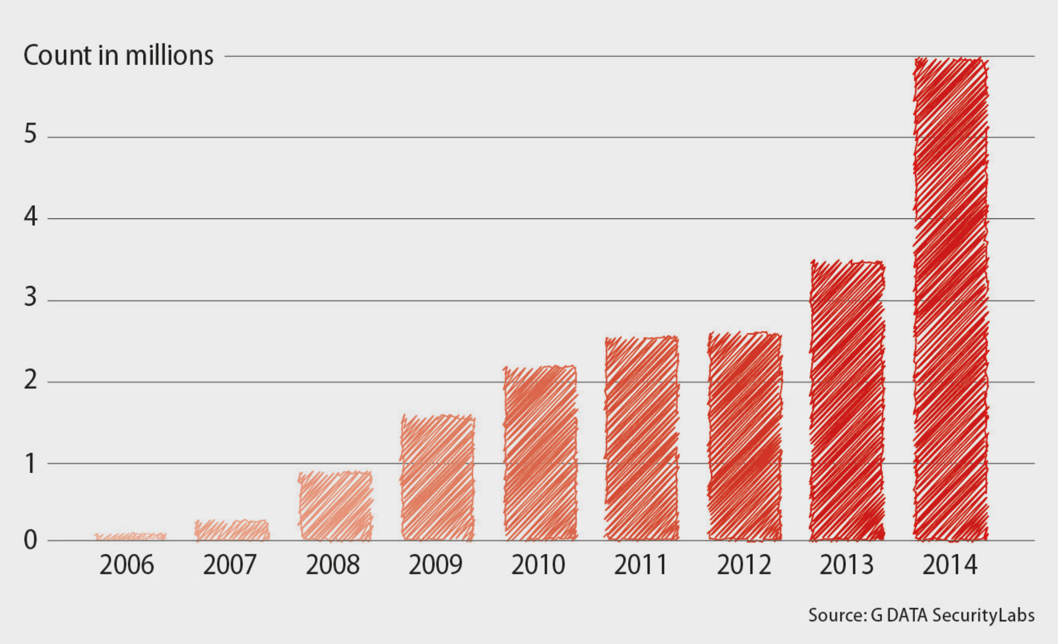
Forecasts and trends

- The experts believe that attackers will turn pure phishing attacks into multiple attacks that also involve malware in future. Potential phishing victims would then not only be afflicted via social engineering, but potentially also attacked by exploit kits.

MALWARE PROGRAM STATISTICS

The second half of 2014 once again broke all previous records and exceeded the predictions of experts by some degree. During this six-month period, G DATA SecurityLabs recorded 4,150,068 new malware types[1]. That is almost 2.3 times the result of the first half of the year and more than the number for 2013 as a whole! In total, almost six million new malware strains were recorded in 2014 (5,998,685).

NUMBER OF NEW MALWARE TYPES



Source: G DATA SecurityLabs

Categories

A malware strain is allocated to a category on the basis of the malicious activities that are registered on a system. Looking at this gives an idea of the type of attacks that cyber attackers are currently investing in heavily.

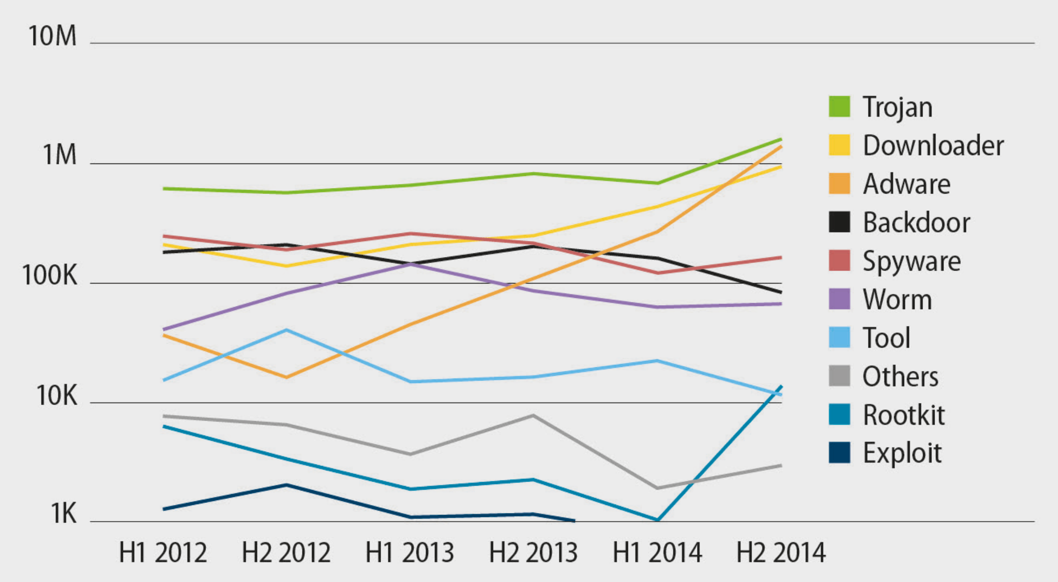
In the past half year, an increase in new signature variants was recorded in almost every category where not just one variant on its own was responsible for the rapid increase. However, some sectors increased significantly more than others.

Adware increased especially. Its share in all the categories was 31.4 percent in H2 2014, as opposed to 14.1 percent in H1 2014; the number of these actually quintupled. Adware overtook downloaders in this study and now takes second place behind Trojan horses in the assessment.

One trend that is set to continue and even gather speed is the bundling of legitimate software with potentially unwanted programs (PUPs) from third party providers. In the statistics on attacks fended off by G DATA, adware is again significantly in front, as can be seen in the Risk Monitor section.

[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 second half of 2014.

DEVELOPMENT OF MALWARE CATEGORIES



Source: G DATA SecurityLabs

There was also an increase in **rootkits**[2] that was striking because of the high numbers involved: the experts counted 18 times more new signature variants than in the first half of 2014, and the number of these increased significantly (but still represents just 0.45% of all categories considered). The numbers of **Trojans** and **downloaders**, which ranked 1 and 2 for some time in the overview in previous studies, have each almost doubled, although their proportions remain almost the same. If attackers want to integrate new computers into their botnets[3] for later exploitation, the three categories just mentioned are very often involved as components of such attacks.

What happens after an infection with botnet malware?
Attackers induce a user to run a malware program, e.g. via social engineering. To do this, they might package their malware in a file that looks legitimate and distribute this **Trojan horse** to as many users as possible – via email, as an apparently interesting video/program, a new, embarrassing photo of friends, a supposed invoice, etc.
The packaged malware could be anything from a banking Trojan to spam bots or backdoors, spyware and so on.
Frequently the attackers package up **downloaders** as a second stage in their attack. The purpose of downloaders is to contact one or more servers and then retrieve data and/or files stored there. The advantage for the attackers is that they can easily swap the files on the server and do not have to change the Trojan horse for each wave of attack.
Rootkits are also frequently part of the packaged malware or downloaded code. They are used to embed the malware on the PC for the longer term and hide it from scanners and monitors as cleverly as possible.

The number of systems infected with botnet malware rose to 40% in 2014 (33% in 2013).[4] This is one possible explanation for the serious increase in numbers in the second half of the year. Following the withdrawal of support for Microsoft Windows XP in April 2014, systems still using this operating system could become a focus for malware and be used as zombies, as they are unprotected against attacks on existing or newly discovered security holes going forwards.

Furthermore, the number of registered attacks by banking Trojans reached a high in H2 2014, as is considered in more detail in the Banking section in this report.

[2] https://www.gdata-software.com/security-labs/information/background-information/rootkits
[3] https://www.gdata-software.com/security-labs/information/background-information/botnets
[4] https://international.eco.de/2015/press-releases/more-zombies-in-the-internet-again-2014-botfrei-de-statistics.html

Platforms – .NET developments still on the rise

The programming of malware as .NET applications has ensured that the proportion of signature variants for the MSIL platform remained equally high in the past half year. In total, new malware variants for Windows platforms make up a 99.9% share.

						Difference	Difference
						#2014 H2	#2014 H2
	Platform	**#2014 H2**	**Share**	**#2014 H1**	**Share**	**#2014 H1**	**#2013 H2**
1	Win	3,868,902	93.2%	1,688,719	91.4%	+129.1%	+118.1%
2	MSIL	279,207	6.7%	158,127	8.5%	+76.6%	+185.8%
3	NSIS	757	<0.1%	399	<0.1%	+89.8%	+200.7%
4	Scripts[5]	562	<0.1%	551	<0.1%	+2.1%	-12.5%
5	WebScripts	464	<0.1%	598	<0.1%	-22.4%	-35.5%

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

RISK MONITOR

The risk monitor shows the Top 10 averted attacks against computer users[6] involving G DATA security solutions[7] and activated feedback[8]. The most frequently averted attacks in the second 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	26.9%
2	Win32.Adware.Browserfox.H	7.8%
3	Gen:Variant.Adware.Graftor.159320	6.3%
4	Adware.Mplug.AF	6.0%
5	Adware.BrowseFox.D	5.5%
6	Adware.BrowseFox.H	4.2%
7	Script.Adware.DealPly.G	3.6%
8	Gen:Variant.Adware.Graftor.159134	2.4%
9	Script.Application.Plush.D	1.7%
10	Adware.RelevantKnowledge.A	0.8%

Table 2: The Top 10 attacks registered by MII in H2 2014

In the second half of 2014, potentially unwanted programs (PUPs) once again dominated the statistics on most frequent attacks. In fact they were responsible for "only" 65% in the Top 10 listed above, which is a drop of 6.8% on the previous half year, although this in no way detracts from the significant preponderance of these attacks.

[5] Scripts are batch or shell scripts or programs that have been written in scripting languages such as VB, Perl, Python or Ruby.

[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 and 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

However, the total number of attacks against computer users increased significantly, which explains the reduction in share.

Gen:Variant.Adware.SwiftBrowse.1 is one representative of a highly variable malware family and, in respect of the absolute numbers of attacks compared to the previous half year, shows a small drop comparatively, but records a drop in share of 55.8% to 26.9% of all registered attacks. 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. Further details on this family have already been published in the G DATA Malware Report H1 2014.

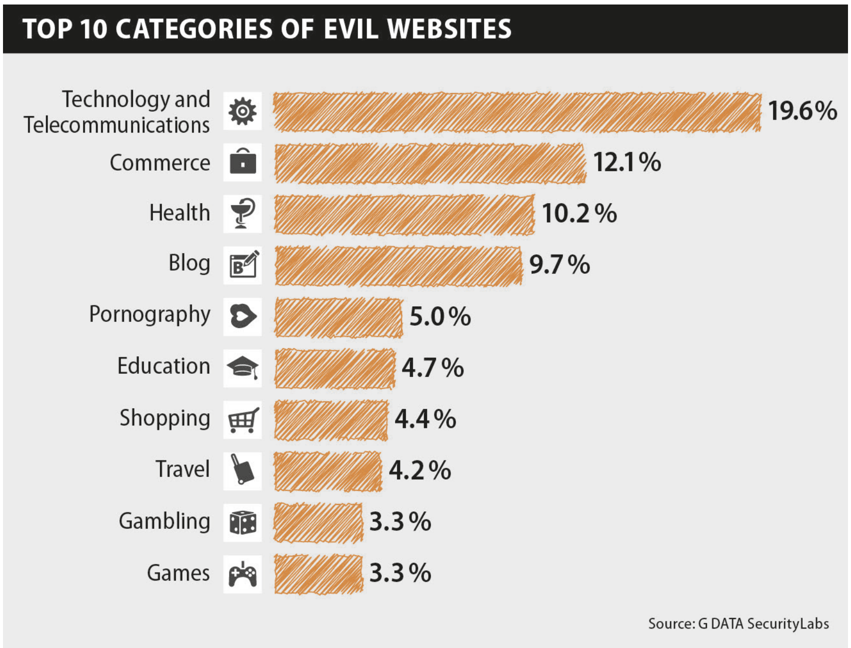
The absolute number of attacks by **Script.Application.Plush.D** increased by almost a third in the last six-month period, but its share remained the same. Every other representative in the Top 10 list is a new entry.

Malware belonging to the **BrowseFox/Browserfox family** was prominent in this recent half year, with three variants in the first six places. This malware installs plug-ins in Microsoft Internet Explorer, Mozilla Firefox and Google Chrome that change the browser settings to generate profit for attackers. The plug-ins change the home page and the search engine used by the user. The browser's security settings are also manipulated to permit "injections". During browser use, JavaScript is injected into the websites visited to display advertising.

WEBSITE ANALYSES

Categorisation by topic

In the second half of the year, the Top 10 websites classed as malicious represented 76.4% in total. More than one in three malicious websites therefore falls into one of the following topic areas.



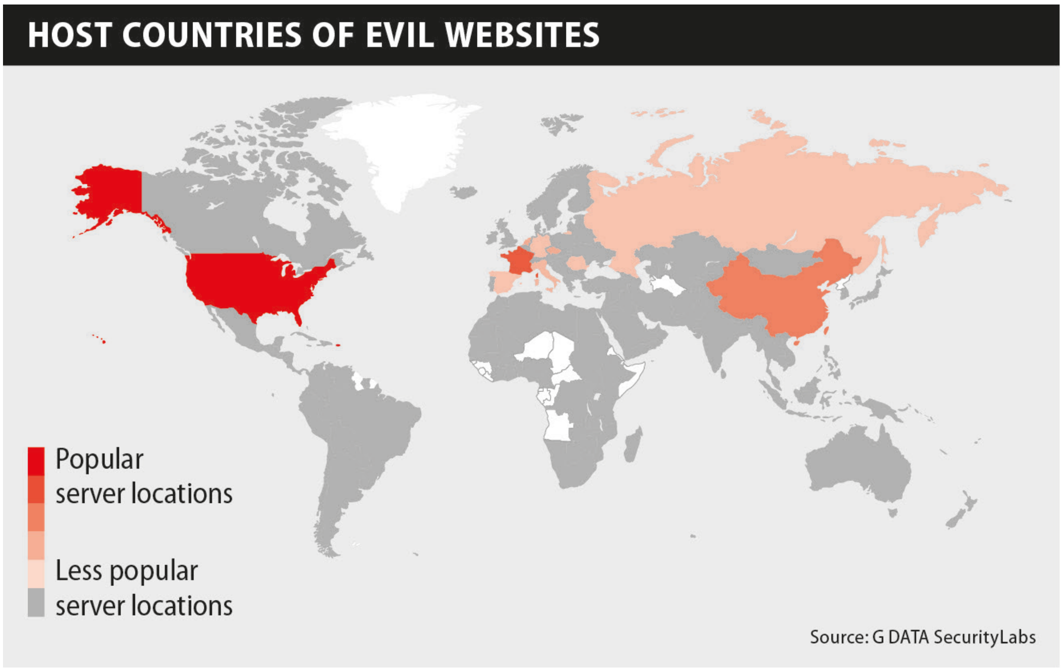
Source: G DATA SecurityLabs

On the whole, the categories represented remain the same, with one exception: the **Games** category once again climbed to **10th place**, replacing **Entertainment**. Both categories are closely related in terms of subject and also swapped places in the previous half year.

The large drop in the share of sites on the subject of **Gambling** is striking: in the second half of the year, they dropped from 24.3% and first place to **9th place** and now account for just **3.3%**.

Categorisation by server location

Attackers have to store their attack websites on servers, or hijack and manipulate existing sites. The following map shows the countries in which the servers with malicious websites are located. Phishing and malware sites are both shown as malicious here, and no distinction is made between domains specially set up and legitimate sites that have been misused.



HOST COUNTRIES OF EVIL WEBSITES

Source: G DATA SecurityLabs

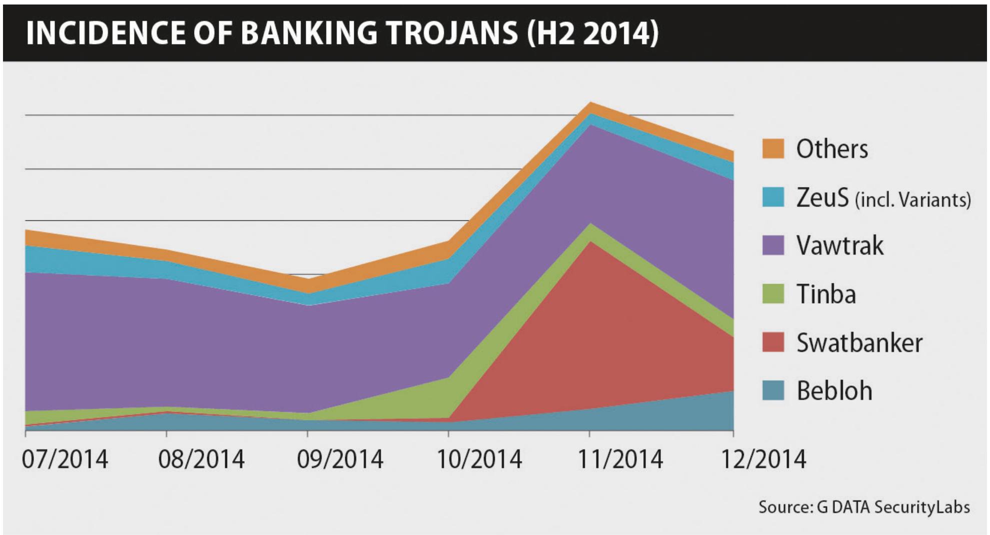
In the study of malicious websites in H2 2014, almost 45% of sites were hosted in the **USA**. Around one in ten sites (10.6%) were on servers in **France**, and **China** is the host country in third place on the list, with 6.1% of all hits. Germany is in 7th place (2.6%) in the current comparison.

BANKING

Trends in the Trojan market

There was a novelty in the banking Trojans market in the second half of 2014 – there were no significant innovations at all compared to previous years. In the past, more and more new Trojans have been appearing very quickly in this sector over the years, with new groups in the background using new attack methods. However, in recent months there have been few changes to report.

The infection numbers for **Tinba**, **Bebloh** and the different variants of the **ZeuS** family remain at a low, albeit constant, level. The **Vawtrak** Trojan, which has been spreading significantly since spring 2014, maintained its high infection rate. The group behind **Swatbanker** in the **Cridex** family continued with its attack method. This does not try to maintain constant infection rates, but carries out waves of attack over several weeks in a "pinprick" style, with infections being made via spam email.



Source: G DATA SecurityLabs

Hence it can be said that the market for banking Trojans has consolidated. There may be a number of reasons for this.

The frequent arrests of criminals in this sector ultimately reflect an increase in pressure from criminal prosecution services. In addition, in the wake of damages that have sometimes spread out of control, the banks have repeatedly improved their security measures in the field of online banking in recent years.

The sharpening of these security measures can sometimes be clearly seen, e.g. in two-factor authentication such as smsTAN or chipTAN. But even though the measures can clearly be seen, they still require a heightened degree of effort to be overcome. Such methods are generally overcome by **social engineering** attacks, where for example a customer is told that he supposedly needs to carry out a "test transaction" for security reasons: no money is meant to be moved here, but in fact that is what happens. However, fewer and fewer users fall for such tricks, reducing the number of successful attacks. Nevertheless, a single successful attack can mean a high yield for the attackers.

Other security measures used by financial institutes and payment service providers are invisible to the attackers, such as the banks' use of algorithms to **detect anomalies**. This can mean that banking transactions involving large amounts of money being moved abroad, for example, cannot be carried out without first checking whether the account holder has previously carried out any transactions to the target country currently in question. Such invisible security measures again reduce the number of successful attacks.

In summary: with attacks via banking Trojans, there is an increased level of risk for the criminals for a greater amount of effort and lower yield. The standstill felt in the market might also be to do with the fact that the criminals require a certain amount of expertise and infrastructure to still be able to carry out such attacks.

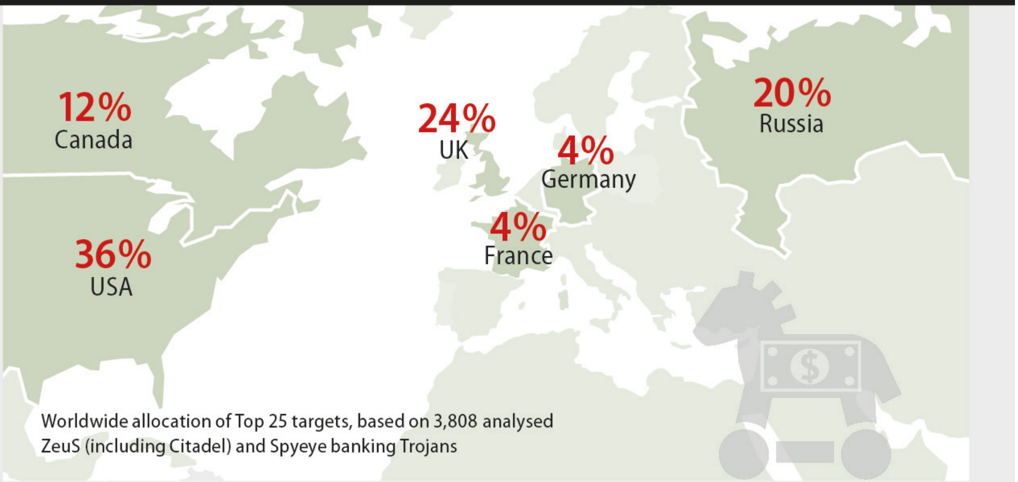
Notably, this does not mean for one minute that the risk for consumers has reduced: in December 2014 the number of averted attacks was 44.5% higher than in January.

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, attackers focus in particular on banking and financial services providers.

As was the case in the first half of 2014, among the 25 commonest targets of banking Trojans were primarily banks in the **English-speaking countries**, which accounted for 72% of instances (36% in the **USA**, 24% in the **UK**, 12% in **Canada**). As previously, there was one **German** bank in the Top 25. In total, there were seven new targets in the Top 25, including one **French** bank, two **Russian** banks, a **Russian** payment service, two banks from the **UK** and a bank from **Canada**.

COUNTRIES TARGETED BY TOP 25 BANKING TROJANS (H2/2014)



Worldwide allocation of Top 25 targets, based on 3,808 analysed ZeuS (including Citadel) and Spyeye banking Trojans

Source: G DATA SecurityLabs

As in the previous half year, the Bank of America was the commonest target of online banking Trojans. The next two targets in the list merely switched places: Citibank is now number two in the statistics, and PayPal number three.

Methodology

In total, 3,808 configuration files were extracted from samples of banking Trojans in the ZeuS family and its clone Citadel, and the SpyEye family. 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 them checked for their validity. Finally, there was a count of which domains occur in how many samples. This enables the relative frequency of the attacks to be determined. The domains are therefore ultimately assumed to be the attack targets. Countries of origin were also allocated to the Top 25 domains, for which the companies' own information on the relevant sites was used.

TOP 25 TARGETS OF BANKING TROJANS (H2/2014)

	Country	Rating Brand value via Brand Finance	Attack Frequency Relative attack frequency, based on 3,808 analysed ZeuS (including Citadel) and Spyeye banking Trojans
Bank of America bankofamerica.com	🇺🇸	**3**	🟩 5.88 %
Citi citibank.com	🇺🇸	**4**	🟩 5.80 %
PayPal paypal.com	🇺🇸	–	🟦 5.75 %
eBay ebay.com	🇺🇸	–	🟧 4.83 %
USAA usaa.com	🇺🇸	–	🟩 4.54 %
Barclays barclays.co.uk	🇬🇧	13	🟩 3.81 %
Chase chase.com	🇺🇸	**5**	🟩 3.73 %
Wells Fargo wellsfargo.com	🇺🇸	**1**	🟩 3.73 %
Royal Bank of Canada royalbank.com	🇨🇦	16	🟩 3.70 %
TSB Bank tsb.co.uk	🇬🇧	53	🟩 3.65 %
Lloyds lloydstsb.co.uk	🇬🇧	53	🟩 3.60 %
HSBC hsbc.co.uk	🇬🇧	**2**	🟩 3.57 %
Canadian Imperial Bank of Commerce cibc.com	🇨🇦	45	🟩 3.31 %
Capital One capitalone.com	🇺🇸	24	🟩 3.28 %
Scotiabank scotiabank.com	🇨🇦	30	🟩 3.10 %
Yorkshire Bank ybonline.co.uk	🇬🇧	395	🟩 2.91 %
Postbank postbank.de	🇩🇪	96	🟩 2.89 %
SunTrust suntrust.com	🇺🇸	87	🟩 2.73 %
Yandex yandex.ru	🇷🇺	–	🟦 2.68 %
WebMoney webmoney.ru	🇷🇺	–	🟦 2.68 %
Uralsib Bank uralsibbank.ru	🇷🇺	–	🟩 2.63 %
BNP Paribas bnpparibas.net	🇫🇷	7	🟩 2.60 %
Shipbuilding Bank sbank.ru	🇷🇺	–	🟩 2.57 %
RBK Money rbkmoney.ru	🇷🇺	–	🟦 2.57 %
Clydesdale Bank cbonline.co.uk	🇬🇧	393	🟩 2.49 %

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

Source: G DATA SecurityLabs