DNS Footprint of Malware

Ed Stoner
ers@cert.org
CERT Network Situational Awareness
Anexa

Automated Run-Time Analysis environment
Malicious Software Catalog of millions of samples
~ 250,000 uniq md5s every 6 months

Network Touchpoints

• Domain Names – 119,000 of them over 6 months
• IP addresses
Malicious Domain Name Research

Anexa
Network Touchpoints(Domain Names)

SIE
Domain Name -> IP address Mappings

SiLK + YaF
1. Find Flow to those IP addresses
2. Find DNS patterns
3. Find DNS lookups to discovered IP addresses
Data Set

Domain Names

- SIE - 27.8k
- Not Found - 91k more

27859 domains → 204931 IPs
Data Set

Domain Names

- SIE - 27.8k
- Not Found - 91k more
- Domain Flux

27859 domains → 204931 IPs
Coverage by MD5

- Not Found
- Found - 41%
Control Case

27859 Malicious Domains

27859 Random Domains
Top Level Domains - Malware

- net: 23.9%
- com: 21.0%
- info: 19.9%
- org: 16.7%
- biz: 6.7%
- cn: 3.0%
- other: 10%
Random TLD distribution

Domains

- .com
- .net
- .org
- .cn
- .de
- .it
- Other
GeoLocation based upon IP address

IP Addr

- China - 29%
- Algeria - 13%
- United States - 10%
- Morocco - 7.5%
- Saudi Arabia - 5%
- Tunisia - 4%
- Germany - 2%
- Other - 28%

Geolocation by MaxMind
Random GeoLocation distribution

IP Addresses

- United States - 58%
- Private/exp. - 10.5%
- China - 5%
- Germany - 3%
- Netherlands - 2.5%
- United Kingdom - 2%
- Other - 19%

Geolocation by MaxMind
Top domains (by md5)

2009-07-17 to 2010-02-10
auto.search.msn.com,23278
www.screenblaze.com,23152
www.wowchian.com,8333
www.fenomen-games.com,6999
www.gamecentersolution.com,4621
downloadfixandlove.com,4339
ads.netbios-local.com,2581
irc.zief.pl,2446
www.jcwz.net,2374
ayb.trinityacquisitions.com,2083
ayb.maximumexperience.com,2083
myart-gallery.com,1736
jet-arts-center.com,1716
videoporntrue.net,1645
freeavtest.com,1497
crystal-arts.net,1361
tubepornlive.com,1300
siteload.cn,1239
hostnsload.cn,1239
pornotube912.com,1225

2010-04-01 to 2010-09-27
mk.maxthon.cn,11516
google.com,8731
download.flvdome.com,7518
submit.flvdome.com,7278
www.jd9.net,7102
auto.search.msn.com,6435
www.screenblaze.com,6187
msn.com,5666
all-internal.info,4478
cfg.353wanwan.com,3987
crl.verisign.com,3950
csc3-2004-crl.verisign.com,3945
digitalartsaward.com,3608
cts.hotbar.com,3009
mediaartsplaza.com,2851
www.fenomen-games.com,2813
ayb.host255-255-255-0.com,2792
ayb.host192-168-1-2.com,2792
ayb.host127-0-0-1.com,2792
config.ie.sogou.com,2623
## Top nameservers (by md5)

<table>
<thead>
<tr>
<th>NameServer1</th>
<th>Count</th>
<th>NameServer2</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1-6.wingdns.net.</td>
<td>10937</td>
<td>ns1-2.nameself.com.</td>
<td>9012</td>
</tr>
<tr>
<td>ns1-4.trafficclub.com.</td>
<td>8986</td>
<td>ns1-4.google.com.</td>
<td>8976</td>
</tr>
<tr>
<td>ns1-5.byet.org.</td>
<td>8928</td>
<td>ns1-2.dns.com.cn.</td>
<td>8845</td>
</tr>
<tr>
<td>ns1-2.bluehost.com.</td>
<td>8795</td>
<td>dns1-2.uni5.net.</td>
<td>8779</td>
</tr>
<tr>
<td>dns1-4.kinghost.com.br.</td>
<td>8771</td>
<td>ns1-2.ukraine.com.ua.</td>
<td>8755</td>
</tr>
<tr>
<td>ns11-16.bigwww.com.</td>
<td>8752</td>
<td>ns,ns2,ns3.pipni.cz.</td>
<td>8744</td>
</tr>
<tr>
<td>ns1-3.surf-town.net.</td>
<td>8739</td>
<td>ns1-2.ignum.com.</td>
<td>8738</td>
</tr>
<tr>
<td>dns,dns2.site5.com.</td>
<td>8737</td>
<td>ns1-4.cloudns.net.</td>
<td>8736</td>
</tr>
<tr>
<td>ns1-4.serveriai.lt.</td>
<td>8735</td>
<td>ns1-3.cnchost.com.</td>
<td>8734</td>
</tr>
<tr>
<td>ns1-2.infobox.org.</td>
<td>8734</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Domain Name Characteristics

<table>
<thead>
<tr>
<th></th>
<th>Baseline Sample</th>
<th>All Malicious Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-Labels (example.com)</td>
<td>3227 (11% of)</td>
<td>67,398 (56% of)</td>
</tr>
<tr>
<td>Three-labels (<a href="http://www.example.com">www.example.com</a>)</td>
<td>7204 (25% of)</td>
<td>45,944 (38% of)</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>36 (0% of)</td>
<td>22,153 (18.5% of total, 50% of 3-label)</td>
</tr>
</tbody>
</table>
Registrars and Dynamic DNS

Dynamic DNS
- 22,153 out of 119,385
- 18.5% of total, but nearly 50% of the 3rd level domains)

Registrars (2nd Level Domains)
- 67,398 out of 119,385
- 56% of total

75% of malicious domains
## Lifetimes

<table>
<thead>
<tr>
<th></th>
<th>Malicious Domains</th>
<th>Random Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime</td>
<td>104 days</td>
<td>110 days</td>
</tr>
<tr>
<td>After Removal of</td>
<td>105 days</td>
<td>165 days</td>
</tr>
<tr>
<td>Akamai, rbls, and cdns</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RBLs – Remote Block Lists  
CDNs – Content Distribution Networks
Parked Domains

Domains that are “parked” on a non-operational IP address

- Often unroutable IP space (192.168.1.1, 127.0.0.1)
- Sometimes strange IP addresses (1.2.3.4, 1.1.1.1)
- Other times popular IP address (google, akamai, microsoft)
Parked examples

- domains parked at google ip space:

  a.emmai.info    ac3n.info    adslstats.net
  boqegouti.org   bujozami.cn  customme.cn
  dreamnaut.no-ip.info  f.unicat.org  forbes-2009.com
  forrodesejomusical.com.br  google-resolve.servehttp.com  gooogle.com
  hackhound.org    hurt23.mine.nu  lanzadorx.com
  mail.xakep.ru    mgq2748586.s124.288idc.com  omfgitzpjx.info
  ruvegaro.cn     sickshot.us.to  speedytorrents.net
  vampire008tw.xxyy.info  viptrips.net  wmi.pho24.info
  www.nuevaq.fm    www.opensc.ws  yc.shockwavesfx.com
## Normal Parking

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>20091129</td>
<td>expired.domain.com</td>
<td>192.168.118.26</td>
</tr>
<tr>
<td>...</td>
<td>....</td>
<td>...</td>
</tr>
<tr>
<td>20091209</td>
<td>expired.domain.com</td>
<td>192.168.118.26</td>
</tr>
<tr>
<td>20091210</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091211</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091211</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091212</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091213</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091214</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091215</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091216</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091217</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091218</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091219</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
</tbody>
</table>
## Normal Parking

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>20091129</td>
<td>expired.domain.com</td>
<td>192.168.118.26</td>
</tr>
<tr>
<td>20091209</td>
<td>expired.domain.com</td>
<td>192.168.118.26</td>
</tr>
<tr>
<td>20091210</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091211</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091211</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091212</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091213</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091214</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091215</td>
<td>expired.domain.com</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>20091216</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091217</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091218</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
<tr>
<td>20091219</td>
<td>expired.domain.com</td>
<td>69.64.155.121</td>
</tr>
</tbody>
</table>
## Example of Parking until Operations

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>20091129</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>...</td>
<td>....</td>
<td>...</td>
</tr>
<tr>
<td>20091209</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091210</td>
<td>badguy.com</td>
<td>123.117.77.10</td>
</tr>
<tr>
<td>20091211</td>
<td>badguy.com</td>
<td>125.34.77.52</td>
</tr>
<tr>
<td>20091211</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091212</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091213</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091214</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091215</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091216</td>
<td>badguy.com</td>
<td>97.67.118.26</td>
</tr>
<tr>
<td>20091217</td>
<td>badguy.com</td>
<td>97.67.118.26</td>
</tr>
<tr>
<td>20091218</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091219</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
</tbody>
</table>
## Example of Parking until Operations

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>20091129</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>20091209</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091210 - Thursday</td>
<td>badguy.com</td>
<td>123.117.77.10</td>
</tr>
<tr>
<td>20091211 - Friday</td>
<td>badguy.com</td>
<td>125.34.77.52</td>
</tr>
<tr>
<td>20091211</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091212</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091213</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091214</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091215</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091216 – Thursday</td>
<td>badguy.com</td>
<td>97.67.118.26</td>
</tr>
<tr>
<td>20091217 - Friday</td>
<td>badguy.com</td>
<td>97.67.118.26</td>
</tr>
<tr>
<td>20091218</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>20091219</td>
<td>badguy.com</td>
<td>255.255.255.254</td>
</tr>
</tbody>
</table>
Fast Flux

“fully qualified domain name (such as www.example.com) to have multiple (hundreds or even thousands) IP addresses assigned to it. These IP addresses are swapped in and out of flux with extreme frequency, using a combination of round-robin IP addresses and a very short Time-To-Live (TTL) for any given particular DNS Resource Record (RR)”
old FastFlux working definition

Previous definition:  
20 different ASNs w/ 25 different IP-addresses  
TTL of less than 2000 seconds
FastFlux Hosting
## Most IPs per Domain – Unsophisticated Criminals

<table>
<thead>
<tr>
<th>Domain</th>
<th>IPs</th>
<th>md5s</th>
<th>handle</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>02fgu145501.cn</td>
<td>4491</td>
<td>44</td>
<td>no</td>
<td>Unknown fastflux botnet c2</td>
</tr>
<tr>
<td>viotto.dyndns.org</td>
<td>1602</td>
<td>1</td>
<td>yes</td>
<td>discusses SpyNet 1.8 and 2.0</td>
</tr>
<tr>
<td>momo26.no-ip.biz</td>
<td>990</td>
<td>1</td>
<td>yes</td>
<td>ZeuS C2, momo.exe, not in virustotal</td>
</tr>
<tr>
<td>malchh.no-ip.biz</td>
<td>901</td>
<td>3</td>
<td>yes</td>
<td>Turkojan v1, discussing turkojan v4</td>
</tr>
<tr>
<td>spy-pc1.no-ip.biz</td>
<td>842</td>
<td>1</td>
<td>no</td>
<td>Poison/BiFrose</td>
</tr>
<tr>
<td>yousufshah.no-ip.biz</td>
<td>661</td>
<td>2</td>
<td>yes</td>
<td>discussing facebook passwords, CyberGate</td>
</tr>
<tr>
<td>souhil5.no-ip.info</td>
<td>632</td>
<td>1</td>
<td>yes</td>
<td>Poison/BiFrose, discussing biFrose</td>
</tr>
<tr>
<td>semao.myftp.biz</td>
<td>607</td>
<td>2</td>
<td>yes</td>
<td>biFrose Variant</td>
</tr>
</tbody>
</table>
Flux Spread of Malicious Domains

![Bar Chart](chart.png)

- 8320 for index 2
- 5994 for index 3
- 4486 for index 4
- 3582 for index 5
- 1491 for index 10
- 435 for index 20
- 96 for index 50
- 23 for index 100
Flux Spread w/ Random Sample

- Malicious
- Random

- Bars for 2: 8320
- Bars for 3: 5994
- Bars for 4: 4486
- Bars for 5: 3582
- Bars for 10: 1491
- Bars for 20: 435
- Bars for 50: 96
Flux Spread w/ CDNs removed

- Malicious
- Random
- w/o CDNS
New Algorithm

- domains with:
  - 20 or more A recs
  - IPs are in 20 or more ASNs
- of those domains:
  - find IP sets with more than 5 addrs in common
  - white list known CDNs
what we're finding

6/01/2010:
cc.allaboutcontrol, com.haijeihefooobeekahkohweto, net.jdhyh1230jh, ru.mmjl3l45lkjdbb

7/15/2010:

08/29/2010:
Flux Statistics
Domain Flux

Definition:

generation of a large number of pseudo-random domains using the same seed

1.) to hide communication channel

2.) to prevent domains being blocked

looks like:

aabdykuiwcymao.biz, aaemxwiugkeq.info, aafueyeoya.biz, aaiahiugkeq.biz,
aaiavsiugkeq.biz, aakmbsiugkeq.biz, aaonhaiugkeq.info, aapgpqeoya.info,
abahfodsholapet.cc, abcyxmnansnan.com, abdqbenansnan.com, acjybkdsholapet.org

OR:

ysggof.1dumb.com, yxnhwhmrckk.dynserv.com, yxrropwfrvz.yi.org,
yybvnivcjei.3-a.net., yzscnmh.afraid.org, zbtjjqq.afraid.org,
zdhmosqbmuy.3-a.net, zeczrpsck.dynserv.com, zibjyomx.hn.org, zpkwnmip.hn.org,
zppkhkxsawq.yi.org., zqptrlup.dynserv.com, zsbbrdwp.dynserv.com
Domains per MD5

[Bar chart showing the distribution of domains per MD5 hash. The y-axis represents the number of MD5s, and the x-axis represents the number of domains. The chart shows a majority of MD5s associated with 1 domain, with a smaller number associated with 2, 3, 4, 5, and 6-10 domains, and a negligible number associated with more than 10 domains.]
NxDomain

need to capture to find:
1.) domain flux
2.) other domains seen for only one day
   - 3096 different md5s (1.2%)
3.) What else are we missing?
YAF

yet another flowmeter
http://tools.netsa.cert.org/yaf
- initial public release Mar. 28, 2006
- processes packets from pcap or live capture
- exports flow to IPFIX format
- tcp reassembly, fragment reassembly
- widely deployed
- supports 10Gbs capture
IPFIX

RFC 5101,5102,5103  (previously Cisco Netflow v9)

abstract data types:

unsigned8, unsigned16, unsigned32, unsigned64, signed8, signed16, signed32, signed64, float32, float64, boolean, macAddress, octetArray, string, dateTimeSeconds, dateTimeMilliseconds, dateTimeMicroseconds, dateTimeNanoseconds, ipv4Address, ipv6Address

over 200 Information Elements already defined
very widely supported in hardware and software
YAF current status

- as of Jul 27, 2010
- now supporting:
  - udp-uniflow
  - FTP, HTTP, IMAP, RTSP, SIP, SMTP, SSH, DNS, IRC, NNTP, POP3, SLP, TFTP
- custom protocol decoders as plugins
- as C code or regex