











# G DATA PC Malware Report





## Contents

	<b>At a glance</b>	3
	<b>New signature variants – has everything levelled off again?</b>	4
	<b>Risk monitor</b>	6
	<b>Categories of evil websites</b>	8
	<b>Categorisation by server location</b>	10
	<b>Banking</b>	
	<b>Banking Trojan trends</b>	12
	<b>Targets of banking Trojans</b>	14
	<b>Methodology</b>	15
	<b>Exploit Kits</b>	16



## At a glance



- In the second half of 2015, experts at G DATA SecurityLabs recorded 2,098,062 new signature variants. This number is 31% less than in H1 2015.
- At 5,143,784, the total number of new signature variants in 2015 was only slightly less than the figure for 2014.
- A look at the reported attacks shows that the Risk Monitor Top 10 covers 39.6% of all those reported. PUPs and adware continue to be dominant here.
- Script.Adware.Dealply.G takes 1st place in the ranking, with 22.9% of all attacks assessed. This browser add-on, which is frequently installed without being noticed, transmits and uses user data that can then be used for various purposes by the developer company.
- In the categorisation of evil websites, the Gambling category is particularly prominent. In the last six months, it has jumped from 13th place to 1st place (18.7%) in the rankings.
- When looking at the countries in which the servers with evil websites are located, the USA was again out in front in this half-year. Around 57% of recorded attacks originated from here. Germany is in 3rd place, with 3.9%.
- The banking Trojan Swatbanker, which was responsible for the highest number of averted attacks since records began (March 2015), almost completely disappeared from the picture.
- Another massive attack by Dridex was recorded at the end of the year. The banking Trojan has been seen before, and it can be assumed that it will continue to be active.
- The assessment of targets of banking Trojans confirms the observation that the Anglophone region continues to be the main target of the attackers. 80% of all target sites identified came from English-speaking countries.
- The Neutrino, Angler, Nuclear and Magnitude exploit kits were particularly prominent in the second half of 2015.
- The attacks on Hacking Team led to information on previously unknown vulnerabilities ending up in the hands of cyber criminals, being built into exploit kits and causing one of a number of waves of attack.
- It was conspicuous in this half-year that two major waves of attack (evidently in the Hacking Team case, presumably in the case of APT28) can be traced back to attack tools used at the government level that have been adapted by cyber criminals.



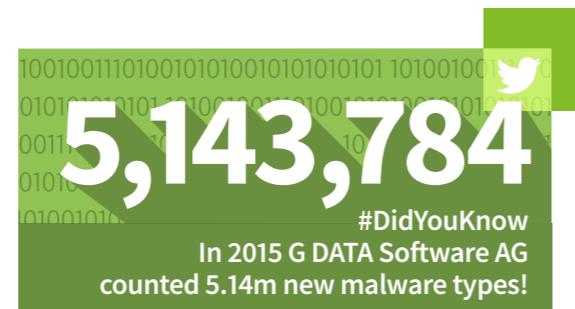
## New signature variants – has everything levelled off again?



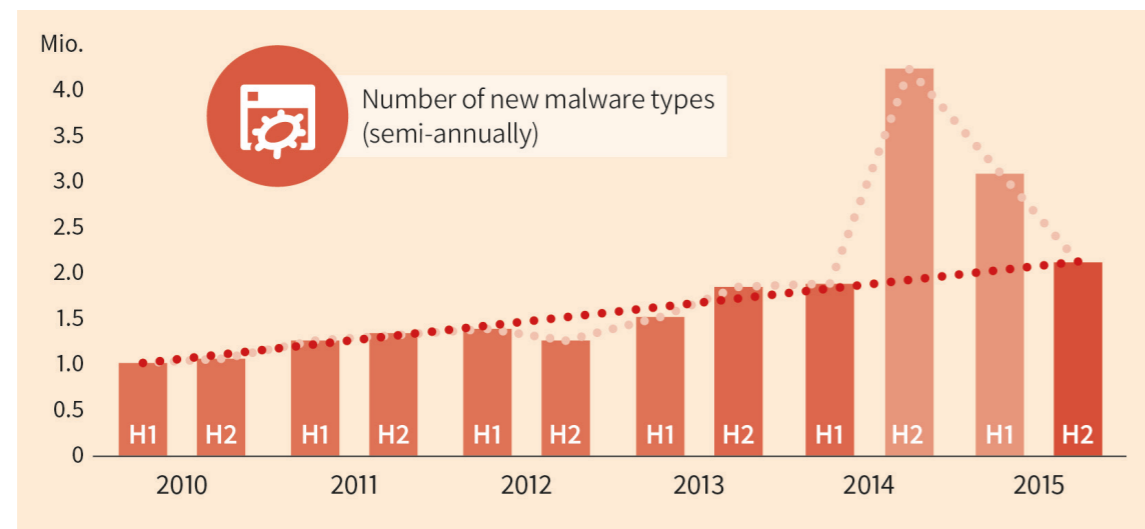
In the second half of 2015, we recorded another drop in the number of new signature variants: 2,098,062 compared to 3,045,722 in H1 2015, which is a decrease of 31%. Even more significant is the drop in the current numbers compared to the second half of 2014 – a decrease of 49.5%! However, this drop neither means an all-clear in terms of the risk to computer users, nor suggests that [conventional virus scanners](#)<sup>1</sup> will soon have served their purpose.

When all of the half-yearly figures for the past five years are considered, some obvious anomalies have risen to the top in the past year and a half, such as those described above that are responsible for the current strong downwards trend in the figures. But when the half-yearly figures are considered without the two big deviations of the second half of 2014 and the first half of 2015, a more consistent picture appears. In this regard, the increase in the figures appears almost linear (see below). It is clear that the number of signature variants is not undergoing a major downwards trend, as might be presumed from the aforementioned anomalies.

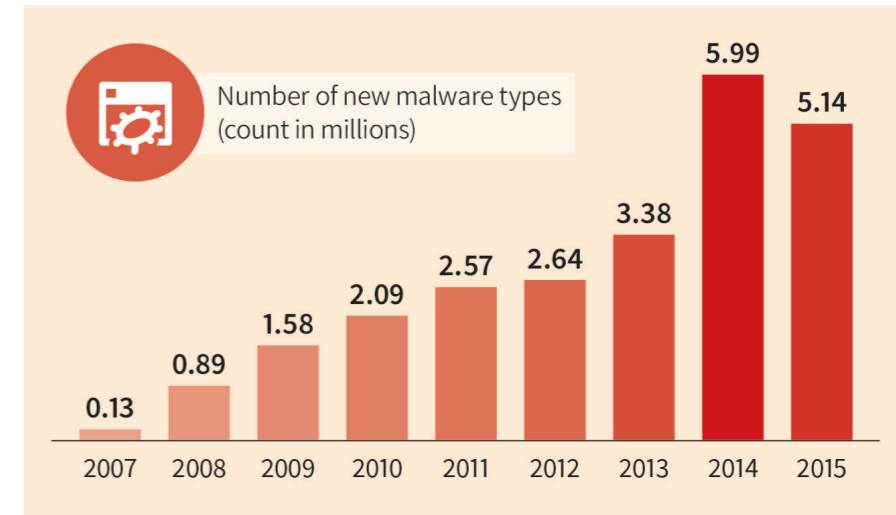
On the contrary, it leads to the supposition that the volume of new signature variants has now levelled at a level that is in line with expectations. This opinion is based on a consideration of the figures for the year overall:



At 5,143,784, the total number for 2015 is only slightly below the figure for 2014 – a drop of 14.3% – but still an undeniably high level for the potential for damage. In addition, it should not be ignored that a single signature variant might either be responsible for the detection of just one file, or indeed might relate to the detection of thousands of malware files.



<sup>1</sup> German only: <https://www.gdata.de/securitylabs/was-ist-eigentlich/virens scanner>



The actual number of malware files is therefore larger than the number of signature variants. Viruses, worms and Trojan horses continue to pose a risk for computer users.

One continually hears claims that “[virus scanners are dead](#)”<sup>2</sup> and declared obsolete. But with such statements, the term “virus scanner” is taken to be the security solution as a whole, which hasn’t been the case for a long time. The creation of signatures for the signature engines continues to be a very important component for the functioning of a comprehensive security solution, but they are just one element of it. These days, no leading antivirus product comes without proactive technologies and Cloud-based protection.

And precisely this ongoing development of proactive technologies might be a critical reason why the number of new signature variants appears to have fallen so sharply. The ongoing development of Cloud protection is leading to the ability to

intercept threats earlier – before they reach the computer.

Fast response times to new attack scenarios are another major advantage compared to conventional signatures. By evaluating just a few incidents, from the Malware Information Initiative for example, instant protection can be provided for the entire G DATA community. And the knowledge acquired can then be used in numerous other protection technologies in the products.

<sup>2</sup> <https://blog.gdatasoftware.com/2014/05/23959-the-evolution-of-anti-virus-solutions-continues>



## Risk monitor



The risk monitor shows the Top 10 averted attacks against computer users involving G DATA security solutions and activated feedback<sup>3</sup>. The most frequently averted attacks in the second half of 2015 are shown below. An up-to-date list for individual months [can always be found on the G DATA SecurityLabs website](https://www.gdatasoftware.com/securitylabs/statistics)<sup>4</sup>.

1. Script.Adware.DealPly.G	22.9%
2. Script.Application.Plush.D	4.6%
3. Win32.Application.OpenCandy.G	2.3%
4. Adware.BrowseFox.BU	2.3%
5. Win32.Application.OpenCandy.O	1.8%
6. Adware.Agent.PJT	1.7%
7. Win32.Adware.IObit.A	1.4%
8. Script.Adware.VBates.A	0.9%
9. Gen:Adware.BrowseFox.1	0.9%
10. Script.Spyware.Skrum.A	0.8%



MII  
Threat Monitor  
H2 2015

The Top 10 in the past half-year make up 39.6% of all reports. This continues the trend from H1 2015 – the variance in reported malware has increased again. Another continuation from the previous months can be seen in reports on Script.Adware.Dealply.G. Once again G DATA customers with MII feedback functions enabled have been exposed to this potentially unwanted program (PUP) most frequently.

This signature's share rose again by 6.7%. Let's look at the background to Script.Adware.Dealply.G.

The counting method in this section varies from the one used for the total number of new signature variants (see page 4). In this section, the number of actual attacks is considered, not the number of new malware types. A single malware type can have a huge effect on the number of attacks, even if the family only happens to have introduced a few (new) variants.

DealPly is a browser add-on that is intended to help users receive comparison offers for the product they are currently looking at when shopping via the browser.

Israeli developer company DealPly Technologies Ltd explains that the add-on “only shows deals or shopping offers that are relevant to the webpage you are browsing at the time. For such pages, DealPly sends just enough non-identifying data to the server to identify the product type you are interested in.”<sup>5</sup> The self-appointed purchase assistance service earns something out of this of course.



At the latest, when the customer clicks on the offer shown by the add-on. In the company's own words, this means that: “when you make a purchase via DealPly, some retailers pay us a small commission.”<sup>6</sup> Basically, of course, every shopper will be pleased at being able to get hold of a product at a lower cost.

But unfortunately, in a large number of cases, such add-ons are not integrated into the browser by the user voluntarily. Rather, they “piggyback” onto installation files (installers) for other programs. One scenario is that a user downloads software from the Internet, yet does so not by selecting the original file on the provider's site but by using a download portal belonging to a third-party provider. Third-party providers frequently bundle the actual software with these piggyback programs as they themselves can make a profit with each installation. When these are launched, inexperienced users are frequently distracted from the addition of the potentially unwanted program.

There are also cases where information on the installation of the add-on software is even actively withheld. This behaviour, which violates ethical principles in the majority of cases, is unfortunately a common practice on the web.

The dangers and irritations with PUPs and the other software described are many and varied:

- The user's data is sent to the developer's server or to an intermediary company without their consent. Without research, a user will not know what data is involved and where it will end up.

DealPly Technologies provides more information about this on its website

- To decide which websites are relevant for the add-on (see above), all of the sites visited be checked. In doing so a “movement profile” for the user could be generated by the operating company. If the add-on is being used in a corporate context, internal URLs and addresses might also be disclosed in this way.
- PUPs are very noticeable to the user inside the browser, but they do not always make do with merely embedding themselves here. When browser add-ons are removed, this is frequently overlooked, and installation routines that are called up repeatedly enable the pests in many cases. This is why search queries such as „How can I remove Dealply?” or “What is Adware.Dealply?” are not uncommon. The [free G DATA CLEAN UP](https://www.gdatasoftware.com/securitylabs/news/article/g-data-clean-up-takes-the-fight-to-obnoxious-toolbars-adsware-1)<sup>7</sup> helps get rid of stubborn adware, toolbars and plugs-ins.

<sup>3</sup> 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.

<sup>4</sup> <https://www.gdatasoftware.com/securitylabs/statistics>

<sup>5</sup> <http://www.dealply.com/faq.html>

<sup>6</sup> <http://www.dealply.com/eula.html>

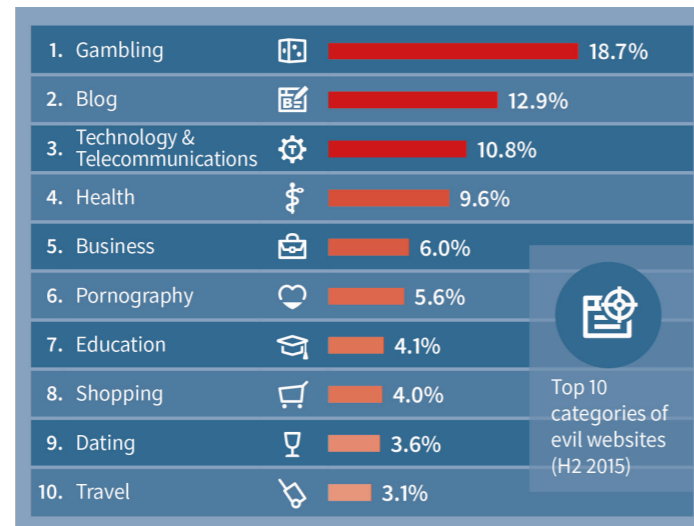
<sup>7</sup> <https://www.gdatasoftware.com/securitylabs/news/article/g-data-clean-up-takes-the-fight-to-obnoxious-toolbars-adsware-1>



## Categories of evil websites



For the second time since the first half of 2014, the Gambling category is at the top of this ranking. In the first half of 2015, it was still in 13th place and so is clearly one of the items worth mentioning regarding evil websites in the past six months.



Online gambling and betting have joined together to form a single market that recorded more than US\$ 40 billion in revenues in 2015<sup>8</sup> – more than three times the amount in the past 10 years. This industry will soon be celebrating 20 years of existence.

It is not unusual for attackers to manipulate the web space of smaller providers and less popular sites and set up their malware and phishing sites there. When security solutions detect such a manipulation, a new evil site is recorded in the appropriate category. In the second half of the year, for example, there was a major campaign in which multiple casino websites had an IFrame embedded which lead to malware domains. This exposed visitors to an exploit kit attack without them noticing ([see page 16](#)).

One might think that the number of visitors to these online casino websites was not that large, but many of the victims did not end up on the gambling site of their own free will. They were involuntarily delivered there via an infected advertising banner (malvertising). And the reach of web banners is sometimes extremely wide.

In the case described above, the fateful advertising banners were displayed on websites along with copies of copyright-protected materials. Even entirely legitimate sites and, especially, blogs often finance themselves by displaying advertising – they want/need to recoup the costs for domains, servers and editing work, especially if what the website is offering is free in itself.

But when doing so, the majority of providers do not select the advertisements being displayed themselves. Instead, they offer marketing space on their website in advertising networks and so leave this to third parties. The advertising networks deliver billions of advertising banners every day, and many smaller networks cannot carry out the checks and security precautions that the bigger providers do. But even with the latter, things can go wrong – as reported in April in the [G DATA SecurityBlog](#)<sup>9</sup>. In 2015 Yahoo!, YouTube and the eBay site in Britain were among the well-known victims of malvertising. As such, they became unwilling distributors of malicious advertisements.

Let's go back to the categories of evil websites and look at 2nd place – blogs. This popular type of publication platform is operated by millions of users – both professionally and privately. 56 million new posts are generated every month on Wordpress blogs alone.<sup>10</sup> Unfortunately the open nature of many blog systems offers more than just advantages. Many users can provide plug-ins and improvements for the system, even though these frequently also contain vulnerabilities. Basic products such as the Wordpress basic platform now have a high degree of security and code quality. Usually, it is the plug-ins and other enhancements that are the real issue here.

By implication, the popularity of the major providers means that a vulnerability can exist in a vast number of systems at the same time. This is a welcome target for cyber criminals. They can look for blogs with vulnerabilities almost automatically, and then manipulate them to deliver malware or phishing attacks, redirect visitors to other sites, or to launch other evil actions.

### ATTACKS FROM THE INTERNET

Surfing the Internet represents one of the biggest dangers for computer users. There are numerous attack options for cyber criminals. Here are two of the most popular types of attack:

#### Phishing sites

Practically a 1:1 copy of a website with an associated login form, e.g. a website for a bank, an email provider or a payment service provider. However, the login data entered is not sent to the actual company/service when logging in, but to the attackers' server. Data misuse and identity theft are among the potential pre-programmed problems.

#### Drive-by infections

As the name suggests, this type of attack happens in passing and generally without the user realising. Manipulated websites first scour the computer's configuration for attackable applications (browser, operating system, software etc.). If a suitable hole is found, an applicable exploit that can misuse the vulnerability is sent to the client. This often enables more malware to be downloaded onto the stricken computer and run, for example FakeAV, backdoors, espionage Trojans, ransomware etc.



#DidYouKnow  
Attacks are lurking everywhere, from gambling (22.9%)  
to travel websites (3.1%)

<https://secure.gd/dl-en-pcmwr201502>  
via @GDataSoftwareAG



<sup>8</sup> <https://www.statista.com>

<sup>9</sup> <https://blog.gdatasoftware.com/2015/04/24277-staying-alert-when-buying-banners-google-s-advertising-service-misused-for-distributing-malware>

<sup>10</sup> <https://wordpress.com/activity/>

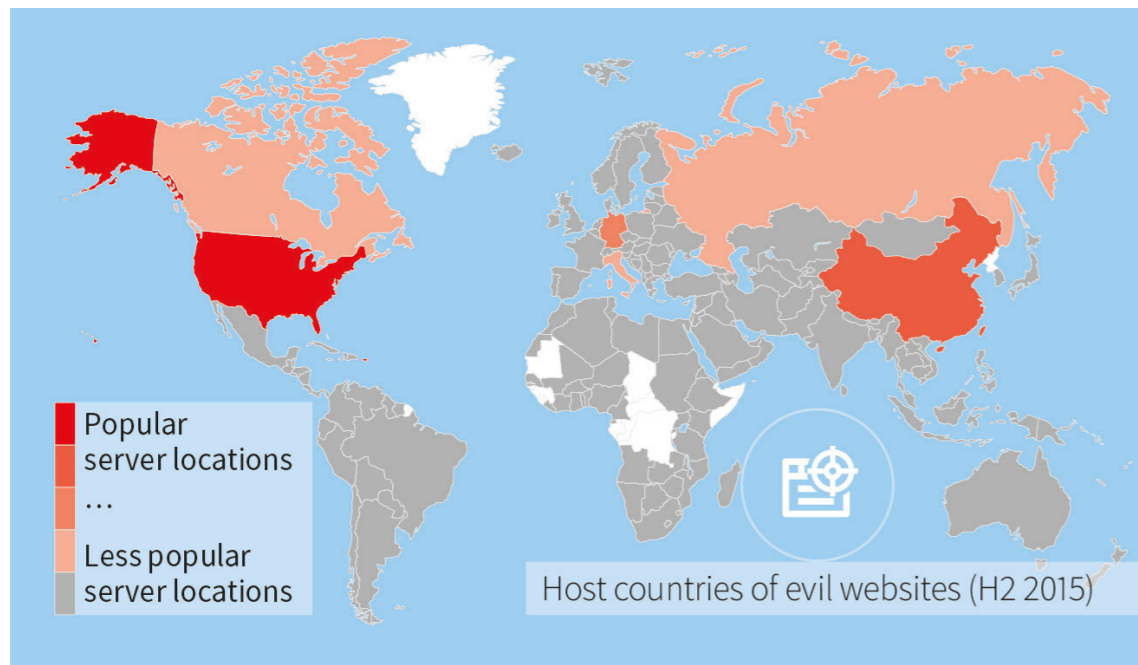


## Categorisation by server location



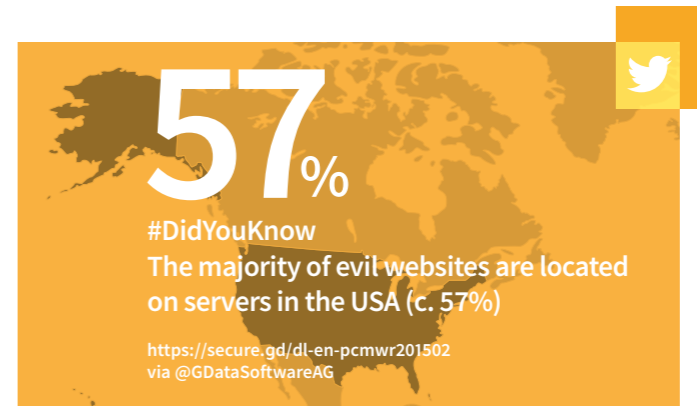
G DATA SecurityLabs not only categorise evil websites by subject, but also by where they are located in the world.

The following evaluation shows whereabouts in the world the majority of evil websites are based that have been reported to G DATA SecurityLabs as being malicious or phishing sites in the second half of the year.



The graphic above shows in which country an attack originates, i.e. where the website server is located. No distinction is made between phishing and malware sites. The top level domain (e.g. .com, .de etc) of the website is of no importance for this evaluation, only which country the computer holding the webspace is located in.

So, for example, it might occur that an evil website ends in .de, but the website's content is held on a server in the USA. In this case the statistics would register an incident in the USA.

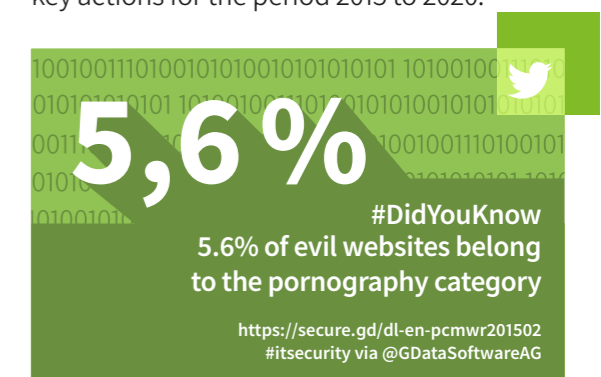


Overall, the number of websites categorised as evil has risen by 45%, which clearly emphasises how attacks from the web represent one of the biggest and growing threats facing computer users. In fact some 57% of registered attacks were carried out via resources hosted in the USA – a clear majority. Furthermore this is another increase compared to the previous half year, in which 43.3% of evil websites were registered in the United States.

China, Hong Kong, Russia and Canada (jointly 14.4%) are among the top placed host countries as well. Europe was relatively little in evidence in H2 2015 – only Germany and Italy appear in the top seven, being jointly responsible for a 6% share.

This leads to the supposition that cyber criminals prefer to use the largely first-rate communication network, but that is done more within the EU to counter criminal acts on the net than in other countries.

This estimation is supported by the agenda recently published by the European Commission with the goal to “fight against terrorism, organised crime and cybercrime”<sup>11</sup>. The EU Member States accordingly intend to collaborate with greater intensity and organisation to act against the stated crimes. “The priority is to identify ways to overcome obstacles to criminal investigations online, notably on issues of competent jurisdiction and rules on access to Internet-based evidence and information,” states one of the key actions for the period 2015 to 2020.



<sup>11</sup> [http://europa.eu/rapid/press-release\\_IP-15-4865\\_en.htm](http://europa.eu/rapid/press-release_IP-15-4865_en.htm)



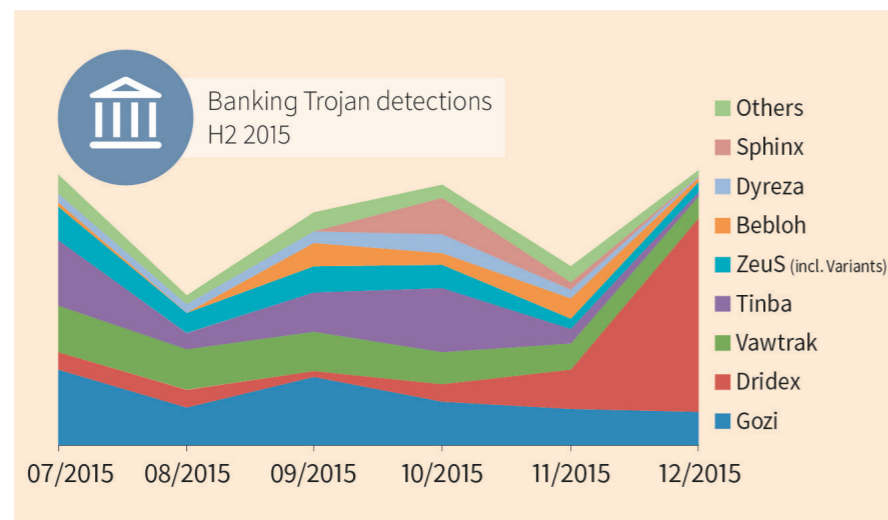
## Banking

### Banking Trojan trends



At the start of the second half of 2015, it initially looked as if attacks by banking Trojans would decrease significantly. The previously dominant Swatbanker, part of the Cridex group, which in March 2015 was

still responsible for the highest number of averted attacks since records began, almost completely disappeared from the picture for unknown reasons.



The malware registered up to this point was spread out at a relatively low level, as the graphic above shows. In July, 25% fewer attacks were recorded than in the previous month, and this figure halved again in August.

However, as the second half of the year unfolded, there was a resurgence in the level of attacks. A new crimeware called Sphinx contributed to this.<sup>12</sup> This is a new variant of the long-known banking Trojan ZeuS, where all of the network traffic is handled via the anonymisation network Tor.

However, this idea is not new; a malware variant that operates in a similar way was identified [by G DATA back in 2012](#)<sup>13</sup>. Ultimately, Sphinx turned out to be a short-lived footnote.

At the beginning of the half-year, no Trojan held a dominant position. However, in October the level of infection reached that of July again.



In November, a major Russian cyber crime ring was broken up.<sup>14</sup> An interesting aside with this is that a film production company that was apparently working on a film about cyber crime was being used as a cover-up for the criminal organisation. A connection with the Dyreza Trojan is suspected, the activities of which were virtually eliminated after the group was taken down. In addition, Tinba and also ZeuS, together with all its variants, were subsequently recorded much more rarely, with the result that the level of attack for November was only slightly above that of August again.

In December, the already well-known banking Trojan Dridex built up a significant lead, distributing itself via [mass emails containing supposed invoices](#)<sup>15</sup>. Overall the level of infection ended up back at that for July.

It is hard to predict the continued development of the existing players. For example, it is questionable whether the attackers behind Swatbanker will return with their previous intensity in the foreseeable future. The attackers behind Dridex are distributing their malware as the Swatbanker attackers did previously,

primarily via spam email. However, the attacks here appear to be occurring more constantly and not intermittently, as with Swatbanker. We expect Dridex to continue to have a significant proportion of the detections in the coming months. Gozi was equally constant, so further attacks can be expected from this as well.

The decreasing volume of attacks might ultimately hint at a paradigm shift on the part of the attackers. While the attacks in recent years have primarily targeted the masses, the focus here might be moving more towards smaller yet particularly lucrative targets – especially corporate accounts.

**Dridex**

#DidYouKnow  
Banking Trojan Dridex: one of the most prominent finance malware strains in H2/2015

<https://secure.gd/dl-en-pcmwr201502>  
via @GDataSoftwareAG

<sup>12</sup> <http://securityaffairs.co/wordpress/39592/cyber-crime/sphinx-variant-zeus-trojan.html>

<sup>13</sup> <https://blog.gdatasoftware.com/2012/09/24033-botnet-command-server-hidden-in-tor>

<sup>14</sup> <http://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS>

<sup>15</sup> <https://blog.gdatasoftware.com/2015/12/24315-dridex-the-comeback-king>



## Targets of banking Trojans

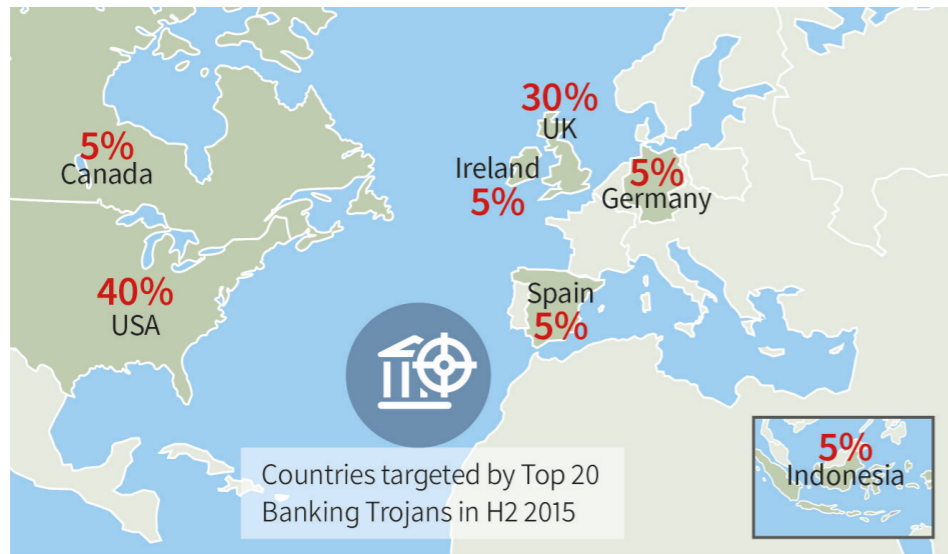
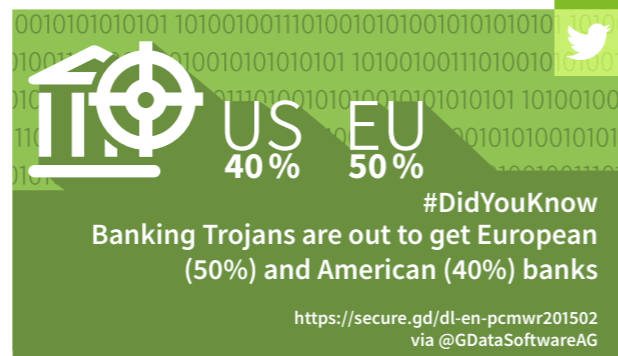


Every banking Trojan attacks specific targets depending on its configuration. Target in this case means that the banking Trojan carries out its attacks when the user of an infected PC visits a specific website. The malware then deploys activity adapted to that target.

As already seen in earlier reports, here again the cyber criminals' preference is for the English-speaking countries. 80% of all target sites identified came from these countries.

With the exception of payment service PayPal, only banks appeared in the list of most common targets. 1st place in the rankings goes to the Santander group, a

bank originating from outside of the English-speaking region, where attacks on this target involve both the bank's Spanish and English portals. In previous investigations, Santander appeared somewhat lower in the rankings.



## Methodology



In total, 4,422 configuration files of the Vawtrak, Tinba, ZeuS (incl. variants such as Citadel), Bebloh and SpyEye families were decrypted and analysed. In the process, Bebloh was added and Swatbanker removed, as it was no longer appearing (see page 12). In the configuration files for these banking Trojans was a list of target sites (i.e. websites for banks, payment service providers, etc). If these sites are accessed by an infected computer, malware specifically prepared for the site (called webinjects) comes into play.<sup>16</sup>

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 level of distribution of the respective Trojan family is taken into account. Because Swatbanker is no longer a particularly dominant Trojan, calculation of the list with an assumed uniform distribution of Trojans was not carried out. In addition, countries of origin were also allocated to the Top 20.<sup>17</sup>

	Country	Rating	Attack Probability
		Brand value via Brand Finance	Based on the analysis of 4,422 samples from the families Vawtrak, Tinba, ZeuS (incl. variants, i.e. Citadel), Bebloh and SpyEye
<b>Santander Group</b> gruposantander.es, santander.co.uk		10	45.00%
<b>Lloyds Banking Group</b> lloydstsb.co.uk, halifax-online.co.uk, ...		35	35.86%
<b>RBS Group</b> rbs.com, natwest.com, ulsterbank.co.uk, ...		60	35.81%
<b>Barclays</b> barclays.co.uk		13	34.99%
<b>Allied Irish Banks</b> aib.ie		181	25.75%
<b>HSBC</b> hsbc.com, hsbc.co.uk, ...		3	25.48%
<b>The Co-operative bank</b> co-operativebank.co.uk		114	25.32%
<b>PayPal</b> paypal.com, paypal.co, paypal.com.mx, ...		-	25.03%
<b>Nationwide</b> nationwide.co.ukcom.sg		94	22.64%
<b>Bank Central Asia</b> klikbca.com		147	19.00%
<b>BBVA</b> bbvanetoffice.com, bbva.es, ...		28	17.79%
<b>Bank of America</b> bankofamerica.com		6	17.57%
<b>Wells Fargo</b> wellsfargo.com		1	17.25%
<b>Chase</b> chase.com, chasecanada.ca, chaseonline.com		7	17.01%
<b>Citi</b> citibank.com, citibank.com.au, citibank.com.sg		5	16.87%
<b>U.S. Bancorp</b> usbank.com		46	16.56%
<b>Citizens Bank</b> citizensbankonline.com		264	16.51%
<b>Fifth Third Bank</b> 53.com		111	16.37%
<b>TD Bank</b> td.com, tdcnadatrust.com		18	15.80%
<b>DKB Bank</b> dkb.de		176	14.64%



TOP 20 Targets of Banking Trojans in H2 2015 (according to Trojan Distribution)

Category: ■ = Bank ■ = E-Payment ■ = Auction

<sup>16</sup> Webinjects involving so-called wild cards or common expressions were mapped onto other webinjects without wild cards where possible. When such webinjects 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.

<sup>17</sup> 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%200%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.





## Exploit Kits



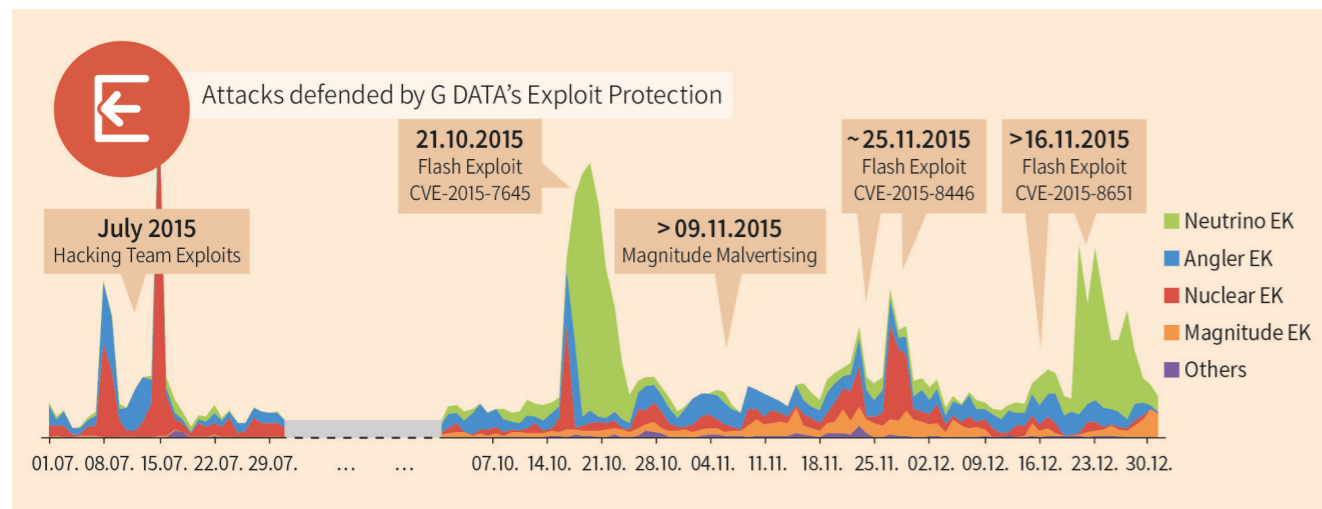
Exploit kits are tools traded in underground markets for automated searches for and exploitation of vulnerabilities. G DATA's PC security solutions contain a component called Exploit Protection that specifically aims to pro-actively fend off exploits. Attacks averted in this way have been mapped to known exploit kits in this study.

The exploit kits Neutrino, Angler, Nuclear and Magnitude were particularly prominent in the second half of 2015. The majority of averted attacks could once again be put down to Angler. However, in looking at this, there was no clear dominance, as in the

previous half-year; Neutrino was practically at the same level.

Furthermore, attacks by Huanjuan, Niteris, RIG and Fiesta were identified, but these largely remain as footnotes. As in the previous half-year, Adobe Flash was the criminals' preferred attack vector.

An initial major wave can ultimately be traced back to an attack on Hacking Team.<sup>18</sup> This is a company that more or less legitimately produces and sells attack tools – to government organisations, for example.



<sup>18</sup> [https://en.wikipedia.org/wiki/Hacking\\_Team#2015\\_data\\_breach](https://en.wikipedia.org/wiki/Hacking_Team#2015_data_breach)



Ironically, practically all of Hacking Team's data was stolen by hackers in the attack and made accessible to the general public on July 5th. Besides interesting information on their customer base, which included pariah states, Hacking Team's attack tools were also published in full. These included exploits for several previously unknown Flash vulnerabilities, called zero-days. The term "zero-day" is used almost comically here as Hacking Team has actually had the exploits since October 2013.

The publication of this data was of course noticed by cyber criminals too. They integrated the attack methods into their exploit kits within a very short time – by July 7th. The number of averted attacks shot upwards after this. G DATA's Exploit Protection provided protection against all these attacks, including Hacking Team's. The attacks lasted until July 10th, when Adobe provided a patch.

Thereafter the situation remained relatively quiet for several months, until, on October 13th, a new Flash exploit (CVE-2015-7645 / APSA15-05)<sup>19</sup> belonging to an exploit kit from a group called APT28, alias Sofacy, was made public.

This is a group presumably associated with the Russian government that is also thought to have been responsible for the attacks on the German Federal Government.<sup>20</sup>

Once again, the cyber criminals adapted the attack within a short time – three days – subsequent to which corresponding averted attacks were identified in G DATA Exploit Protection. Adobe managed to provide an update to remove the vulnerability at practically the same time as the cyber criminals' attacks began. It presumably helped that the vulnerability had already been discovered by a security researcher two weeks beforehand and reported to Adobe.<sup>21</sup>

Nevertheless, as it took a certain amount of time for updates to actually be distributed to users, a similar number of attacks was ultimately recorded as with the exploits integrated into the attack tools following the attacks on Hacking Team.

<sup>19</sup> <https://helpx.adobe.com/security/products/flash-player/apsa15-05.html>  
<http://malware.dontneedcoffee.com/2015/10/cve-2015-7645.html>

<sup>20</sup> [https://en.wikipedia.org/wiki/Sofacy\\_Group](https://en.wikipedia.org/wiki/Sofacy_Group)

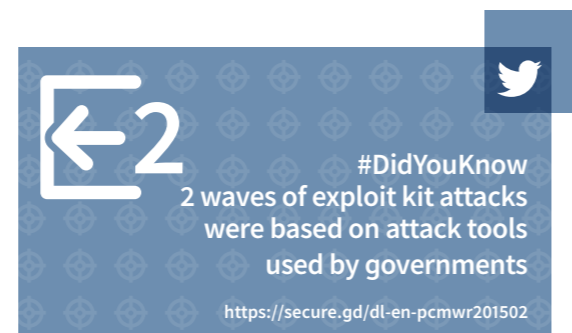
<sup>21</sup> <https://twitter.com/natashenka/status/655083143456665600>



The individuals behind the Magnitude exploit kit came onto the scene relatively late and began an attack using CVE-2015-7645, which was backed up with malvertising, on November 9th.<sup>22</sup> In this case the exploit kit was embedded via advertising banners into websites that are in no way malicious and that appear unsuspecting to users. However, as the exploit kit used at the start of November was no longer entirely new, the intensity of attacks was not so great as with the initial wave of the other exploit kits. However, compared to the Magnitude attacks of the previous months, we still recorded a significant increase.

During the course of the half-year, Flash was a focus for the attackers on two occasions: firstly from November 13th (CVE-2015-8446 / APSB15-32).<sup>23</sup> Unlike the previous waves of attack, this one began just a few days after the release of a security update by Adobe and turned out to be correspondingly less effective. Another wave of attacks started on December 21st and targeted the vulnerability described in CVE-2015-8651 / APSB16-01.<sup>24</sup> This was specifically exploited by the Neutrino exploit kit until Adobe published a security update on December 28th. As the vulnerability was open for a full week, significantly more attacks were recorded for this.

As before, Flash remains the most significant attack vector for exploit kits. Besides Angler, Neutrino in particular has played a major role this year, as has Nuclear to a lesser extent. The speed of adaptation of the attackers was particularly noticeable with Angler and Neutrino. Bigger waves of attack than before were registered for Magnitude, especially in the context of malvertising. However, the volume of recorded attacks did not reach the scale of the other exploit kits.



It was conspicuous in this half-year that two major waves of attack (evidently in the Hacking Team case, presumably in the case of APT28) can be traced back to attack tools used at the government level that have been adapted by cyber criminals.

The risk of such attack tools falling into the hands of cyber criminals has long been discussed by security researchers. The existence of this risk has now been confirmed.



<sup>22</sup> <https://blog.malwarebytes.org/exploits-2/2015/11/magnitude-exploit-kit-activity-increases-via-malvertising-attacks/>

<sup>23</sup> <https://helpx.adobe.com/security/products/flash-player/apsb15-32.html>

<sup>24</sup> <https://helpx.adobe.com/security/products/flash-player/apsb16-01.html>



### About G DATA

G DATA Software AG is the antivirus pioneer. Founded in 1985, the company, which is based in Bochum, developed the first software to combat computer viruses more than 30 years ago. Today G DATA is one of the leading providers of Internet security solutions and virus protection, with over 400 employees worldwide.



SIMPLY  
SECURE