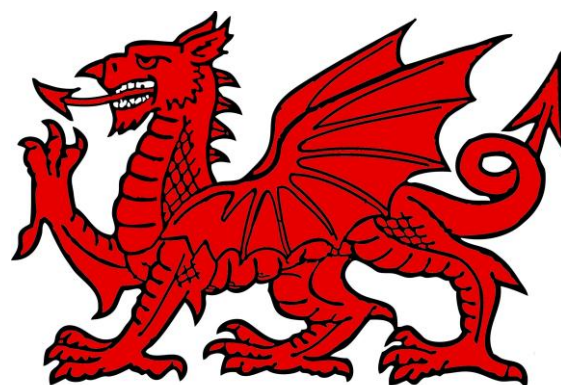


MALWARE INFECTIONS MARKET



TEAM CYMRU
WWW.TEAM-CYMRU.ORG

Browsing webpages on the Internet isn't without risks. Even when you are only visiting 'trustworthy' sites. They could be compromised and contain 'evil code'. The Underground economy (UE) is the facilitator for this threat. There are dedicated marketplaces selling exploit kits. These kits are able to abuse vulnerabilities in browsers and applications, with the goal of infecting as many users as possible. This paper looks at the market place for exploit kits and what kind of interaction it has within the UE.

Internet users are reminded to regularly update their operating system and some applications via alert messages. Whether it is the Mac OS X, Windows or Linux operating system, these systems offer an easy interface for the update process. Some users would have decided to automatically install new updates and they might not be reminded of it anymore. In that case new updates for the operating system will be downloaded once they come available and installed. What happens however if a third-party application like winzip, Flash or the PDF reader contains vulnerabilities? In some cases the application itself might have asked the user to update to a newer version. Not everyone might realize that the programs on their system, whether it is a desktop computer or phone, pose an equal security risk as the operating itself. Just recently Apple found a vulnerability on their IOS platform where the PDF implementation could cause the iPhone or iPad to become compromised.

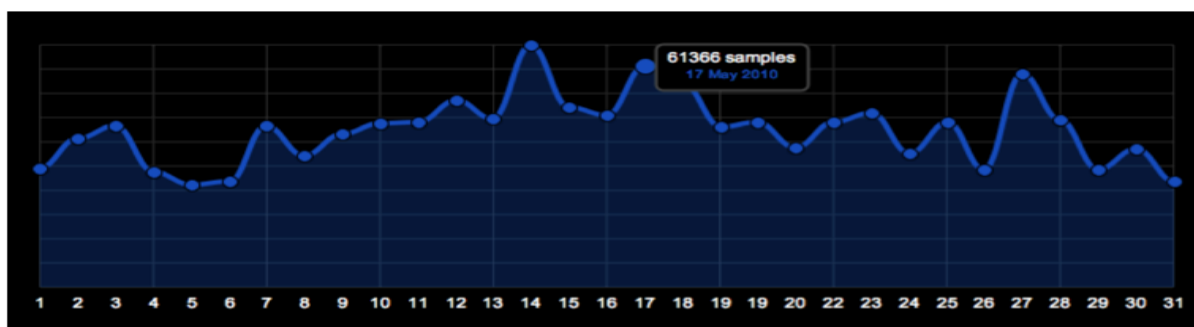
The Underground Economy has taken advantage of this knowledge. It works like any other marketplace; the demand for new exploit methods has created a profitable trade. Exploit kits are for sale with the latest methods of infecting as many users as possible. Team Cymru analyses thousands of malware samples each day and recent trends have shown, not surprisingly, that PDF documents are very popular in application-based exploit methods. PDF exploits have been around for quite some time. Recent media coverage on this subject has linked PDF exploits to several high profile attacks. Our analysis has showed that other popular applications targeted are Flash and Java. These application exploits seem to be very prevalent as there is a high chance of end-users having these applications installed on their system. PDF documents in particular seem to lend themselves very well for targeted attacks. With more and more Internet users aware of the risk of opening executables in email attachments, there is a higher chance that the targeted user will open a PDF file that has been emailed to them in comparison to an exe file.



Browser Independent

Another advantage is that PDF's and Flash content are both delivered to the user via browsers, while they can also take the browser out of the equation in the sense that the vulnerability doesn't have to be in the browser itself. The PDF exploit will target the PDF reader, not the browser. An example of a malware family taking advantage of this is the Gumblar virus. It tries to exploit the user via both PDF and Flash vulnerabilities via so-called drive-by-downloads. Once successful, the exploit will force the system to install or download additional executables onto the machine.

To get users to visit the exploit site, Gumblar uses redirections to point the victims to the actual drive-by-download location. Interestingly, in this process, many legitimate servers are involved. One of the threats, once infected with Gumblar, is to have your FTP credentials stolen. If those FTP account details happen to be linked to public websites, Gumblar can use these credentials to link that website in the infection process. In this case the infected machine becomes a contributor to the infection chain.




Graph showing the number of malware samples seen in a recent month

Gumblar isn't the only malware family that combines PDF and Flash exploits on one page to find victims. Another malware family using the same technique is **Gootkit**. This malware family targets PDF and Flash and also uses FTP credentials. The reason behind this similarity is that these exploits are available via exploit kits, also known as Browser Exploit Kits or Browser Exploit Packages (BEP) in the Underground economy.

The quality of these Kits varies, at least from the point of view of the criminal. Analysis showed that a lot of drive-by download sites don't infect all users. It can be that the particular exploit that is being used, only works on Windows XP service pack 2, or service pack 3. However that doesn't seem to be too big of an issue for the miscreant. If they are able to infect a legitimate website with their code, their conversion rate will yield enough results in the end. A sufficient percentage of Internet users will have the right system profile for their attack to succeed.



Wellcome, root Browsers Systems Country Referers



System	Visits	Percent	Loads	Efficiency	Total efficiency
Windows XP	1102	76.26 %	280	25.41 %	19.38 %
Windows Vista	179	12.39 %	6	3.35 %	0.42 %
Windows 2003	96	6.64 %	85	88.54 %	5.88 %
Unknown	35	2.42 %	0	0 %	0 %
*BSD Unknown	22	1.52 %	0	0 %	0 %
Windows 2000	6	0.42 %	2	33.33 %	0.14 %
Linux Unknown	4	0.28 %	0	0 %	0 %

Screenshot of an exploit kit administration page showing the number of 'installations based on Operating System..

Besides vulnerabilities in PDF or Flash, an exploit kit will allow the miscreant to try several different attack vectors. These are based, for example, on the installed applications or type and version of the browser of the visiting user. As this data is shared by default by almost all browsers, this allows the attacker to modify the attack based on each user and try a custom made attack without alerting the user.

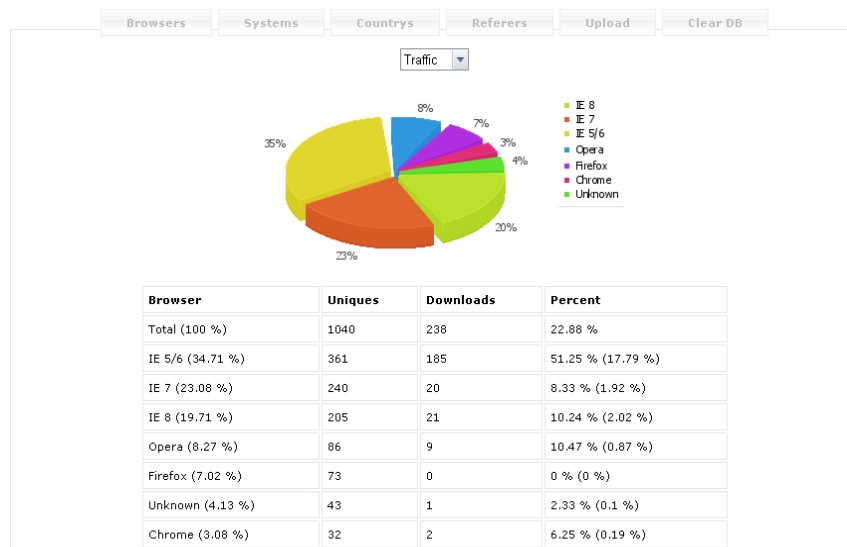
Depending on the type of exploit kit that is being used, multiple applications can be targeted. These include Java, Yahoo Messenger, Winzip, Realplayer, Apple Quicktime and **many others**. Some exploit pages also contain smart tricks, where the users will be shown a 404 page while the exploit is being loaded. In other cases, the miscreant has setup a suspended page on the main page in what seems to be an effort to attract fewer complaints. IP geographical lookup also allows the attacker to target specific countries, based on the country of 'residence' of the visiting IP.



Browsers Systems Countryys Referers Clear DB

Country	Uniques	Downloads	Percent
Total (100 %)	2589	618	23.87 %
Germany (63.58 %)	1646	381	23.15 % (14.72 %)
United States (18.23 %)	472	94	19.92 % (3.63 %)
Unknown (18.04 %)	467	142	30.41 % (5.48 %)
United Kingdom (0.08 %)	2	1	50 % (0.04 %)
Luxembourg (0.08 %)	2	0	0 % (0 %)

Screenshot of the Liberty exploit kit administration page showing the number of 'installations based on Country of origin.



Screenshot of an exploit kit administration page showing the number of installations based on Operating System..

Market

The economics around exploit kits shows that this is a growing market place. More exploit kits have recently become available and prices vary from hundreds to thousands of dollars. These are offered with conversion rate statistics and advertisements showing the install rates in different countries. Interested parties will have the ability to buy the pack by itself or buy additional services for having the webserver and pack setup for them.

Zombie Infection Kit связка эксплоитов

Zombie Infection Kit - инструмент для создания армии зомби (ботнет сетей) - это эффективно трафика в загрузки.

--=[Функциональность]=--

- Классическая административная панель управления;
- Загрузка до трех файлов одновременно через шеллкод;
- Очистка статистики двумя кликами мыши;
- Статистика: браузеры, системы, страны, рефералы, эксплоиты;
- Не вызывает крэша браузера;
- В составе связки присутствуют самые актуальные на сегодняшний день эксплоиты.

Скриншоты:

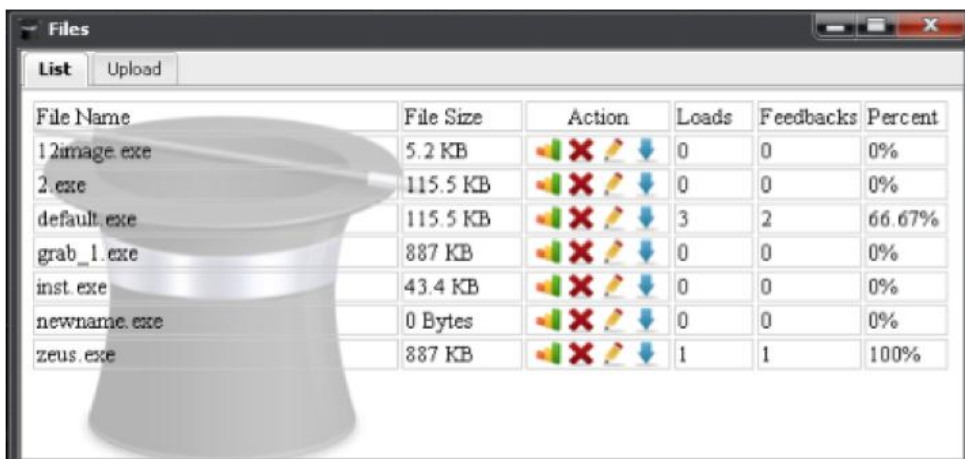
<http://img408.imageshack.us/img408/5605/54313703w.png>

<http://img267.imageshack.us/img267/9123/28435442.png>

<http://img716.imageshack.us/img716/3746/25009032.png>

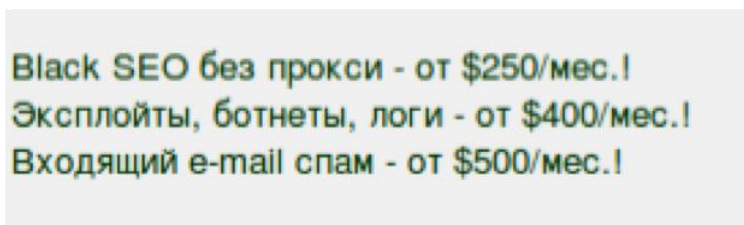
<http://img138.imageshack.us/img138/985/33472429.png>

A large number of exploit kits use **PHP and MySQL** on the server side and are easily installed on cheap web hosting servers. Most exploit kits will come with a graphical interface to allow the miscreant to view statistics of their installation attempts. The image below is a screenshot of the YES exploit kit, showing a demonstration of installation numbers for specific files. Not surprisingly one of the files listed is 'zeus.exe', the name of a well known banking trojan.



File Name	File Size	Action	Loads	Feedbacks	Percent
12image.exe	5.2 KB		0	0	0%
2.exe	115.5 KB		0	0	0%
default.exe	115.5 KB		3	2	66.67%
grab_1.exe	887 KB		0	0	0%
inst.exe	43.4 KB		0	0	0%
newname.exe	0 Bytes		0	0	0%
zeus.exe	887 KB		1	1	100%

Yes Exploit kit screenshot showing files optional to be installed.



Black SEO без прокси - от \$250/мес.!
Эксплойты, ботнеты, логи - от \$400/мес.!
Входящий e-mail спам - от \$500/мес.!

Russian Advertisement text showing prices on hosting malicious content.

So how do the miscreants get traffic to their site? If they don't know how to, the Underground economy forums provide a solid base for the novice in this area. Manuals in the UE list several options, including to hack existing websites and add iframe links. An iframe link added to a legitimate popular site via sql injection, can yield many installs. Other options include seeding via P2P files, Spam runs or with the purchase of stolen FTP credentials to automatically add an iframe by modifying webpages linked to those FTP accounts. The resulting traffic from the exploit pages will in the end result in infections.

Bulletproof-hosting

A continuous issue in the exploit kit landscape, is 'reliable' hosting for the actual infection sites as these sites have risk of being taken down quickly. If reliable hosting is a problem, there is likely someone to offer this service without any difficult questions being asked.

Some miscreant hosting providers will even advertise, with prices listing the monthly cost of hosting a botnet or exploit page on their server. These services however come at a high cost and appear to be far higher than average hosting prices.



cases they are selling the 'traffic' generated by their kits. A popular way of making money for the miscreants running the exploit kits is via Pay-Per-Install (PPI) programs. The miscreant signs up as an affiliate and retrieves the executable from the PPI sites and then distributes the .exe onto the compromised machines via his exploit kit interface. In a previous paper we have described the PPI process in more detail.

Conclusion

For the average Internet user, some simple healthy habits might help to prevent infection via drive-by download. Many exploits used in these kits have been around for quite a while, so updating applications will certainly help. At the same time, getting a system 100% secure is nearly impossible. For those who don't want to be at risk, browsers in sandboxed environments or virtual machines might be a good option. See our tips [pages](#) for more advice.

About Team Cymru:

Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. By researching the 'who' and 'why' of malicious Internet activity worldwide, Team Cymru helps organizations identify and eradicate problems in their networks.

More information on online security, visit our tips page :

<http://www.team-cymru.org/ReadingRoom/Tips/>

