How malware attacks the Windows platform, 2013

Exploit kits and drive-by consequences – June 2013

Document written and evaluated by:

CSIS eCrime Unit

Contact: ecrime@csis.dk

Publish date: June 7, 2013

Contents

1 Abstract

CSIS has over a period of approx. six months collected real-time data from various so-called exploit kits. An exploit kit is understood to be a commercial hacker toolbox that is actively exploited by IT-criminals in order to take advantage of vulnerabilities in popular software.

This study is an update of "How Windows get infected with malware" which was first published in September 2011 (http://www.csis.dk/en/csis/news/3321/)

2 About CSIS Security Group

In 2003, CSIS Security Group was founded with a mission to meet the growing threat of IT criminals. Today, CSIS has become the leading Nordic supplier of eCrime services, and cooperates with all the Danish banks, and a series of major European financial institutions.

The security experts of CSIS are among the best in the world, which is proven by them winning the DefCon 2011, the world's unofficial hacker championship. Thus, CSIS is the preferred IT security adviser by many companies, the state, and the media in Denmark.

The knowledge gained by continually following the IT-criminals' whereabouts is redeployed in the development of solutions that provide optimum protection to organizations as well as private individuals.

CSIS Security Group product strategy

- CSIS Security Group wants to offer the most extensive and cost effective IT security solutions in the Nordics. To reveal, document, and prevent security breaches for our customers. To support the IT security responsibly with gathering and analysis of information to prevent IT related crimes and harmful user behavior.

- CSIS Security Group's IT security solutions ensure that management as well as the technical staff has access to an updated overview of the current status, and documents governance and control of security exposures 24x7.

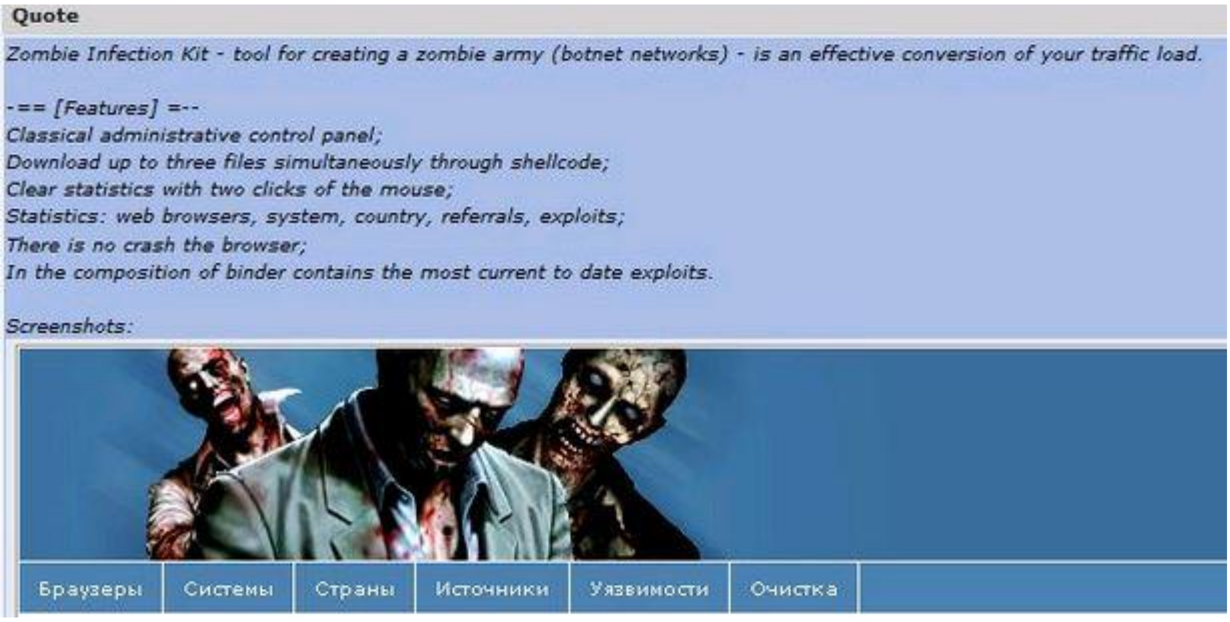
- CSIS Security Group's target is to be among the top 3 suppliers within standardized, stabile and modular IT security products, while providing economies of scale through a centralized solution with the possibility for strategic outsourcing.

3 The state of exploit kits

Approximately 84.3 % of all virus infections can be traced back to the drive-by attacks from malicious or compromised websites. This report also reflects the interesting fact that within the past six months several new exploit kits have emerged as part of the growing underground economy just as the people developing and selling these tools have become considerably more aggressive and visible in their marketing. It should also be noted that the time from the discovery of vulnerability and to it becomes publicly known and accepted into the commercial exploit kits has markedly decreased. Exploit kits are frequently supplied with complete SLA (Service Level Agreements) where the buyer is guaranteed new fresh exploits and updates during the license period.

Exploit kits used in these attacks can be bought by anyone. Even people without any technical skills what so ever can use these tools as they are usually very user friendly, well documented and come with support and regular updates. The kits can also be bought as part of a Crime-as-a-service which often includes a SLA. This resembles legitimate software and clearly illustrates how well organized the underground economy has become.

Pricing of these kits may vary from somewhere between just a few dollars to several hundred depending on the scope of use.



Quote

Zombie Infection Kit - tool for creating a zombie army (botnet networks) - is an effective conversion of your traffic load.

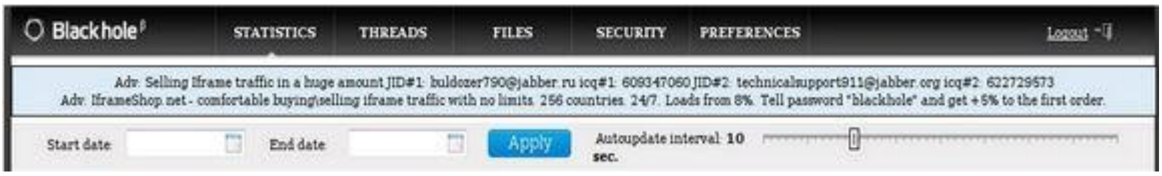
-== [Features] =--
Classical administrative control panel;
Download up to three files simultaneously through shellcode;
Clear statistics with two clicks of the mouse;
Statistics: web browsers, system, country, referrals, exploits;
There is no crash the browser;
In the composition of binder contains the most current to date exploits.

Screenshots:

Figure: Zombie exploit

3.1 Exploit kits in action

Data is collected from many different commercial exploit kits that have been abused by cybercriminals to infect Windows systems globally. The exploit kits in this study includes (but are not limited to) *Black Hole, CoolEK, Sweet Orange, RedKit, Sakura, Phoenix, Crime Pack,* *NeoSploit, Gong Da, Neutrino, Styx, Bleedinglife, Eleonore, Nuclear, Yang, Propack, RedBOT, Upas* and *CritXPack*. The majority of these are sold more or less publicly.



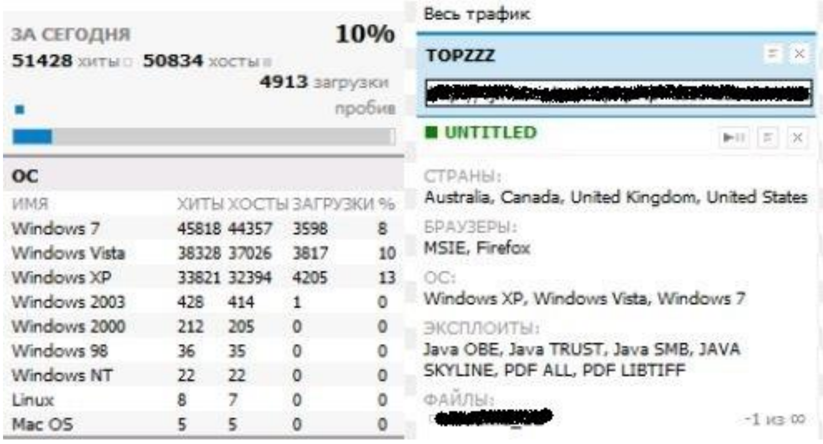
Adv: Selling Iframe traffic in a huge amount JID#1: buldozer790@jabber.ru icq#1: 609347060 JID#2: technicalsupport911@jabber.org icq#2: 622729573
Adv: IframeShop.net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

Start date: End date: Autoupdate interval: 10 sec.

Figure: The admin panel of the Blackhole Exploit Kit.

Some of the people distributing these kits even include their own banners (blackvertising) which certainly fuels the distribution of various dark market services such a "Pay Per Installs" (PPI) and Iframe trafficking. The pricing of such blackvertising, according to Blackhole's primary distributor, known as "Paunch", placing a banner in the kit costs $700 per month. The exact numbers of impressions are unknown; however there certainly are a lot of Blackhole users out there and the fact that all of these "users" are blackhats, it will hit a concentrated audience.

The exploit kits include a user friendly interface with a subset of parameters which can be tweaked by the attacker depending on the scope of the campaign. They even include full statistics of infected clients from where also the datasets in this study is derived.



ЗА СЕГОДНЯ
51428 хиты 50834 хосты
4913 загрузки
пробив

ОС

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Windows 7	45818	44357	3598	8
Windows Vista	38328	37026	3817	10
Windows XP	33821	32394	4205	13
Windows 2003	428	414	1	0
Windows 2000	212	205	0	0
Windows 98	36	35	0	0
Windows NT	22	22	0	0
Linux	8	7	0	0
Mac OS	5	5	0	0

Весь трафик
TOPZZZ
[redacted]
UNTITLED
СТРАНЫ:
Australia, Canada, United Kingdom, United States
БРАУЗЕРЫ:
MSIE, Firefox
ОС:
Windows XP, Windows Vista, Windows 7
ЭКСПЛОИТЫ:
Java OBE, Java TRUST, Java SMB, JAVA SKYLINE, PDF ALL, PDF LIBTIFF
ФАЙЛЫ:
[redacted]
-1 из ∞

So in line with the previous study from 2011, the statistics are based on data from the underlying statistical modules related to these exploit kits. This approach helps to ensure an as precise picture as possible of the threats and how Windows machines are infected since it is reflecting "real-time" and "in the wild" numbers.

3.2 Software targeted and exploited

The statistical material covers approx. 843,100 user exposures from which as much as 39.12 % have been infected with virus / malware due to missing security updates for Microsoft Windows operating system and 3rd party applications. When analyzing these data we quickly noted that especially three different third party products was the culprits of infection and they sum up to Adobe Flash, Adobe Reader/Acrobat and Java JRE. These 3rd party applications are installed on millions of PC around the globe.

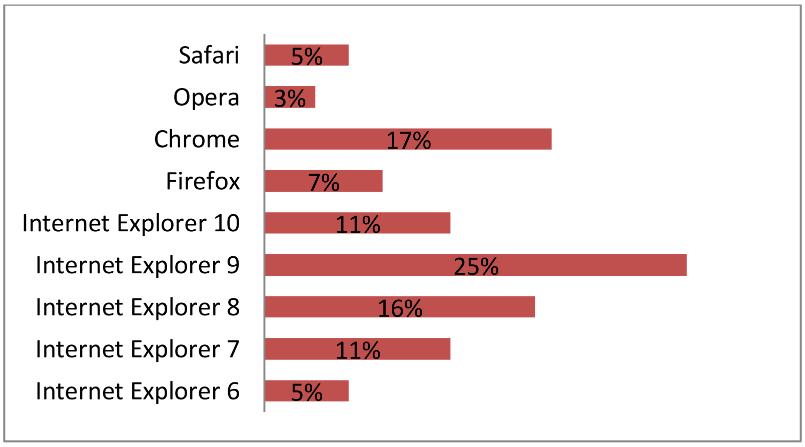
What is Adobe Flash?
Adobe Flash Player allows you to view and interact with SWF and FLV files (files that are read by Flash Player) created and published across the Internet using your browser or mobile device. Adobe Flash Player allows authors of SWF and FLV files and the websites hosting those files to use local shared objects (LSOs). LSOs can be used in a similar manner as cookies, and can be used for a variety of purposes such as keeping track of information you provided and remembering your preferences.

What is Adobe Reader/Acrobat?
Adobe Reader is the standard program for viewing PDF documents.

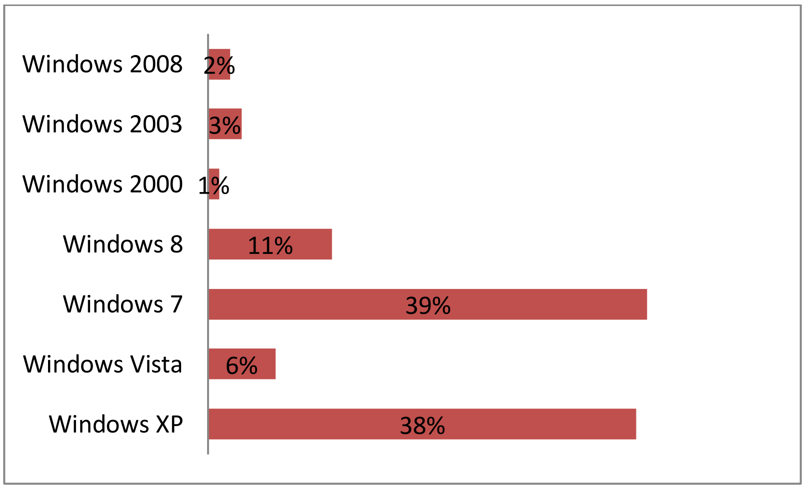
What is Java JRE?
Java is a programming language and computing platform first released by Sun Microsystems in 1995. There are lots of applications and websites that will not work unless you have Java installed – including the NemID application used to log on Danish Online Banking sites and many public and governmental sites.

4 Statistical overview

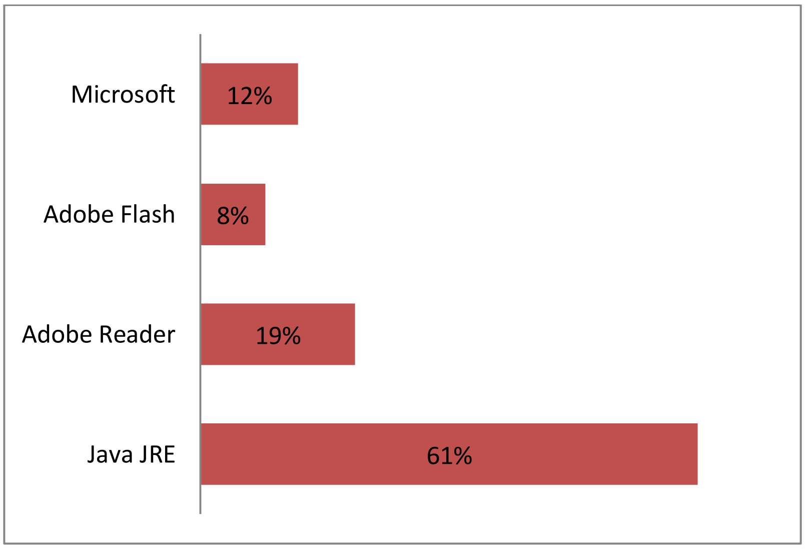
The thousands of users, who unknowingly have been exposed to these drive-by attacks, have used the following Internet browsers (figures are rounded up):



The distribution on various versions of MS Windows is as follows:



When this data is compared with which vulnerable software that was used to infect the system at hand, we see the distribution below:



Please note that "Microsoft" covers the entire Microsoft product/application portfolio affected by the exploit kits.

Whether or not the specific exploit kit should be delivered or not is often decided by a browser plug-in script:

```
java: plg_all_vers('Java'),
adobe_reader: plg_ver('AdobeReader'),
flash: plg_ver('Flash'),
quick_time: plg_ver('QuickTime'),
real_player: plg_ver('RealPlayer'),
shockwave: plg_ver('Shockwave'),
silver_light: plg_ver('Silverlight'),
vlc: plg_ver('VLC'),
wmp: plg_ver('WMP')
```

The specific vulnerabilities/exploits which are abused during the time of testing are listed here:

Oracle Java JRE
CVE-2011-3544
CVE-2012-4681
CVE-2012-5076
CVE-2013-1493
CVE-2013-2423
CVE-2012-1723
CVE-2012-0507

Adobe Reader
CVE-2007-5659
CVE-2008-2992
CVE-2009-0927
CVE-2009-4324
CVE-2012-0754
CVE-2010-0188
CVE-2008-0655

Adobe Flash
CVE-2011-0611
CVE-2011-2110

Microsoft
CVE-2006-0003
CVE-2010-1885
CVE-2011-3402
CVE-2012-1889
CVE-2012-1876
CVE-2012-4969
CVE-2012-4792

5 Disclaimer

The information within this document may change without notice. Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information; CSIS Security Group has verified the data as thoroughly as possible.

In no event shall CSIS Security Group be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.

The document may not be distributed or shared without prior written permission from CSIS Security Group A/S.