



SIMPLY
SECURE

G DATA **SECURITYLABS** MALWARE REPORT

HALF-YEAR-REPORT
JANUARY – JUNE 2015

G DATA SECURITYLABS

CONTENTS

CONTENTS	1
AT A GLANCE	2
MALWARE STATISTICS	3
Risk Monitor	3
WEBSITE ANALYSES	5
Categories of malicious websites.....	5
Categorization by server location.....	7
BANKING	9
Trends in the Trojan market.....	9
Targets of banking Trojans.....	10
Methodology.....	10
G DATA BankGuard thwarts damages of more than 100 million €.....	13
EXPLOIT KITS	14
Conclusion and outlook	15

AT A GLANCE

- The first half of 2015 saw 3,045,722 new strains of malware. This is a growth of slightly more than a quarter (26.6%) below the record of the second half of 2014. But it is about two thirds (+64,8%) higher than the number of the same period last year. On average this is 12 new malware strains per minute. We expect that the number of new malware strains will be well above the level of 2014.
- The total of all malware strains since 2006 is now 22,393,098.
- The Top 10 of prevented malware attacks is dominated by Adware and Potentially Unwanted Programs (PUP). Dealply and Graftor are the most prevalent families in this field.
- Health care was the topic most prevalent of all websites identified as malicious (26,6%). Websites of this category also launched campaigns promising a rather dubious rain of money.
- The topic "personal advertising and dating" is new in the Top 10. Sites from this category offer to install paid premium services or launching expensive phone calls.
- Malicious and fraudulent websites are still most frequently hosted in USA, China, and France. Ukraine with 5% is new in the Top 10 and made it to position 4. It is unclear whether and how this relates to the political havoc in this region.
- The number of attacks carried out by Banking Trojans will presumably be rising in 2015 for the first time since 2012.
- The Swatbanker family caused an all-time-high of repelled attacks in March 2015, due to successful email campaigns. Its main targets were bank customers from Germany, Austria, and Poland. The activities continued until June 2015.
- During the first half year of 2015 the sum of prevented damage by BankGuard passed the mark of 100 million Euro.
- Exploits for vulnerabilities are integrated into exploit kits after just a few days. Users who do not keep their systems up-to-date easily fall victim to cyber criminals. Attackers use exploit kits to silently and automatically check PCs for a large number of vulnerabilities at a time and to subsequently compromise PCs, e.g. during the visit of a website (drive-by-infection).
- The vulnerabilities in Adobe Flash were most frequently abused to silently, and automatically attack and compromise PCs (Exploit). Exploits based on Java were scarcely used, due to the implemented "click-to-play" function default in the most popular browsers. "Click-to-play" might also help to minimize the use of Flash exploits in the near future.
- On January 21st the Angler Exploit Kit integrated an exploit for a new and undisclosed vulnerability in Adobe Flash (CVE-2015-0311). In the subsequent weeks the experts of the G DATA SecurityLabs measured new records for the prevention of exploits.
- Another peak in the number of repelled exploit was caused by the integration of the Nuclear Exploit Kit in advertisements of a Google AdSense content supplier. The attackers deployed the Nuclear Exploit Kit with the aim of infecting millions of users with malware.

MALWARE STATISTICS

The number of new malware variants in the first half of 2015 is significantly smaller than the number for the previous half year, and to an extent harks back to the figures prior to the perceived anomaly of H2 2014. Overall 3,045,722 new signature variants were registered.

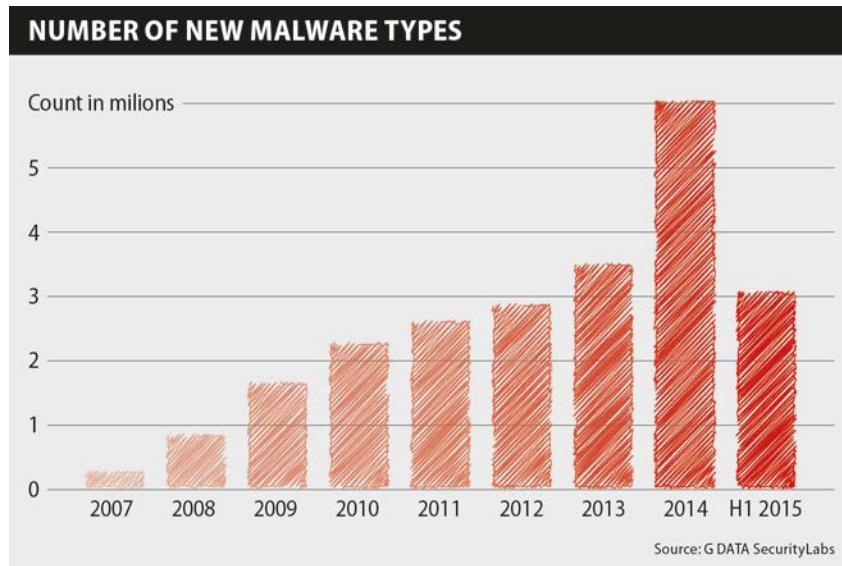


Figure 1: Number of new malware types

This is a growth of slightly more than a quarter (26.6%) below the record of the second half of 2014. But it is about two thirds (+64,8%) higher than the number of the same period last year. On average this is 12 new malware strains per minute. We expect that the number of new malware strains will be well above the level of 2014. The total of all malware strains since 2006 is now 22,393,098.

Risk Monitor

The risk monitor shows the Top 10 repelled attacks against computer users involving G DATA security solutions and activated feedback¹. The most frequently repelled attacks in the first half of 2015 are shown below. An up-to-date breakdown by individual month is always available on the G DATA SecurityLabs website².

The way of counting in this section differs from that for the overall number of malware strains, because the numbers of actual attacks are evaluated here rather than the number of new malware strains. A single malware variant can have a major effect when the number of attacks is counted, even when the family has probably produced only few (new) variants.

¹ 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 repelled, 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.

² <https://www.gdatasoftware.com/securitylabs/statistics>

It is notable that the Top 10 for this half-year make up only 43.5% of all reported incidents, and so cover 21.5% fewer reported incidents than in the previous half-year. This indicates greater variance in the malware, which is counter to the focus being on specific strains of malware.

Rank	Name	Percent
1	Script.Adware.DealPly.G	16,2%
2	Adware.BrowseFox.BU	8,0%
3	Script.Application.Plush.D	5,3%
4	Gen:Variant.Adware.Graftor.173090	3,2%
5	Gen:Variant.Adware.Graftor.159320	3,1%
6	Gen:Variant.Adware.Graftor.159134	2,1%
7	Adware.RelevantKnowledge.A	1,6%
8	Win32.Application.OpenCandy.G	1,6%
9	Win32.Adware.IObit.A	1,5%
10	Win32.Application.Dealply.H	0,9%

Table 1: Top 10 attacks reported to MII

The trend in "potentially unwanted programs" (PUPs) was again confirmed in this half-year. The mass distribution of malware in this category is a direct continuation of the numbers for 2014. Whereas

Gen:Variant.Adware.SwiftBrowse.1 topped the rankings in the last report, with 26.9%, first place in this half-year goes to **Script.Adware.DealPly.G**. This was previously in 7th place, and its frequency has increased by 12.6%.

Also conspicuous is the marked presence of **Gen:Variant.Adware.Graftor** malware, which is related to **BrowseFox** adware. Typically this malware is supplied along with a wide range of freeware and is installed voluntarily to a greater or lesser extent. Once embedded in the system, the installed browser is manipulated and system services and drivers that are used for things such as a local proxy are installed. One of the forms of manipulation mostly used is to replace the start page and default search engine in the browser. Furthermore, advertising is incorporated in various places by the adware and displayed in pop-ups, for example.

WEBSITE ANALYSES

Categories of malicious websites

Recent half-years in this investigation have held relatively few surprises – the attackers have seemingly focused on the exploitation of websites with technical or gambling content. However, evaluation of the first half-year of 2015 reveals something new:

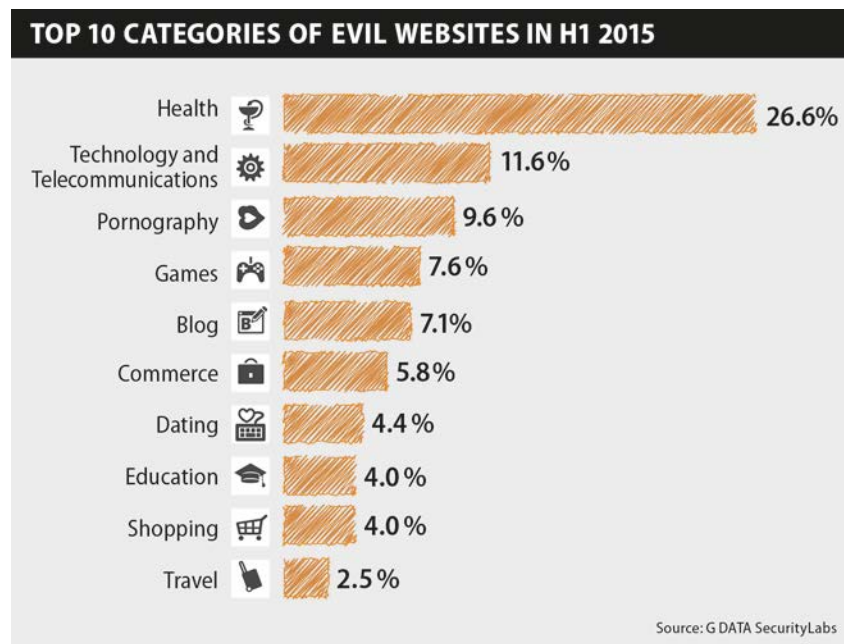


Figure 2: Top 10 categories of evil websites

The key statistical data shows that the current Top 10 categories cover an 83.1% share of all classified websites.

This is an increase of 4.7% compared to the second half of 2014 and, after H2 2012 (88.6%), is the second highest value since the investigation began. The remaining 16.9% cover 63 other subject areas.

The **health care** category currently takes 1st place, with a share of 26.6%. This means that more than one in four evil websites belongs to this category. One campaign that we have identified in this category is the so-called Money Rain campaign. With this, websites promise various methods of supposedly making it "rain money" on the reader with great ease. The design of these sites changes at irregular intervals, but the premise always remains the same.

INVESTOREN-JOURNAL

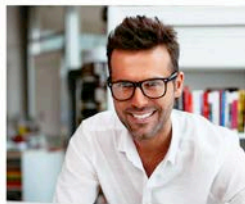
Startseite	Finanzen	Technik	Wirtschaft	Medien	Alle geschichten	Portfolio	Markt-news	Video	Investieren	Mehr	
MARKT-TICKER											
Dow	-3.35	Nasdaq	-8.52	S&P 500	+1.59	Treasury	-0.43	Oil	-1.55	U.S. Dollar	+0.041
10,891.62	+9.82%	2,426.23	+8.35%	1,171.00	+8.14%	10-year yield	3.54%	Price/barrel	\$74.10	1 Euro =	\$1.2558

Entdecken Sie, wie Marco Lehrer 2300 € pro Woche ZUSÄTZLICH verdient!

Marco Lehrer, 35-jähriger Mann aus Grafenau, gibt sein Geheimnis preis ...

Meine E-Mail-Adresse lautet:

...@mail.com



Neue Welt des schnellen Profits!

Interviewt von Manuela Kaiser
12. Oktober 2014

Marco Lehrer aus Grafenau hat erreicht, wovon viele Menschen nur träumen. Er verdient mehr als sein Vorgesetzter und seine Freunde. Marco war auf der Suche nach der richtigen Gelegenheit, um nach seiner Arbeitszeit **zusätzliches Geld zu verdienen** und trotzdem noch genug Freizeit für seine Familie und Hobbys zu haben. Er sagte: „Als Anwalt liegt mein Einkommen über dem Durchschnitt, jedoch arbeitet meine Frau nicht, da sie sich Zuhause um unser Baby kümmert. So reicht mein derzeitiges Einkommen nicht dafür aus, den Lebensstil, den wir führen, aufrechtzuerhalten.“

Aber all das änderte sich, als Marco den **Handel mit Binäroptionen** entdeckte.

Mehr als
1257400
Menschen handeln bei

Sagen Sie JA zu einem zusätzlichen Einkommen!

JETZT BEGINNEN

Keine Vorkenntnisse nötig
Der Erfolg ist nicht garantiert. Bitte lesen Sie die Geschäftsbedingungen.



Screenshot 1: A Money Rain campaign from early 2015

Attackers do not only exploit websites in the health care category with this type of scam, but 37% of websites that are clearly connected with Money Rain do come from this category. Screenshot 1 shows a page with one of the versions of this scam, in which there are similarities to the system used in previous campaigns (such as use of the same email service, for example³). The campaigns are directed at people who want to work from home and attackers try to lure their victims with more or less shady promises for cash.

In one of the dubious money campaigns, the initiators even try to use a YouTube video that they have created themselves

to lend a serious tone to the whole undertaking. "Breaking news" for the supposedly rapid "rain of money" is presented in the style of a news update, as shown in Screenshot 2.

Another surprise is the subject area of **personal advertising and dating**, a category that has not previously appeared. This heading covers websites on which romantic or sexual contacts can be made, along with advertisements for paid-for services such as premium call numbers for local services. Pornography, ranked third in the current evaluation, is associated with the cliché that websites with adult content are more dangerous than others. The experts at G DATA SecurityLabs have debunked this myth.⁴ Dangerous websites lurk everywhere.

Alleinerziehende Mutter aus Berlin verdient €7.650/Monat von zu Hause.

Abonnieren 10

477 Aufrufe

Veröffentlicht am 26.02.2015

Alleinerziehende Mutter aus Berlin verdient €7.650/Monat von zu Hause. Sie werden es nicht glauben, wie Sie das schafft!

► Sign Up: <http://.../reg...>

Screenshot 2: The video shows in "Breaking news" style how easy it is purportedly to earn money

³ G DATA SecurityBlog: <https://blog.gdatasoftware.com/blog/article/dubious-casino-tips-being-distributed-via-spam-email.html>

⁴ G DATA SecurityBlog: <https://blog.gdatasoftware.com/blog/article/two-major-it-security-myths-debunked.html>

Categorization by server location

When attackers exploit websites to cause damage to computer users through malware or phishing attacks, they have numerous options for doing so; however, one of two situations always underlies what they do:

- 1) The attackers have taken over a legitimate website and are attacking the often numerous visitors to the site. However, they are also damaging the actual operator – by attacking the infrastructure, through loss of reputation, and possibly financially as well through increased traffic to the website.
- 2) The attackers have set up their own website to serve their purpose. In doing so they bear the costs of the infrastructure themselves and generally only cause damage to the potential victims who are lured or diverted onto the site. In the underground, shady service providers offer ways of bringing visitors to a website. This costs just a few Euros for thousands of visitors.



Figure 3: Host countries of evil websites

So-called malvertising campaigns fall into Category 1. This artificial word is made up from "malware" and "advertising" and describes the distribution of malware across advertising networks. The misuse of the **Google AdSense** network⁵ has been particularly conspicuous in the first half of 2015 in this regard. Because of the widespread distribution of this advertising service, visitors to even prominent websites have been exposed to infection by the **Nuclear Exploit Kit**. This incident has shown once again that advertising is not just tedious but also dangerous.

The following evaluation shows whereabouts in the world the majority of evil websites that have been reported to G DATA SecurityLabs as malicious or fraudulent in the first half of the year are based. The location of the website indicates where the website's server is⁶:

⁵ G DATA SecurityBlog: <https://blog.gdatasoftware.com/blog/article/staying-alert-when-buying-banners-googles-advertising-service-misused-for-distributing-malware.html>

⁶ The top level domain (e.g. ".de" or ".fr") indicates where the domain name has been registered and is not considered here. Furthermore, no distinction is made between whether the site has been hijacked or specially set up for an attack.

Some countries are especially attractive targets for cyber criminals, as both the infrastructure and the cost of web space are very favorable there. Also the national laws relating to cybercrime and associated matters are of importance to the criminals and their choice. 43.3% of all evil websites are located on servers in the **USA**. This value is at almost the same level as in the previous half-year. **China** has become more attractive as a host country and is now in 2nd place, with 9.5%. **France** on the other hand has dropped to 3rd place (8.2%). Overall there has been as little change in the top placings as there has in the conditions specified above.

However, fourth place is interesting. The experts at G DATA SecurityLabs have recorded an increase in malicious websites on servers in the **Ukraine**. In H1 2015, the share was 5%, giving it 4th place in the list. In previous years, however, the **Ukraine** played no part worth mentioning in this evaluation. An association with the continuing political conflict in the Ukraine and the numerous media reports concerning a cyberwar between the **Ukraine** and Russia cannot be ruled out.

BANKING

Trends in the Trojan market

The market share for the various families of banking Trojans also changed in the first half of 2015. It began where it left off in 2014, with a relatively high number of infections by the **Vawtrak** family. The level of **Vawtrak** infections then appeared to almost halve in mid-February. **Bebloh** also halved from March compared to the previous month, to then become almost insignificant in the evaluation for June by G DATA SecurityLabs. **Tinba** also dropped in significance, in this case from April. At the same time, **Gozi** became visible again in the first half of the year for the first time in a long time. **Zeus** and its variants remained at the usual level, with the **Zeus-VM** variant reaching a peak in June.

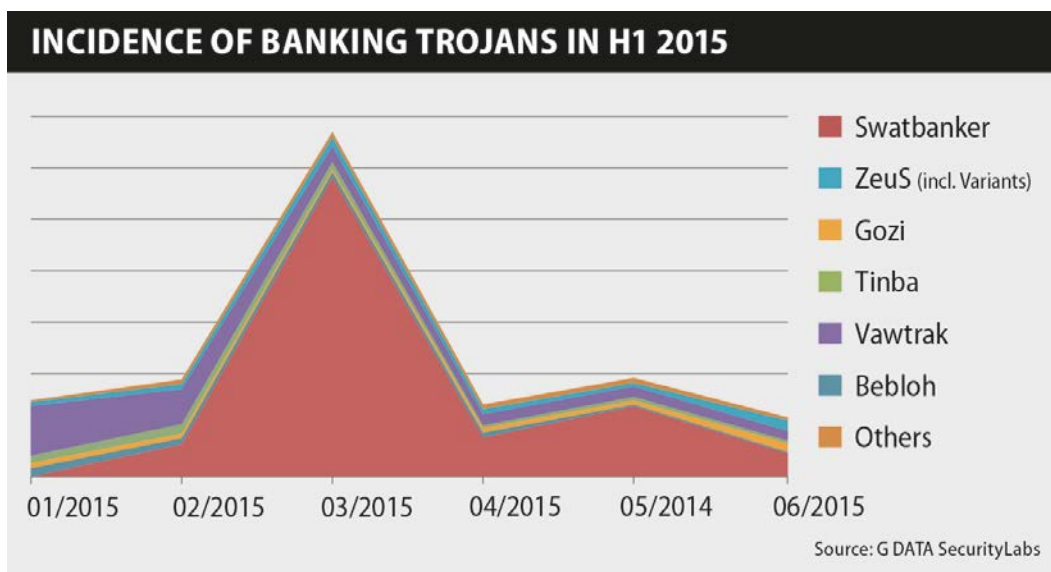


Figure 4: Incidence of banking Trojans

The most conspicuous occurrence in the first half of 2015 started in late February, when a new wave from the group linked to **Swatbanker**, the **Cridex** group, began posing a risk for PCs. Previously, waves of attacks by email had not been unusual for this Trojan, but this wave was so successful that in March 2015 the highest number of repelled banking Trojan attacks since records began was measured. Also unusual was the fact that the wave did not stop within a few weeks as usual, but carried on until mid-June. Also, shortly before the wave of attacks ended, there was another unusual occurrence: the attackers apparently were targeting computers in the German Parliament's intranet⁷. Whether or not there was a connection to a previously reported attack on the Federal Parliament⁸ remains unclear.

⁷ G DATA SecurityBlog: <https://blog.gdatasoftware.com/blog/article/banking-trojan-has-targeted-bundestag.html>

⁸ https://de.wikipedia.org/wiki/Cyberattacken_auf_den_Deutschen_Bundestag

Targets of banking Trojans

Every banking Trojan attacks specific targets depending on its configuration. Target in this case means that the banking Trojan carries out its attacks when the user of an infected PC visits a predetermined website. The malware then deploys activity adapted to that target.

If it is assumed that every family of Trojans occurs with the same frequency, i.e. if the number of occurrences is normalized, a picture appears that is similar to 2014 H2. In this case the 20 most frequent targets with the highest probability of attack come from the English-speaking countries – with the exception of two Spanish banks. First place on the list goes to **Wells Fargo**. Besides banks, the auction portal **eBay** and payment service provider **PayPal** appear on the list (c.f. Table 2). As the past half-year of our measurements was largely dominated by the **Swatbanker** wave described above, the 20 **Swatbanker** targets correspond exactly to the 20 most endangered targets. **Swatbanker** exclusively attacks banks in Germany, Austria and Poland. The target of attack with the highest overall probability of infection with a banking Trojan was **Volksbank's fiducia.de** portal, closely followed by the other **Swatbanker** targets (see Table 3).

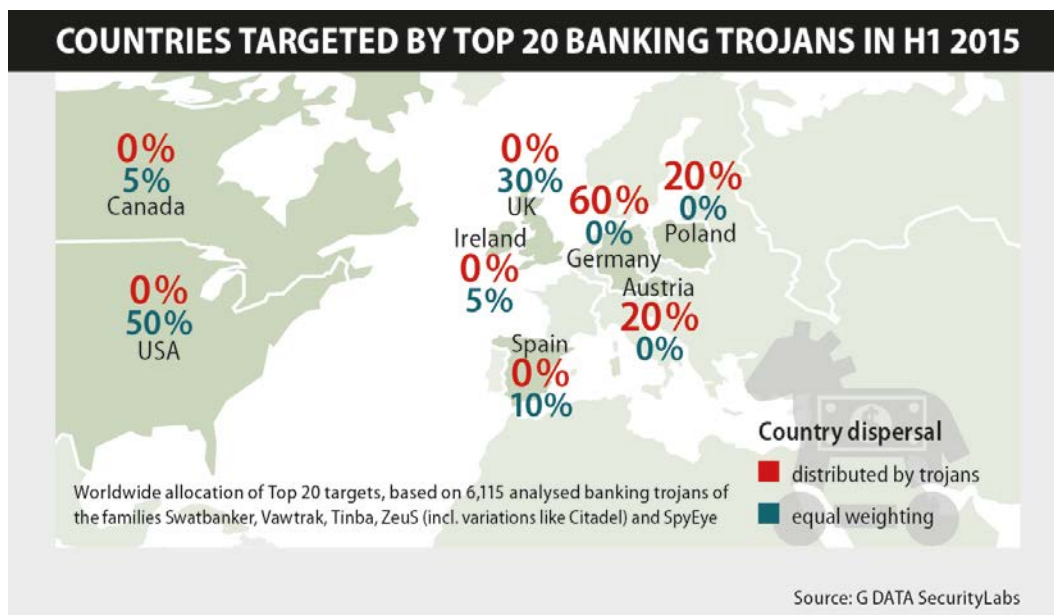


Figure 5: Countries targeted by Top 20 Banking Trojans








Methodology


The method of analysis has been updated for this Malware Report. The list of supported banking Trojan families has been expanded to include the following families: **Swatbanker**, **Vawtrak**, **Tinba**, **ZeuS** (incl. variants such as **Citadel**) and **SpyEye**. Overall 6,115 configuration files were decrypted and analyzed. The configuration files contain a list of target sites (i.e. websites of banks, payment service providers etc.) that are attacked using special malicious code (called web injects)⁹. In one case it was assumed that all Trojans occurred in equal distribution (c.f. Table 2). But for the graphic for the distribution of Trojans, the level of distribution of the respective family of Trojans is taken into consideration (c.f. Table 3).

⁹ Web injects involving so-called wild cards or regular expressions were mapped onto other web injects without wild cards where possible. When such web injects matched multiple domains, they were put into groups where they were checked manually for plausibility. In addition, the domains for the target sites were extracted and checked for validity. Finally a count was made of which domains (or groups) occur in how many samples.

The percentage value given corresponds to the probability of a target that is infected with a banking Trojan also being on the list of attack targets. The country of origin is also allocated in the Top 20 (c.f. Figure 5)¹⁰.

TOP 20 TARGETS OF BANKING TROJANS IN H1 2015 (TROJANS EQUALLY WEIGHTED)

	Country	Rating Brand value via Brand Finance	Attack Probability Based on the analysis of 6,115 samples from the families Swatbanker, Vawtrak, Tinba, ZeuS (incl. variants), SpyEye
Wells Fargo wellsfargo.com		1	35.28 %
HSBC hsbc.co.uk, hsbc.com, hsbc.com.hk, ...		3	34.07 %
Lloyds Banking Group lloydstsb.co.uk, halifax-online.co.uk, ...		35	32.13 %
Barclays barclays.co.uk		13	30.05 %
RBS Group (RBS, NatWest, Ulster) nwolb.com, rbsdigital.com, ...		60	27.92 %
PayPal paypal.com, paypal.co, paypal.com.mx		-	27.55 %
Bank of America bankofamerica.com		6	27.32 %
Chase chase.com, chasecanada.ca, chaseonline.com		7	27.08 %
Citi citibank.com, citibank.com.au, citibank.com.sg		5	25.98 %
TD Bank tdcanadatrust.com		18	24.18 %
U.S. Bancorp usbank.com		46	24.04 %
Citizens Bank citizensbankonline.com		264	23.20 %
smile smile.co.uk		-	22.60 %
Fifth Third Bank 53.com		111	22.11 %
The Co-operative bank co-operativebank.co.uk		114	22.02 %
BBVA bbvanetoffice.com, bbva.es, ...		28	21.47 %
SunTrust suntrust.com		93	20.61 %
eBay ebay.com, ebay.de, ebay.co.uk, ebay.ca, ...		-	20.10 %
Santander ES gruposantander.es		10	19.79 %
Allied Irish Banks aib.ie		181	19.77 %

Category:  = Bank  = E-Payment  = Auction

Source: G DATA SecurityLabs

Table 2: Top 20 targets of banking Trojans (Trojans equally weighted)

¹⁰ The companies' own information on their respective sites was used for this. In case of doubt with the grouping, the location of the parent company was taken as the country of origin. The Brand Rating comes from Brand Finance (<http://www.rankingthebrands.com/PDF/Brand%20Finance%20Global%20Banking%20500,%202015.pdf>), where the rating of the parent company was used and not a separate rating. Where multiple labels exist for domain groups, the highest-placed brand was used as the basis.

TOP 20 TARGETS OF BANKING TROJANS IN H1 2015 (AFTER TROJAN DISTRIBUTION)

	Country	Rating Brand value via Brand Finance	Attack Probability Based on the analysis of 6,115 samples from the families Swatbanker, Vawtrak, Tinba, ZeuS (incl. variants), SpyEye
Volksbanken (Fiducia) fiducia.de		42	71.91 %
Deutsche Bank Gruppe deutsche-bank.de, norisbank.de, ...		19	71.90 %
GE Capital gecapital.de		-	71.88 %
Targobank targobank.de		77	71.80 %
Flessabank flessabank.de		-	71.77 %
Bank1Saar bank1saar.de		42	71.77 %
Commerzbank commerzbanking.de, commerzbank.de, ...		75	71.77 %
Sparda-Banken sparda.de		42	71.77 %
PKO Bank ipko.pl		115	70.61 %
mBank mbank.pl		310	70.55 %
ING PL ingbank.pl		26	70.55 %
Citi PL citibankonline.pl		5	70.55 %
DKB dkb.de		176	70.44 %
Sparkassen DE berliner-sparkasse.de, haspa.de, ...		174	69.84 %
Volksbanken (GAD) gad.de		42	69.77 %
comdirect comdirect.de		75	69.76 %
Bank Austria bankaustria.at		152	69.76 %
BAWAG PSK bawagpsk.com		322	69.76 %
Sparkasse AT sparkasse.at		78	69.76 %
Raiffeisen raiffeisen.at		110	59.99 %

Category:  = Bank  = E-Payment  = Auction

Source: G DATA SecurityLabs

Table 3: Top 20 targets of banking Trojans (regarding Trojan distribution)

G DATA BankGuard thwarts damages of more than 100 million €

Customers of G DATA are protected against banking Trojans by BankGuard technology, which has been in use since April 2011 and is patented¹¹. BankGuard repels tens of thousands of attempted attacks every year. There was a total of 182,457 thwarted attacks to the end of the first half of 2015.

In a study by **Google**, an average likelihood of success of 13.78% was calculated for comparable attacks¹². At the same time, the **Federal Criminal Police Office** considers the average total damages to be some €4,000 per case.¹³ When these figures are added up, the total damages prevented by BankGuard exceed the 100 million Euro mark (€100,570,298.40).

In Figure 6, it can be seen by extrapolating the previous half-year to the year as a whole that the number of cases will increase in 2015 for the first time since 2012. **Swatbanker** from the **Cridex** family is primarily responsible for this. The Trojan has now been causing trouble since January 2014 and the waves of attack are clearly gaining in effectiveness. As banks in **Germany, Austria** and **Poland** have been the main targets of the attacks, customers of these can currently be considered especially at risk. Banks from **English-speaking countries** are the next targets of attack and are mainly targeted by **Vawtrak**.

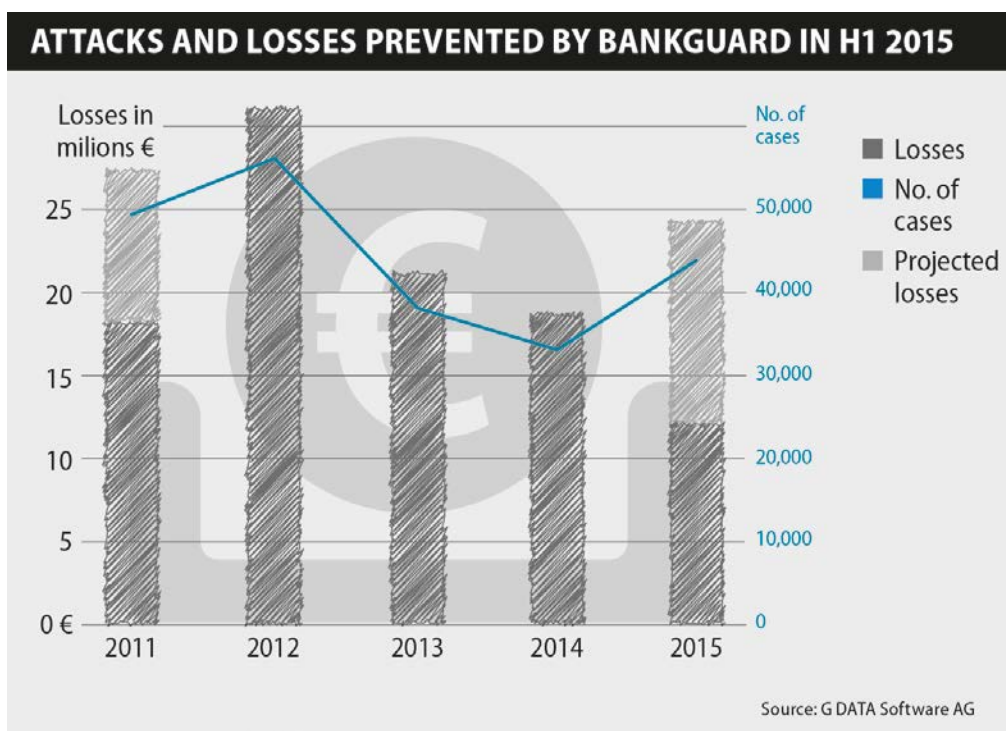


Figure 6: Attacks and losses prevented by BankGuard

¹¹ Patent no. US8898781

¹² http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf

¹³ http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

EXPLOIT KITS

G DATA's Exploit Protection provides generic protection against the automated exploitation of software vulnerabilities. Such exploits are offered in underground forums in competing product lines called exploit kits. Analysis of the repelled attacks shows that three exploit kits were especially dominant in the first half of 2015 – **Angler, Nuclear and Neutrino**. Other exploit kits for which attempted attacks have been registered were **RIG, Sweet Orange, Magnitude, Niteris, Fiesta and Huanjuan**.

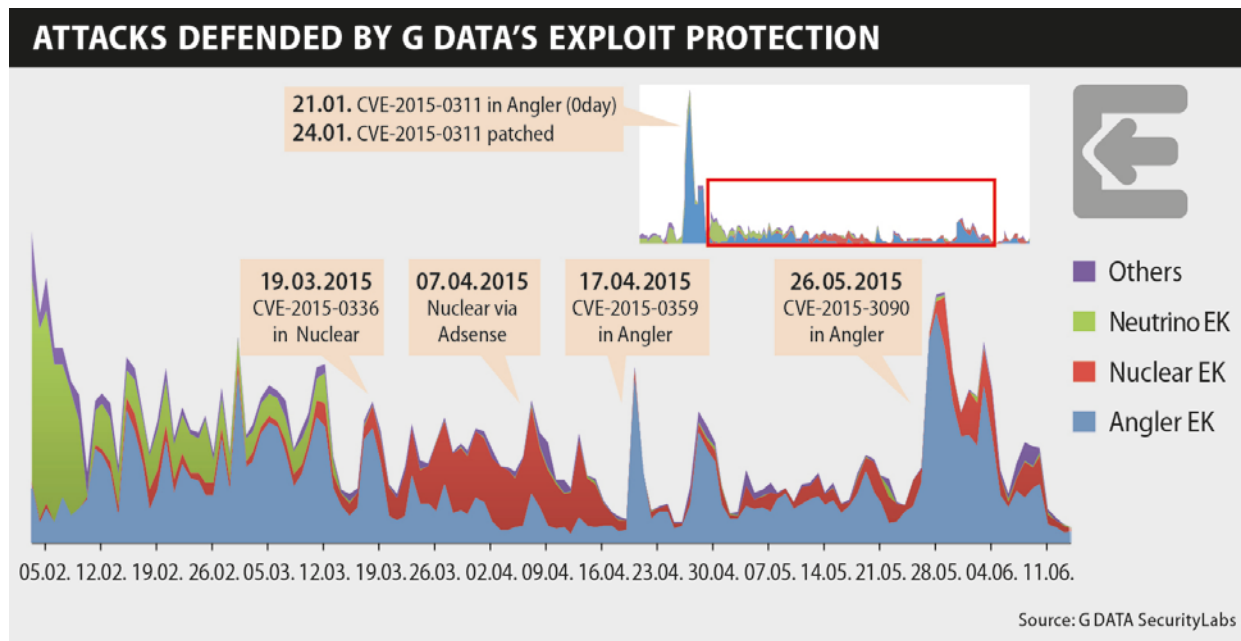


Figure 7: Attacks defended by G DATA's Exploit Protection

Adobe Flash has continually been in the attackers' focus during this half-year. This means that a particularly large number of exploits has been developed for this platform, as the chances of successfully infecting a PC have been particularly high. Previously the main talking point in this regard involved Java because of the continual emergence of new security holes. However, the attractiveness of Java might have declined simply because browsers have more and more protective functions built into them now. For example, since version 26 of Firefox appeared at the end of 2013, "click to play" has been enabled by default¹⁴. This means that, prior to running Java applets, users must confirm that they really want them to be executed. However, as attackers using exploit kits are relying on the drive-by infection being carried out in the background, invisible to the user, and requiring no user interaction, such innovation is making Java less attractive for the attackers. With Google Chrome, "click to play" for Java applets has been the standard for some time. Since Chrome version 42 in April 2015, Java support has been removed altogether.¹⁵ No general "click to play" for Java has been implemented in Internet Explorer, but at least the execution of outdated versions has been prevented since August 2014.¹⁶

Consequently attackers have switched to Adobe Flash as the preferred attack vector. In the browser default configuration, there was still no "click to play" for this, but there has been a sufficiently large number of security holes and program errors (or bugs) that can be exploited to take control of computers. The exploits used can also

¹⁴ https://bugzilla.mozilla.org/show_bug.cgi?id=914690

¹⁵ <https://www.java.com/de/download/faq/chrome.xml>

¹⁶ <http://blogs.msdn.com/b/ie/archive/2014/08/06/internet-explorer-begins-blocking-out-of-date-activex-controls.aspx>

be very successful at circumventing the security mechanisms in current Windows versions, such as DEP, ASLR and CFG¹⁷. As a result, Flash exploits extend beyond the boundaries of the browser in terms of functionality.

The largest number of repelled attacks in the first half of the year can be traced back to the **Angler Exploit Kit** campaign in January. On January 21, a previously unknown and unclosed Flash vulnerability called **CVE-2015-0311/APSB15-03**¹⁸ was made available to all users of the kit. Records of repelled attacks show how dangerous such zero day exploits are. On January 24, a corresponding update, 16.0.0.296, which could be used to remove the vulnerability, was published by Adobe. Shortly afterwards, in early February, the exploit for this now closed hole and several older Flash exploits were added to the **Neutrino Kit**. Even at this point, relatively high numbers of infections were being achieved. Many computer users had still not brought their version of the Adobe product fully up to date and hence remained vulnerable to this attack.

Another zero day attack on Flash, involving the **Huanjuan Exploit Kit** via the **CVE-2015-0313/APSB15-02** vulnerability¹⁸, has been around since January 13. However, the number of affected users was small.

Also of note is a campaign for the **Nuclear Exploit Kit**. A security hole for which Adobe had already released a patch on March 12 was exploited from March 19 by the **Nuclear Exploit Kit**. In this case the attackers managed to distribute the exploit via the **Google AdSense** network. This extremely popular advertising platform is used by numerous providers of popular websites. In this case, website visitors were attacked by the advertising being displayed. This coup resulted in a clear peak in repelled attacks.¹⁸

Even more Flash vulnerabilities were identified later in the half-year. These were also published in exploit kits shortly after the release of a patch by Adobe to remove the vulnerability. Hence only users that did not have the patch were affected, showing once again how important the timely installation of official updates and patches is for computer users.

As an example, the vulnerability **CVE-2015-0359/APSB15-06**¹⁸ was removed by Adobe on April 14, yet just three days later, on April 17, it was integrated into **Angler**, and into **Neutrino** on April 27. Vulnerability **CVE-2015-3090/APSB15-09**¹⁸ was closed on May 12. **Angler** integrated an exploit first, on May 26, followed shortly afterwards by **Neutrino** on May 29. Other subsequent examples include the combination of vulnerabilities **CVE-2015-3104** and **-3105/APSB15-11**¹⁸, which was removed by Adobe. In this case, the patch dated June 3 was followed by integration of the exploit into the **Magnitude Exploit Kit** on June 16. The final patch of the half-year released by Adobe was for **CVE-2015-3113/APSB15-14**¹⁸ on June 23. The first integration, again by the **Magnitude Exploit Kit**, followed four days later on June 27, followed two days later by **Angler**.

Conclusion and outlook

Attacks on Adobe Flash posed the greatest threat for web users in the first half of 2015. Particularly effective in the exploitation of this was the **Angler Exploit Kit**, especially with the prominent attack involving the zero day exploit in January. Furthermore, **Neutrino** has played a part since mid-March, but was then increasingly superseded by **Nuclear**. As the people behind **Angler** have acted very effectively and updated their exploit kit in very short cycles, a major role for this can also be expected in the second half of the year.

¹⁷ <https://blog.coresecurity.com/2015/03/04/exploiting-cve-2015-0311-a-use-after-free-in-adobe-flash-player/>

¹⁸ <https://helpx.adobe.com/de/security/products/flash-player.html>