

Web Exploits: There's an App for That

M86 Security Labs Report

EXECUTIVE SUMMARY

In the last few years M86 Security Labs has seen a dramatic increase in attack or exploit kits. These easy-to-use kits are the backbone of exploits in the “wild”. M86 Security Labs research reviews how exploit kits are developed, distributed and monetized globally. The turnover of exploits is quick. The success rate is high. And, all of this for very minimal cost for the exploit kit users and operators. The details in this report will provide a fundamental understanding of how exploits operate and give the reader a true sense of the business behind the crime.

In the Internet security industry, the terms “exploit kit” or “attack toolkit” are commonly known and understood by security researchers. However, to the average Internet user, these exploit kits are unfamiliar. So, what exactly are these tools? Why are they written? Who uses them and what makes them so popular -- especially, in the wrong hands?



Figure 1: Crimepack Exploit Kit Login Page

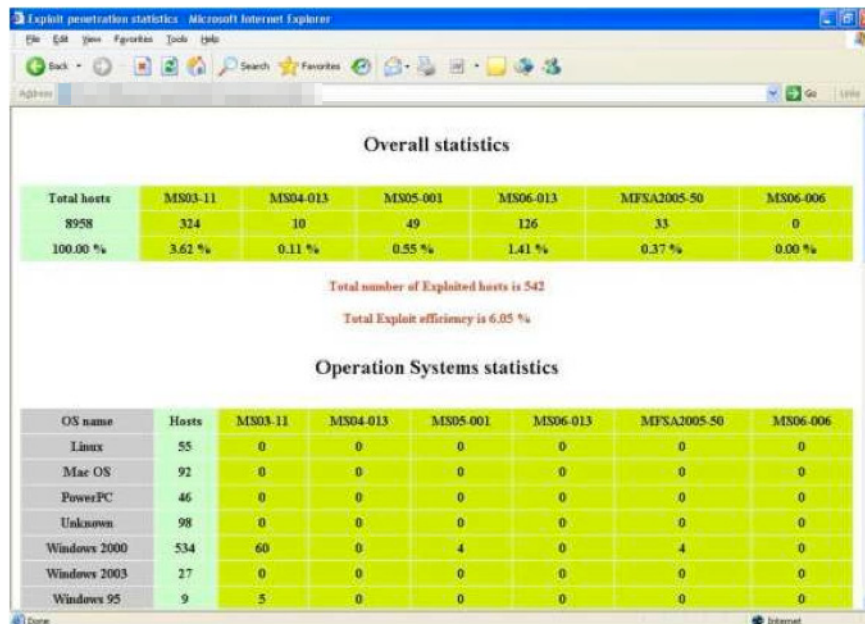
Figure 1 illustrates the login page for one of the newest toolkits available today. It glorifies cybercrime as a serious business, showing images of money, drugs and a gun to convey the typical rewards you can expect when you use the “crimepack” exploit kit.

The main motivation driving the cybercrime industry is the possibility of monetary gain. Cybercriminals find it easier, faster and more cost effective to make money by buying exploits rather than taking the time to create exploits themselves. The demand for these types of tools drives opportunities. Savvy, knowledgeable individuals with skills in developing Web applications and basic knowledge in hacking have filled a niche by creating exploit kits.

ANATOMY OF AN EXPLOIT KIT

An exploit kit is a Web application that is developed using web technologies such as PHP and database products such as MySQL. They allow a kit user to take advantage of the most known exploits in popular applications, such as Microsoft's Internet Explorer, Adobe Acrobat, Reader and Flash Player, as well as many others. The kit is installed on a web server somewhere connected to a database for logging and reporting. The kit interfaces are web based, as you can see in the early example of Web Attacker in Figure two. Cheap, free and highly anonymous web hosting is easily available today and many Cybercriminals take advantage of these types of services to host their exploit kits.

Exploit kits began appearing in early 2006. The first known, popular exploit kit was Web Attacker, which exploited seven previously known vulnerabilities targeting Internet Explorer and Mozilla Firefox browsers. Before exploit kits were available, Cybercriminals had to craft and develop their own exploits, which involved research and testing to discover new vulnerabilities, a highly technical task.



The screenshot shows the 'Web Attacker' exploit kit interface in a Microsoft Internet Explorer browser window. The page is titled 'Exploit penetration statistics' and displays two main sections: 'Overall statistics' and 'Operation Systems statistics'.

Overall statistics

Total hosts	MS03-11	MS04-013	MS05-001	MS06-013	MPSA2005-50	MS06-006
8958	324	10	49	126	33	0
100.00 %	3.62 %	0.11 %	0.55 %	1.41 %	0.37 %	0.00 %

Total number of Exploited hosts is 542
Total Exploit efficiency is 6.05 %

Operation Systems statistics

OS name	Hosts	MS03-11	MS04-013	MS05-001	MS06-013	MPSA2005-50	MS06-006
Linux	55	0	0	0	0	0	0
Mac OS	92	0	0	0	0	0	0
PowerPC	46	0	0	0	0	0	0
Unknown	98	0	0	0	0	0	0
Windows 2000	534	60	0	4	0	4	0
Windows 2003	27	0	0	0	0	0	0
Windows 95	9	5	0	0	0	0	0

Figure 2: Early Exploit Kit Web Interface 'Web Attacker'

The availability of Web Attacker opened the floodgates to newer exploit kits, such as MPack and GPack. As these kits grew in popularity, new exploit kits began to appear more frequently. In the last six months, M86 Security Labs has observed at least a dozen new kits being used in the wild.



The screenshot shows the 'Unique Pack' exploit kit web interface. The page has a dark header with the text 'UNIQUE pack' and 'Unique sheaf spoils'. Below the header, there are tabs for 'Statistic', 'Referer', 'Country', 'Clear', and 'Logout'. The main content area displays two tables: 'Operation Systems' and 'Browsers'.

Operation Systems:

Operation Systems	Totals
Linux	621
Mac OS	2691
Other	629
Windows 2000	140
Windows 2003	151
Windows 95	1
Windows 98	23
Windows ME	19
Windows Vista	12107
Windows XP SP1	23539
Windows XP SP2	5491

Browsers:

Browsers	Totals/Loads/%
Firefox	19933/896/4.50 %
IE	20069/1478/7.36 %
Konqueror	20/0/0.00 %
Mozilla	3659/0/0.00 %
Opera	1711/184/10.75 %
Other	37/0/0.00 %

Function Vparivatel:

Function Vparivatel	Totals
Look details	0

At the bottom, there is a summary row: All Vpars - 0, All Hits - 45429, All Loads - 2558, total % - 5.63 %.

Figure 3: Unique Pack Exploit Kit Web Interface

Exploit kits are routinely being advertised in underground hacker forums. Often, the interfaces to these kits are in Russian, with English being used sparingly indicating perhaps, their target market.

Общая статистика - Страны - Рефералы - Зашедшие IP - Скаченные IP - Очистить - Выйти

Общая статистика		Top10 стран	
Всего хитов	25	United States	10
Всего загрузок	0	Unknown	9
Пробив	0%	Korea, Republic of	2
Пробив по IE	0%	Australia	1
Статистика по браузерам		Italy	1
Unknown	19	Japan	1
MSIE 7	6	Romania	1
Статистика по ОС			
Unknown	19		
Windows XP	6		

Figure 4: AdPack Interface in Russian

PRICING AND PACKAGING

Figures 5 and 6 display examples of advertisements for exploit kits. Figure 5 shows an advertisement for the Fragus exploit kit that supports a multilingual interface, while Figure 6 highlights the Crimpack exploit kit which promises the “highest (exploit) rates for the lowest price.”

Fragus-support

Reputation: 0

Fragus v1.0 - a bunch of exploits

Fragus v1.2 - a bunch of exploits

Admin:

- * Nice design
- * **Multilingual interface (English, Russian)**
- * Admin password protected
- * Expanded statistics on browser (including version), operating systems, countries, exploit, referral ostuku
- * The ability to watch the actual summary statistics without reloading page
- * Files downloaded from the admin panel
- * Ability to specify a file name with which your EXE will be loaded into the system
- * The ability to separate traffic from sellers and keep separate statistics for each
- * The ability for each of the sellers to specify a file or load a random
- * The ability for each seller to specify a different set from the list of exploits, as well, and for general Traphen, it allows off retarding browser sploty for politsya
- * Ability to provide a unique link to the seller on a separate page of statistics without authorization to validate the data
- * The ability to quickly clear, as the overall statistics, and for each seller separately
- * Fragus allows you to monitor ostukami each of the exploits and display it in a convenient form, the ability to knock on the URL is for many EXE
- * Just Fragus gives you the ability to conveniently find a link to traffic, as in the clear, and in an encrypted (encrypted iframe) for general traffic and for ea
- * Settings whole system of directly from admin

Screenshots of the admin panel (first version):
authorization
statistics
Files
Dealers traffic
references to traffic
settings

Figure 5: Fragus Exploit Kit Advertisement in a Forum

We are here to introduce to the newest exploit system on the market and a whole new concept for the people:

"highest rates for the lowest price"



We do not focus on having a fancy ajax layout and shitty rates combined with outrageous prices like other packs, we focus on the outcome.

All exploits used are modded to perfection to get the highest rates out of it possible.
And instead of throwing together as many exploits as possible (like other packs out there)
We decided to handpick a few with higher effectiveness

That includes:

Globals

- + Flash10
- + Adobe Acrobat Reader (<= 9.2)
- + JRE (Many vulnerable)
- + AGGRESSIVE MODE**

Internet Explorer

- + MDAC
- + DSHOW
- + MS09-002

** This is a feature that can be turned on/off from the settings panel
It's a Java applet that will popup asking the user to run the applet, If he approves, exe will load.

Figure 6: Crimepack Advertisement

Sometimes the professional nature of these exploit kits can be seen in their own dedicated Web sites (Figure 7).



ICQ 5654-84282

IMPROVE YOUR BUSINESS WITH

EXPLOIT PACK FROM RUSSIA

(HOW TO BUY)

(SCREENSHOTS)

[more info .ru]

Information

YES Exploit System v. 2.x

We are proud to present a new version-line of our product - "YES Exploit system 2". It's one of most effective browser-exploit packs from Russian blackhat community and it working very successful for a long time. There is excellent quality and good support, be sure - many people trust us.

Undetectable for AV-scanners and doesn't crash browsers.
Stable free av-cleaning procedure every two weeks for licensed users.
Any unexperienced user can work with YES-Exploit system - just read a manual in pack.

It includes the following mod-exploits:
Url_print, Collab.collectEmailInfo, Collab.getIcon, MS09-002, DirectShow(MPE02), MDAC_AdoDb, XML Parsing, Spreadsheet, WMEncoder, fontTags, TN3270, compareTo, JNObject and a few other.

Small overview :

Friendly architecture for plugins and modules.
Blocking filters: IP, cookies, exploited IPs.
Designed for all MS-operation systems.
Integrated encryption of exploits "on-the-fly" [you may choose one from 3]
Detected exploits switch-off function to save your traffic if some exploit has been detected by AV.
Different encryption for PDF-out.

...and more

Figure 7: YES Exploit Pack Web Site

Prices for these exploit kits vary from less than \$100.00 USD to over \$1,000.00 USD. However, the majority of exploit kits tend to be sold for anywhere between \$400.00 USD to \$1,000.00 USD.

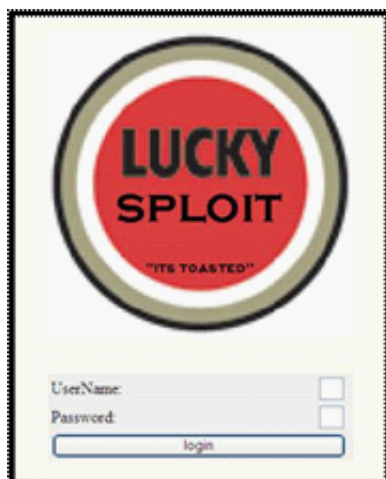


Figure 8: LuckySploit Kit is Sold for Over \$1,000.00

Current version 2.2.1 prices:

\$400 - 1 License

1 License includes:

- + Domain locked one domain (subdomains unlimited)
- + 2 new domain builds if blacklisted
- + Support
- + Minor updates for free
- + Discount on new releases

Extras:

1. Domain re-build for other domain (50\$)

*** NOTE: YOU ARE NOT ALLOWED TO RESELL/SHARE, IF WE CATCH YOU DOING THIS YOUR LICENSE WILL BE REVOKED ***

2. AV-Cleaning (\$80 first time, \$50 after)

If you are interested in promoting/reselling, you will get a good offer

Screenshots can be found at:

[http://profile \[REDACTED\]](http://profile [REDACTED])

Contacts:

MSN: [crimepack@\[REDACTED\]](mailto:crimepack@[REDACTED])

ICQ: [REDACTED]

Figure 9: Crimepack Exploit Kit Cost, Features and Add-ons

- The sale of exploit kits for a flat fee
- The purchase of an obfuscator replacement for an additional fee (to prevent anti-virus software from recognizing malicious code)
- Extra cost to cover any new hosting domains (in the event the current domain is discovered and becomes blacklisted by Security Vendors)
- Simply add new exploits to increase the successful exploitation rate

По вопросам покупки:
Служба поддержки так же ответит на все ваши вопросы:

Translated: For purchasing information ICQ...
Support is also willing to answer all your questions, ICQ...

The heart and soul of the exploit kits are the exploits themselves. The kits typically employ the most well known, published exploit code. Most often, we see unchanged proof of concept code from security related sites or forums, ranging from fairly old to the latest zero-day exploits. Beyond browser-based exploits, M86 Security Labs has noticed an increase in popularity of Adobe Flash, Java classes, and PDF-based exploits.

```
<html><body><div style="display: none"><ul><li id="Tr6yRx6">14z1z156G149A138W155q144v150q149X71D106r150R148S151E147H140f15
<script>
var RHv17cR = new String(""); RHv17cR = document.getElementById("Tr6yRx6").innerHTML;
FqqDbipr = document.lastModified; var eight = 8; mGtab6Lr = 0;
mGtab6Lr = abab(FqqDbipr); RHv17cR = RHv17cR.replace(/["0-9]/g, '');
function jKHUKiU1KyYXKH ( ZqbP2w,V532Th5B ) { var zQNZXi31 = new String();var ZnJnfPLSMQ = new String();
var mGB10cN10 = ZqbP2w.split(';'); for(EuAcF = 0;EuAcF < mGB10cN10.length-1;EuAcF++)
( zQNZXi31 = String('f:rom<#a#r'<code>.replace(/@|&|'\\'|\\|\\|\\|/ig, ' ');(mGB10cN10[EuAcF] - V532Th5B);
ZnJnfPLSMQ = ZnJnfPLSMQ + zQNZXi31); return ZnJnfPLSMQ;var vnfjqq = Date();MdLcK = jKHUKiU1KyYXKH(RHv17cR,mGtab6Lr);
var mGB10cN10 = 'zQNZXi31';function krasddk(zxc) {eval(zxc); return;};krasddk( MdLcK );</script></body></html>
```

In the case of malicious Javascript code, it is almost always obfuscated, greatly reducing the effectiveness of classic signature-based security products.

[Browsers](#)
[Systems](#)
[Countries](#)
[Referers](#)
[Clear DB](#)

Traffic

Browser	Uniques	Downloads	Percent
Total (100 %)	912	556	60.96 %

Page 6

From a Cybercriminals perspective, the most important piece of the exploit kit is the administration panel, which is a Web-based interface that allows the user to configure and obtain information from the exploit kit. Upon successful exploitation, the user can change the malicious executable to be distributed, or potentially update their database configuration.

The user can also view statistics using the Web-based interface. The kind of statistics available to the user varies from the number of successful exploits, the victim's geographical location, the operating system, and browser type and version being used by their victim, among other details.

With only a few hundred dollars, anyone can become the proud owner of one of the latest versions of an exploit kit. This wasn't difficult until now, right? It's interesting to note that at this point, there are very few difficulties faced by the novice user of an exploit kit, even one with minimum technical skills.

HOSTING THE EXPLOIT

In order to configure the exploit kit, the user must install it onto a Web server. It's very easy to find free hosting, or for minimal cost, paid hosting can provide the standard set of services needed to install an exploit kit, such as PHP and MySQL.

```
Установка:  
- Заливаем файлы на сервер  
- Загружаем ваш exe файл в папку со ссылкой с названием 1.exe  
- Создаем базу данных  
- Открываем файл config.php и вписываем данные базы, полный линк до pdf.php и полный линк до load.php,  
а так же пароль/логин на доступ к статистике (пароль в MD5 надо шифровать два раза!)  
- Далее вводим в браузере http://ваш_сайт/spl/_install.php  
если установка прошла гладко, то увидите "Installation finished Please delete install.php"
```

Figure 13: Readme for UniquePack

Translation:

Installation:

- Upload the files to the server
 - Upload your file to the same folder and rename it to 1.exe
 - Create DB
 - Open config.php and add db information, full path to pfg.php and full path to load.php,
Also password/login for statistics access (password should be encrypted using MD5 twice!)
 - Now browse to http://your_site/spl/_install.php
- If installation succeeded, you will see "Installation finished Please delete install.php"*

The most technical information a user needs to know are basic Unix commands for copying a file ("cp"), modifying file permissions ("chmod"), and removing a file ("rm"). Knowing these three simple commands can result in a successful installation of an exploit kit. In some cases, even this knowledge is not necessary, as some toolkits can be fully installed through a Web-based interface as can be seen in Figure 14.

```
* Fragus hidden from search bots, which allows for longer does not scorch domain  
* Fragus best optimized to work with high traffic and minimal load on the server  
* Installation takes less than 2 minutes, no need to go into a file and something to edit his hands, the installer will help you
```

Figure 14: Fragus Installation—Easy Install

One of the most important measures of every exploit kit is the percentage of successful exploits, also known as the Exploitation Rate. This rate depends on several parameters, such as the type of traffic or quality of the exploit code, and the ability to customize exploits for every victim (based on browsers and/or other client application versions).

The most important criteria is the selection of available exploits that are used by the exploit kit. Most kits provide a different set of exploits for different browsers-- from the antiquated MDAC exploit for Internet Explorer 6, to the Holy Trinity of infamous PDF exploits (printf, collectEmailInfo and getIcon) which affect the large user base of Adobe Acrobat/Reader users. Of course, the best option for successful exploitation is zero-day exploits. Most often, the exploit kit creators continually update the set of exploits included in their product to maintain a high exploitation rate.

```

Версия 1.3.2 [16.12.2009]
* Добавлен pdf Doc.media.newPlayer (на сегодняшний день еще 0-day <=9.2)
* Изменен шрифт и шрифт pdf
* Добавлена java calendar

Версия 1.3.1 [16.11.2009]
* Добавлена хорошая функция блокировки ботов SE (поисковых систем и прочих), уменьшает риск спалить домен.
  - добавлен Robots.txt
* Немного переделан pdf
* Полностью переделан Java D&E (небольшой прирост пробы, хорошо на опере, теперь полностью адекватный отступ)
* Добавлен соц лаг, не жалит еще, отступ идет не с выдачи соц лага, а непосредственно после скачивания и запуска файла.

Версия 1.3 [25.10.2009]
* Обновлено определение браузера и ОС по куэр агенту, теперь полное предоставление того что вы идёте с траффа от windows/linux до мобильных/rocket
* Сплоты выдаются только Windows экзран.
* Добавлена хорошая функция блокировки ботов SE (поисковых систем и прочих), уменьшает риск спалить домен.
* Переделан pdf
* Браузеру IE pdf выдается только в случае если установлена уязвимая версия adobe acrobat.
  - и омаканию в Firefox и Opera можно определить версию плагина adobe acrobat
* Добавлен Java D&E (небольшой прирост пробы, хорошо на опере)
* Добавлены некоторые ActiveX эксплойты для IE (незначительно).
* Новые багины

Версия 1.2 [27.07.2009]
* Убран Snapshot
* Добавлен Spreadsheet, эксплойт для IE при установке офис.
* Добавлена возможность загрузки файла через админку.
* Изменен pdf.

Версия 1.1 [15.07.2009]
* добавлен DirectX DirectShow эксплойт, дает проба на XP, 2003 на IE 6-7.
* добавлен Font Tag, эксплойт для Firefox 3.5
* изменен шрифт ифрейма
* новые изменения в старых сплотах.

Версия 1.0 [27.04.2009]
* Релиз.
сплоты в связке:
MDAC
MS009-02
Snapshot
Telnet - for opera
PDF collab.getIcon
PDF Util.Printf
PDF collab.collectEmailInfo

```

Figure 15: Eleonore Version Details

Translation:

Version 1.3.2 (16.12.2009)

- pdf Doc.media.newPlayer added (currently 0-day <= 9.2 (Adobe Reader version)
- Pdf Crypting changed
- Java calendar added

Version 1.3.1 (16.11.2009)

- Blocking SE bots (search engines) functionality added. Reduce the risk of domain disclosure
- Robots.txt added
- Pdf was changed a little
- Java D&E renewed (increases exploitation rate, works for opera)

Version 1.3 (25.10.2009)

...

Pdf provided only if vulnerable Adobe acrobat version installed

...

Version 1.2 (27.07.2009)

...

Snapshot removed

Spreadsheet added

...

Version 1.1

DirectX DirectShow exploit added

Tag Font exploit added, exploiting Firefox 3.5

...

Version 1.0 (release)

Exploits:

MDAC

MS009-02

Snapshot

Telnet - for opera

PDF collab.getIcon

PDF Util.Printf

PDF collab.collectEmailInfo

Some exploit kits do allow the user to choose the set of exploits to be implemented, but generally they are preconfigured.

IMPLEMENTING THE EXPLOIT

After the successful deployment of an exploit kit, the only remaining task is how to direct the largest possible number of victims to the kit's exploit page. This is a fundamental problem faced by the user of the kit. Like any business, the exploit buyer seeks to maximize its exposure and subsequently the revenue. So, how does the attacker solve the problem? There are a few options: the first is to utilize sending spam messages with an appropriate link (often known as a blended threat email), another popular method is to create bogus Web sites and promote them through various search engine optimization (SEO) techniques. However, the most effective technique is injecting iFrames within a legitimate Web site that direct back to the exploit page. The iFrame injection is possible by attacking legitimate Web servers (for example, using SQL injection) or if available, using stolen FTP credentials. Exploit kit operators might carry out these activities themselves, or pay someone else for these services.

In order to increase the exploitation rate, a user needs people to visit their exploit page. To achieve this, there are individuals who specialize in selling Web traffic for any purpose.

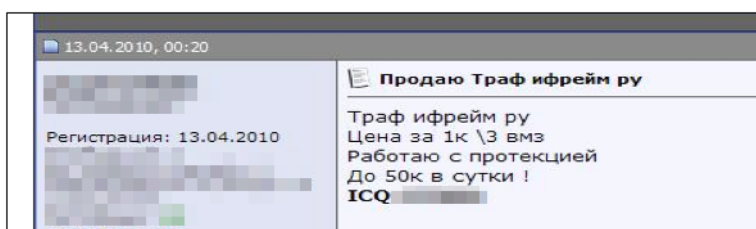


Figure 16: Selling Traffic (1,000 Redirects for 3 Units)

Translation:
Selling Traffic iframe .ru
Traffic iframe .ru
Price for 1K / 3 WMZ (web money)
Working with protection!
Up to 50K in a day!
ICQ ...

Cybercriminals will select traffic which is most suitable for their planned criminal activity. For example, if the user plans to drop banking Trojans onto victims' machines to steal money from their bank accounts, the Cybercriminal will prefer traffic from wealthy Western countries where there is a higher chance to find people using online banks.

STATISTICS

From this point, the exploit kit's malicious page will be provided to the victim without their knowledge. The law of large numbers, which holds that even a small percentage of a large number is still a large number, allows novice criminals create a small-scale botnet in a fairly short time.

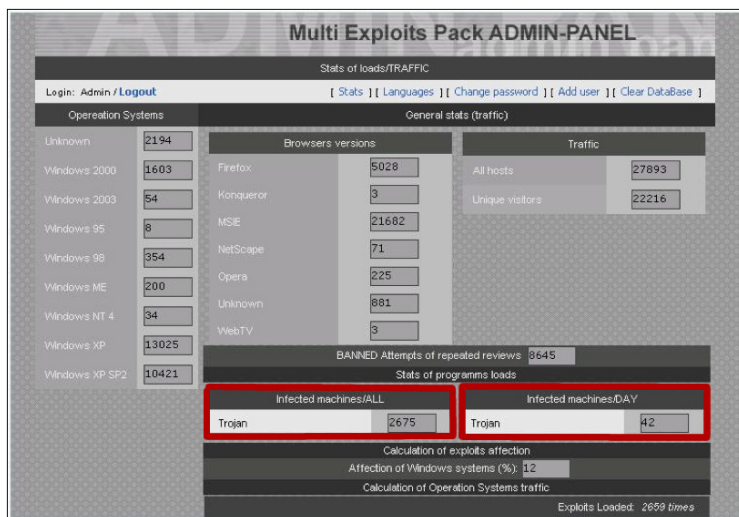


Figure 17: MultiExploits Pack Panel

In Figure 18, the LuckySploit exploit kit user has the extended capability to monitor the kit's performance in real time.

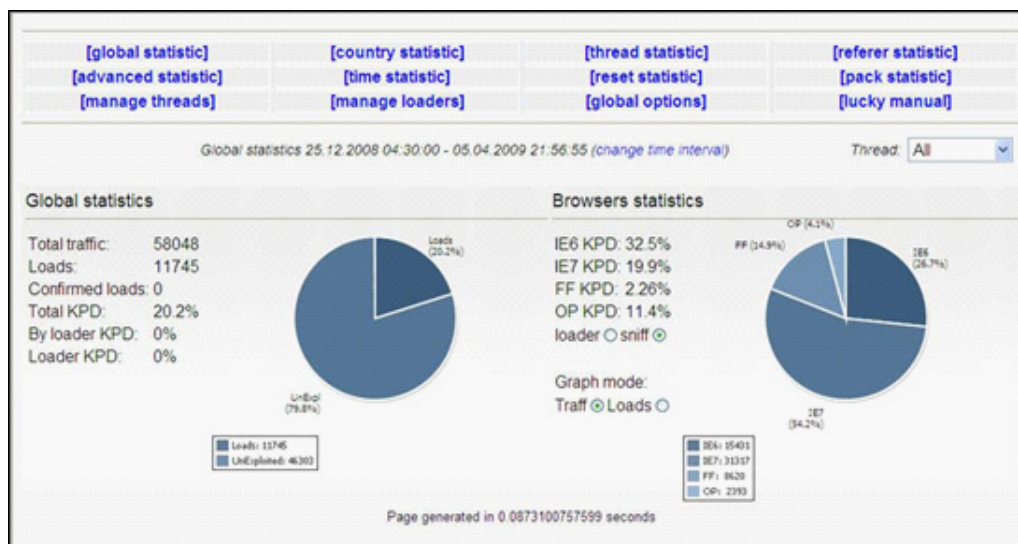


Figure 18: LuckySploit Statistics

MONETIZATION – HOW DO THE EXPLOIT KIT OPERATORS MAKE MONEY?

After acquiring an exploit kit, the chief goal of the cybercriminal is to make money, and there are numerous ways this may be achieved. But first, it's important to understand that the operators of exploit kits are merely one part of an extensive underground economy where the participants are often specialized, offering tailored products and services to other players through shady forums and personal contacts.

Cybercriminals are interested in using exploit kits to install malware for personal gain and potential profitability. The kit operators may install their own creations or third-party malware. In most cases, the installed malware is usually a version of a bot client which enables the bot herder to control the infected host for the following purposes:

- Stealing critical information from the victim, e.g. keyloggers or other malware attacks where the stolen data is later sold or used.
- Using the victims' computing resources for sending spam, where the bot herder earns money for messages sent, or by signing up to a spam affiliate program like the common "Canadian Pharmacy" program.
- Installing other malware like fake anti-virus scareware, where revenues can be earned from successful "registrations", or Pay-Per-Install (PPI) programs.

One popular example of a cybercriminal's method of making money is Pay-Per-Install (PPI) programs, where the criminals are paid for installing third-party malware. In this case, the exploit kit operator finds a suitable PPI program and becomes an affiliate. Affiliate members obtain malware from the PPI program's Web site and get paid for each successful install of the malware on a victim's computer. PPI programs are prolific and varied; some PPI programs create their own malware, while others are merely distributing third-party malware. The malware itself can vary, ranging from information stealers like Zeus, spambots like Rustock, password stealers, or generic downloaders. The exploit kit operator might also bundle several pieces of malware from different PPI programs in the payload.

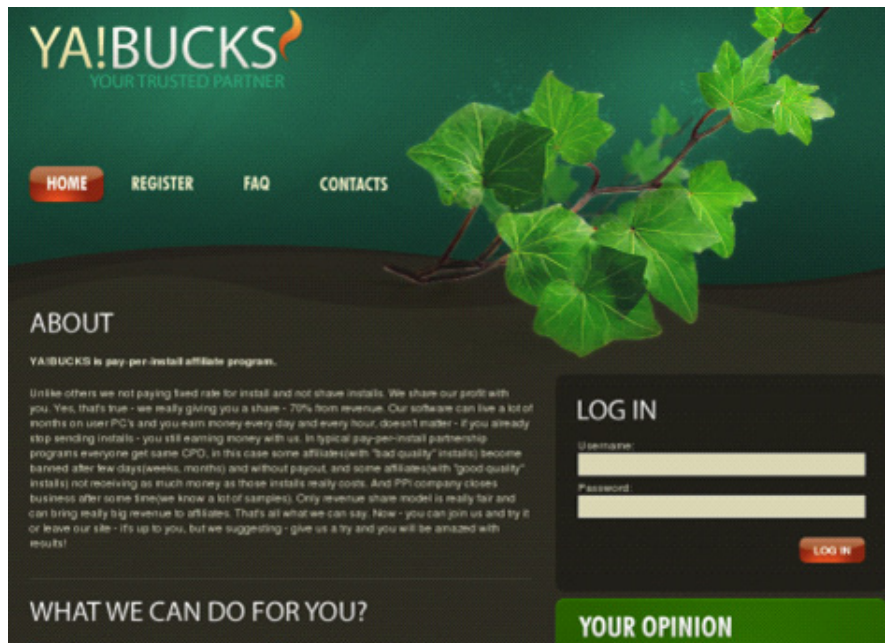


Figure 19: Example of a Pay-Per-Install Program Web Site

Payments of successful installs are made regularly to affiliates, often on a daily or monthly basis. The rates per install vary depending on what country the target computer is located. The United States is a favored country, where installs command a higher price. Below is a recent pay schedule for one PPI site:

Country	Rate per 1,000 installs \$US
USA	170
Canada	120
United Kingdom	110
Australia, Europe	50

Figure 20: Pay Per Install Pay Schedule

Other types of payment programs also exist. Notable are those programs dealing with fake anti-virus 'scareware' products, which trick users into paying 'registration' fees to enable the 'protection' software. These programs have a revenue sharing model, where affiliates are paid a share of the revenue generated from the registration fees originating from their installs. Some sites advertise up to a 60% share of these revenues.

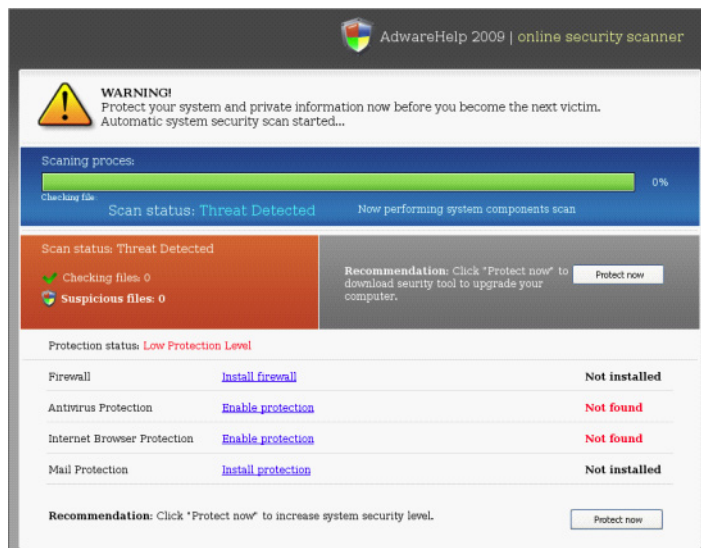


Figure 21: Fake Anti-virus Programs Use Revenue-sharing from 'Registration' Fees

Another way an exploit kit operator may make money is by renting out their fully working system to others by supplying login privileges to the admin console. Here, the other party does not have to concern themselves with the exploit kit or its configuration, because they merely use it and drive traffic to their own chosen landing page. In this way it is a service provided to others just like those now popular in the commercial world, Crimeware-as-a-Service?

In order to give life to some of the concepts above, let's consider a real life example, which we observed in February 2010 through a spam campaign touting 'photoshock' pictures. The operator of the exploit kit most likely paid another party to perform the spam campaign for them, and in this case the spam originated from the Pushdo/Cutwail botnet.

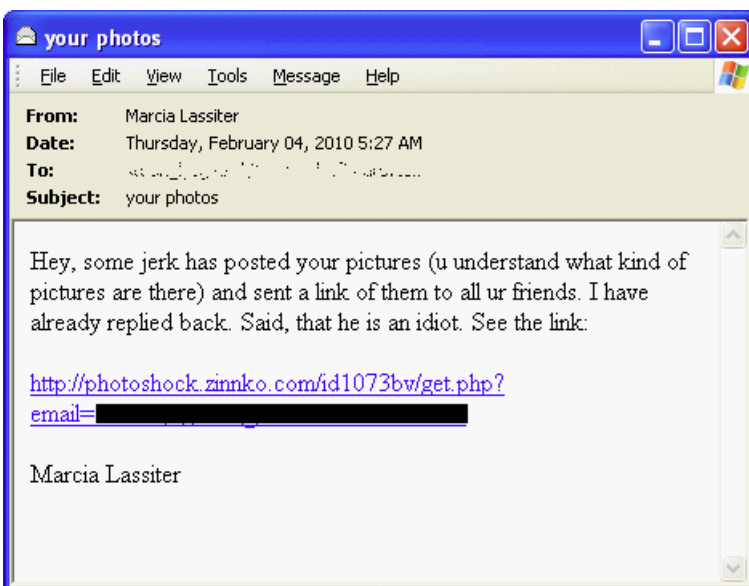


Figure 22: Spam Campaign Driving Users to a Web Page

In this case the landing page contained a hidden iFrame that allowed exploits to be served up from another server hosting the FS Pack kit.



Figure 23: Hidden iFrame Pulling in Content from a Remote Server Hosting an Exploit Kit

The admin pages from the exploit kit clearly show the zinnko.com referrer domains used in the spam campaign, as well as another campaign using facebook.com in the URLs.

Home	Browsers	OS	Countries	Referrers	Reedit pdf/swf Cleaning
Domain	Number				
Unknown	1032				
auth.facebook.com	577				
auth.facebook.com	537				
auth.facebook.com	512				
auth.facebook.com	497				
auth.facebook.com	497				
auth.facebook.com	466				
auth.facebook.com	439				
auth.facebook.com	431				
auth.facebook.com	419				
auth.facebook.com	418				
auth.facebook.com	379				
auth.facebook.com	336				
auth.facebook.com	330				
auth.facebook.com	329				
archive.	294				
photosbank.	280				
photobanl	270				
archives	260				
photoshock	249				
photostock	248				
letitbit	233				
archive	232				
photobank	218				
archives	206				
letitbit	204				
archive.	201				
photostock	200				
archive	194				
photosbank	194				
archive	187				
photosbank	185				
photosbank	185				
photoshock	180				
photostock.sadewar.org	178				

Figure 24: FS Pack Admin Console Shows Referrers Domains Used in Spam Campaigns

The admin page in Figure 25 shows 5,032 successful installs for the day. Assuming a PPI model where the affiliate is earning a modest \$100.00 USD per 1,000 installs, this would result in revenue of about \$500.00 USD for the day.

Home	Browsers	OS	Countries	Referrers	Reedit pdf/swf Clean
Per Day:					
Unique	39172				
Downloads	5032				
Total:					
Hits	64367				
Unique	39172				
Downloads	5032				
Punched	12.85 %				

Figure 25: FS Pack Admin Console Showing Number of Successful Installs at 5,032

SUMMARY

In this paper we have looked at the history of exploit kits or attack toolkits, seen examples of what they look like, how they work and discussed what they can be used for. Also of importance was the point on just how little technical knowledge an aspiring Cybercriminal needs to become active.

The second part of the paper looked at the money trail. We discovered how much these kits are sold for, therefore how much their creators are making. We then went down a level and looked at the kit operators and the different options they have to make money. We presented detail on one method, Pay-Per-Install or PPI programs and how the operators were either paid for each successful install or received a share of any revenues through affiliate programs.

The aim of this paper was to explain the exploit kits, how they work and how easy they are to use. It hopefully gives some insight into why we are seeing such a massive increase in the number of attacks targeting exploits and to what we are facing in today's Internet threat landscape.

List of Exploit Kits

- WebAttacker
- MPack
- GPack
- AdPack
- IcePack
- Neosploit
- MyPolySploit
- XCore
- UniquePack
- LuckySploit
- Yes Toolkit
- SPack
- Liberty
- Fiesta
- Eleonore
- MyLoader
- SEO Toolkit
- JustExploit Elite Loader
- Clean Pack
- Shamans Dream
- Siberia
- Fragus
- Max Toolkit
- CrimePack
- FSPack
- and others

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 04/25/10