Coping With Malware and Other Sorts of Automated Abuse

Joe St Sauver, Ph.D.
(joe@internet2.edu or joe@uoregon.edu)
Security Programs Manager, Internet2

Tuesday, October 6th, 2009 4:30-5:30PM Navarro Room
Internet2 Fall Member Meeting, San Antonio, TX
http://www.uoregon.edu/~joe/malware/

Disclaimer: all opinions expressed are solely those of the author and do not necessarily represent the opinion of any other entity or organization.

Is Malware Something That Your University and Internet2 Should Be Concerned About?

Malware, PII Breaches, Spam & "Fire Drills"

- Most colleges and universities remain exceedingly concerned about the theft of personally identifiable information (PII).
- While PII can be accessed via a variety of routes including mis-coded web-based applications (e.g., things like SQL injection attacks), PII breaches can also occur as a result of systems becoming infected with malware.
- Malware infections can also result in compromised hosts acting as spam sources, often causing university email to get broadly blocked as a result.
- Finally, malware can tend to drive a "fire drill" culture as security staff spend all their time dealing with compromised systems rather than having the time and resources to "get in front of" some of the other cyber security threats they face.
- **It is absolutely key for every college and university to stay on top of the malware issue.**

Malware Is Getting More Serious, Not Less

- We're seeing more malware in circulation, as malware authors get better at automatically tweaking and repacking malware so as to avoid detection by signature-based antivirus products.
- If the bad guys/bad gals release a newly tweaked version of their malware every hour, but antivirus vendors only release new signatures a couple times a day, the bad folk are guaranteed a period during which detection will be poor.
- The sophistication of malware is also increasing as:
  -- professional occupational specialization takes place (some miscreants specialize in writing code, others search for new vulnerabilities, still others manage existing compromised systems or register new domain names, etc.)
  -- cyber criminals empirically learn what works and what doesn't (the world is one giant laboratory for them!), and
  -- profits from past criminal activities become available to underwrite and support future malware-related projects.

Why Is Malware Getting Distributed?

- Speaking of "profit," at one point, miscreants distributed malware just for "street cred"/fame, but now (with the exception of nation-state hacker/crackers), it is **all about money.**

- For example, pay-per-install affiliate programs are now available which pay people to surreptitiously install malware on computer system.

- And, of course, miscreants want your personal information so they can take money from your bank account, use your credit card number, etc.

Security & The Internet2 Strategic Plan

- The Internet2 Strategic Plan includes "Task G:" "Develop and promote cost-effective methodologies, standards, and best practices for security and end-to-end application performance. Implementations must be possible under real-world conditions across campus, regional, national and international networks," see http://www.uoregon.edu/~joe/task-g/task-g.pdf
- As part of that process, and as mentioned in the Task G writeup, we've identified a number of security areas which Internet2 could work on; see the table at http://www.uoregon.edu/~joe/security-tasks.pdf
- **Item #2 on that table is "Malware"**
- But is malware *really* something that Internet2 should be worrying about? Is malware *really* "in scope?"

Narrow vs. Broad Scope of Work

- Some people may think that Internet2 security efforts should only be concerned about threats which use/target the network, things like
  -- high bandwidth DDoS attacks,
  -- BGP route injection and other attacks against the network control plane, or
  -- attacks against IP multicast, IPv6 and other advanced network protocols, etc.
- We have a slightly broader perspective. From our point of view, Internet2's security agenda properly includes
  -- **all material security threats to Internet2 sites (when viewed from an end-to-end perspective), including any cyber security threats which, if "mis-handled" could interfere with Internet2 network operations.**

People Do "Funny" Things To Try to Cope With Malware... And Unfortunately They Often Do Those "Funny" Things At The Network Layer!

- The network layer is an understandably attractive potential control point for managing cyber threats -- you can "handle" a problem once (at the network layer) rather than having to fix 1000's of individual systems.
- Unfortunately network-based cyber security solutions have the potential to cause an errosion of network transparency, causing what was once a clear pipe to now be encrusted with firewalls, anti-spam appliances, anti-malware appliances, peer-to-peer traffic shaping appliances, censorware web gateways, etc.
- That complexity can directly interfere with maintaining a fast, simple, and easy-to-diagnose-and-fix network.

Passive vs Active Middleboxes

- While we have no problem with passive intrusion detection systems such as Snort, Bro, etc., we have substantial concerns about network middleboxes which actively block or modify network traffic.
- We've talked about these concerns before, so rather than belaboring those issues here again, let's just briefly recap some issues with active security middleboxes:
  -- middleboxes may not be able to go fast enough, and may thus act as network throughput "choke points"
  -- middleboxes may (unintentionally) break legitimate traffic
  -- middleboxes may mask or hide compromised hosts, delaying or hindering remediation of those hosts
  -- middleboxes may complicate the diagnosis and and correction of non-security network problems

"But We Have To Fight Malware Somewhere!"

- If we're not going to fight malware on the network, we do need to fight it somewhere else (unless we just want to give up entirely!)
- The logical option is to fight malware on host systems (such as desktops and laptops, mail servers, etc.), even if that means dealing with many individual systems rather than one network. While this may seem laborious, doing so correctly recognizes that:
  -- we may not have visibility into all network traffic (e.g., some traffic will be encrypted end-to-end), and doing just traffic analysis of traffic sources and sinks may not be enough to spot all threats
  -- malware may also attack from non-network sources (such as tainted CDs or infected USB memory sticks)

Reconceptualizing Malware, Security and Privacy

Let's Step Back: What Is "Malware?"

- "Malware" is "malicious software" that's installed on a computer without the knowledge and informed consent of the computer's owner. It includes things like:
  -- viruses
  -- worms
  -- trojan horses
  -- bots
  -- root kits
  -- adware
  -- spyware
  -- scareware
  -- keyloggers
  -- dialers
- Differences between those types of malware don't really matter. What does matters is what malware does.

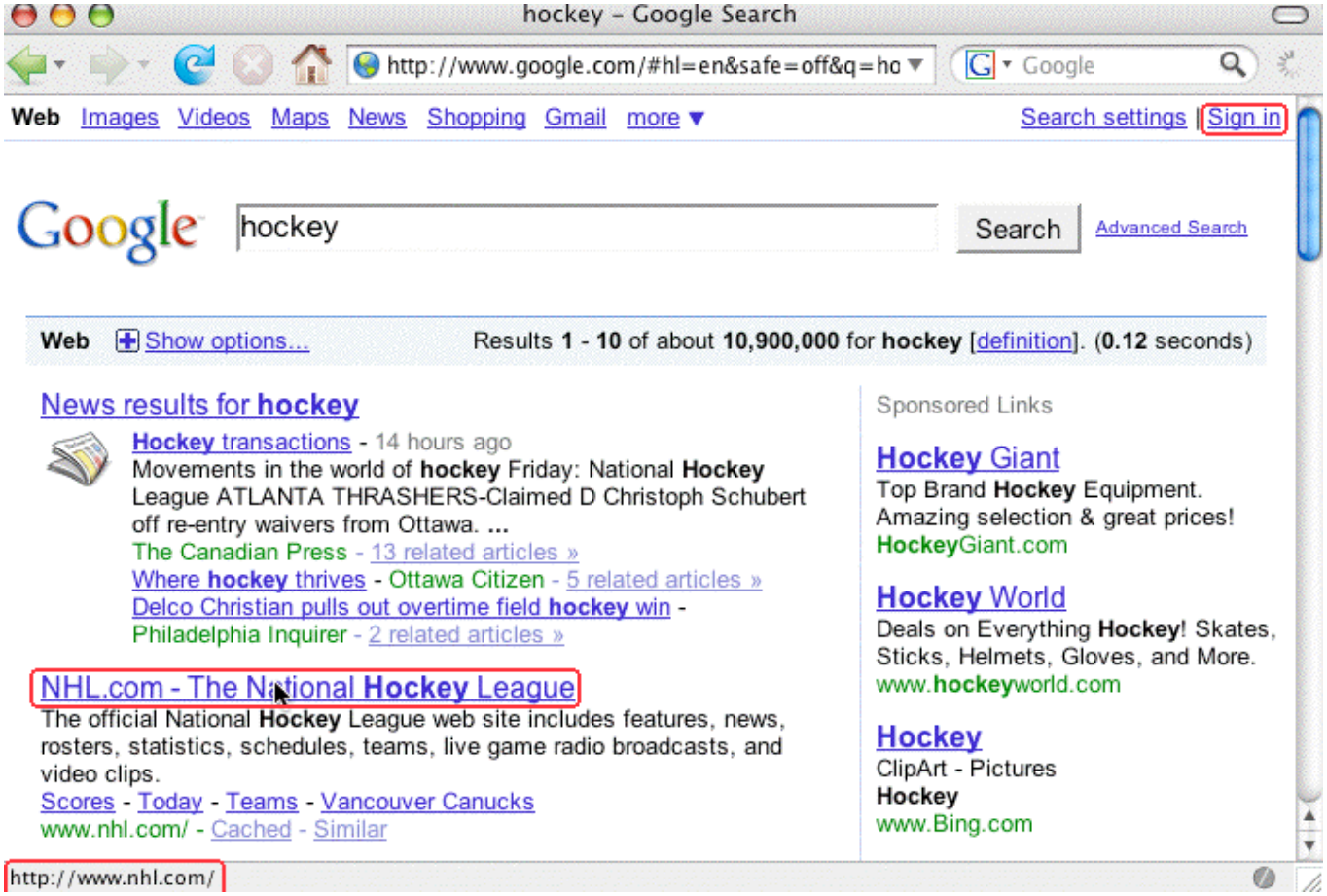
Some Specific Malicious Behaviors

- Not surprisingly, over time a variety of specific evil characteristics have been identified which make "malware" "malware"... See "General Criteria for Detection," www.mvps.org/winhelp2002/criteria.htm including (among 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
  - -- and there are many others hostile behaviors...

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 to even 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)

Example: Search Results for "Hockey"



Where do you go if you click on the www.nhl.com site?
It *looks* like you'd go to www.nhl.com, doesn't it?

BUT If You Right Click and Copy That Link 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." But, of course, most users do run with Javascript enabled...

Is This Behavior Fully Disclosed in the Google Privacy Policy?

- 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...

- Security and privacy are often closely intertwined
- Even premier online destinations routinely collect information about your behavior, and they'll even tell you that they're doing so, but **no one pays attention**
- Many times **you have the power to reduce disclosure of your private information** (e.g., in this case, you can do so by not using 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

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 a material source of concern.
- **Oh yes: and even though I've told you about this exposure, I bet you'll <u>still</u> keep on using Javascript!**

Cyber Security Is Something You Choose

- While we'll talk about a variety of technical issues relating to malware in the remainder of this talk, you should recognize that **in virtually every case, you have choices you can make which will reduce or eliminate your exposure. You can choose to be secure online -- if you want to be.**

- Being secure in a malware-rich environment may involve inconvenience, or forgoing some online services, or going through extra hassles.

- But we're all adults, and presumably we'll all make the choices that are best for our individual circumstances.

Avoiding Infection: Steps To Take On The Desktop Or Laptop

Job #1: Avoiding Infection

- One of our primary objectives is to stay away from malware, while still getting our work done, and if you're a cyber security professional, you want to achieve that same objective for your users.

- This may involve protective measures both on the desktop (or laptop), and on servers.

- Let's talk about steps to help avoid infection on the desktop first.

Choice of Operating System

- We know that virtually all malware targets PCs running some form of Microsoft Windows. Thus, the simple step of using something other than Microsoft Windows, like a Mac running OS X, can immediately make the majority of the malware that's in circulation largely irrelevant.
- By way of "eating our own dogfood," I would note that Internet2 itself has moved to the Mac for its staff
- However, we do know and understand that:
  -- There's still a huge existing installed base of PCs
  -- Macs may cost up to 2x what a similar PC might cost
  -- Some software which you might prefer to be able to use may only be available for Windows
- But what can you do if you don't have any choice about running on Windows?

At Least Run The Latest Version of Windows

- If you must run Windows, do your best to run the latest version of Windows.
- Currently there is a huge problem in that much of the Windows world is semi-stuck, running Windows XP rather than Windows Vista or Windows 7 when it is available (see http://www.microsoft.com/windows/windows-7/).
- Note that Windows XP Professional was first offered for general availability on 12/31/2001.* **Mainstream support ended 4/14/2009.** While extended support will be available through 04/08/2014, you should be planning how you'll get everyone off Windows XP now, rather than waiting until you've only got just a year or two left.

---

* http://support.microsoft.com/lifecycle/?LN=en-gb&C2=1173

A Free Thing: Don't Run As Administrator

- One simple (and free!) step that is often overlooked is to not use the Windows Aministrator account unless you are doing some task where you specifically need those privileges (such as when you're installing new software).

- By running from a regular account with lesser privileges, the damage that a rogue application can cause can, at least sometimes, be reduced or eliminated.

- There are sites which go into this concept in more depth, for example see http://nonadmin.editme.com/

Enable Data Execution Prevention (DEP)

- "Programs" (executable code) and "data" (used by programs) should always be strictly separate; programs should not be able to jump into/run code residing in "data" areas of memory. DEP enforces that restriction, and that restriction can keep (some) malware from executing (although it isn't a magic bullet).
- For more information, see:
  "A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003," http://support.microsoft.com/kb/875352
- Note that DEP "Opt-In" (contrary to what it sounds like) doesn't cover all programs, so if you want to go "whole hog" with DEP, adjust this to "Always On" (but that may keep some poorly-written programs from running)

Disable Auto-Run for Removable Media

- Windows computers can automatically run applications when removable media gets inserted. For example, a child's game might auto-run when the CD is inserted.
- Miscreants writing malware have exploited auto-run to automatically run malware residing on removable media, such as a USB memory stick, CD, etc.
- **You should generally disable auto-run on most PCs (or at least configure auto-run to require user confirmation)**
- For more information on this issue, see
  -- "Test your defenses against malicious USB flash drives" http://blogs.computerworld.com/test_your_defenses_against_malicious_usb_flash_drives [URL split due to length]
  -- "How to Disable the Autorun Functionality in Windows," http://support.microsoft.com/kb/967715

A/V: Site Licensed Desktop Antivirus Product

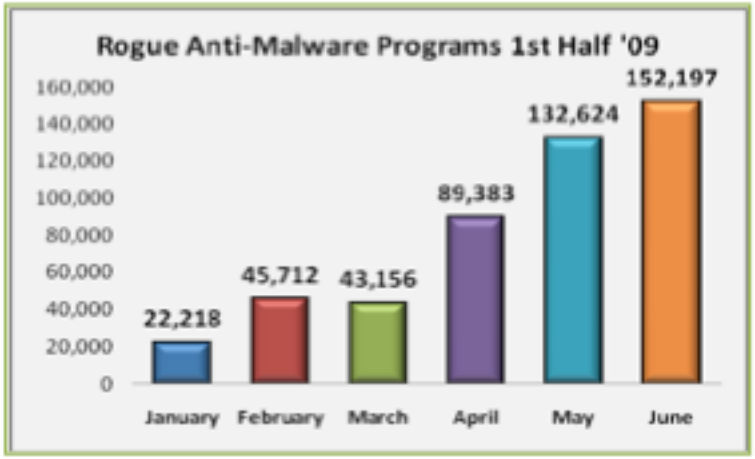
- We'll assume (as a given) that your site, like virtually all universities, site licenses some sort of commercial antivirus product for your desktops and laptop systems
- Things to look for when negotiating such a contract:
  -- work to get agreement that the licensed number of copies will by definition be sufficient for the entire campus community (avoid having to track copy-by-copy)
  -- insure that the product you license covers all malware threats (e.g., don't license just an antivirus product w/o the vendor's separate "anti-spyware" product!)
  -- insure you have coverage for work and home systems
  -- make sure you have a solution for PCs *and* Macs
  -- strive for a multi-year agreement; you really don't want to hassle around switching or renegotiating A/V products every year

Free Antivirus Products Also Have A Role

- Sometimes you may run into a person who may have an infected system (despite having an antivirus product installed), or someone who doesn't have any antivirus package at all. In those cases, it can be helpful to have a free antivirus product available, either for installation and routine use by the non-community member, or for a one-time "second opinion." Options available include:
  -- http://free.avg.com/
  -- http://www.kaspersky.com/virusscanner
  -- http://home.mcafee.com/downloads/freescan.aspx
  -- http://www.microsoft.com/Security_Essentials/
  -- http://security.symantec.com/
  -- http://housecall.trendmicro.com/
- Note: while you may be tempted to do so, do **not** install more than one antivirus product at a time.

Beware Rogue Anti-Malware Programs

- Be careful that users looking for free antivirus products do not accidentally download a rogue anti-malware program. Rogue anti-malware programs ("fake antivirus programs," "scareware," etc.) are malware which always find "infections" on your "PC" (even if you're running a Mac!), and are proliferating at a phenomenal rate:



www.antiphishing.org/reports/apwg_report_h1_2009.pdf

Some Antivirus FAQs

- **Q.** "What's the 'best' antivirus program to use?"
  A. That's hard to say because we know that cyber criminals will intentionally tweak malware prior to release to avoid particularly good and/or popular A/V products.
- **Q.** "If I scan all my email traffic on the server, do I still need to use a desktop antivirus product, too?"
  A. Yes, you do still need a desktop antivirus product because users may get malware via vectors other than your email server, e.g., via shared USB memory sticks, tainted web pages, instant messages, etc.
- **Q.** "I use a Mac. Do I <u>really</u> need an antivirus product?"
  A. While malware for the Mac is still rare, it does exist, and the malware environment could worsen overnight. You should run antivirus software on all your systems.

THE WEB: Which Web Browser Should I Use?

- Your choice of web browser can also have a material impact on your vulnerability to web-based malware.
- While many Windows users run Microsoft Internet Explorer by default (either because that's what came with their system or because a particular application, such as a campus ERP installation) requires it, alternatives are available which you should also consider.
- Some popular alternatives on Windows include:
  -- **Firefox** (http://www.mozilla.com/en-US/firefox/)
  -- Opera (http://www.opera.com/)
  -- Chrome (http://www.google.com/chrome)
- Whatever browser you use, you're generally best off running the **latest supported version** that's compatible with key campus software (such as your ERP system or your teaching and learning system).

Some Web Browser Vulnerability Stats

- **Internet Explorer 8.x**
  (http://secunia.com/advisories/product/21625/)
  12 vulnerabilities in 4 Secunia advisories, 50% (2 of 4) advisories unpatched as of October 3, 2009, most serious unpatched advisory is rated "Less critical"
- **Internet Explorer 7.x**
  (http://secunia.com/advisories/product/12366/)
  88 vulnerabilities in 38 Secunia advisories, 24% (9 of 38) advisories unpatched as of October 3, 2009, most serious unpatched advisory is rated "Moderately critical"
- **Internet Explorer 6.x**
  (http://secunia.com/advisories/product/11/)
  158 vulnerabilities in 139 Secunia advisories, 16% (22 of 139) advisories unpatched as of October 3, 2009, most serious unpatched advisory is rated "Moderately critical"

Some Web Browser Vulnerability Stats (2)

- **Firefox 3.5.x**
  (http://secunia.com/advisories/product/25800/)
  18 vulnerabilities in 4 Secunia advisories, 25% (1 of 4) advisories unpatched as of October 3, 2009, most serious unpatched advisory is rated "Not critical"
- **Opera 10.x**
  (http://secunia.com/advisories/product/26745/)
  0 vulnerabilities in 0 Secunia advisories
- **Google Chrome 3.x**
  (http://secunia.com/advisories/product/25720/)
  1 vulnerabilities in 1 Secunia advisories, no unpatched vulnerabilities as of October 3, 2009

Another Perspective on Browser Vulnerabilities

- One popular (estimated 80% of all documented security vulnerabilities in the 2nd half of 2007*) web attack vector is cross site scripting, where a specially crafted web page runs (or attempts to run) a script from another untrustworthy site. Browsers try, with varying levels of success, to prevent this from happening.
- An excellent resource: XSS (Cross site scripting) Cheat Sheet (see http://ha.ckers.org/xss.html) shows a variety of cross site scripting vulnerabilities, including which browsers are (and are not) vulnerable to each exploit.
- **There are lots of other things you can also do…**

---

* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

Disable Scripting in Your Browser

- Javascript and related scripting technologies in the browser can enable some amazing "Web 2.0" sites.
- However, browser scripting can also enable some show stopping vulnerabilities.
- Your best bet is to disable scripting entirely, if you can, but as we've previously mentioned that may be difficult or impossible to live with.
- If you can't disable scripting, consider running NoScript and disabling scripting everywhere except where you have no viable alternative.
- NoScript is available at http://noscript.net/
- **Really, if you do nothing else as a result of this talk, get scripting in your web browser under control!**

Pay Attention to PDF Helper Apps

- A popular malware attack vector is PDF files
- Virtually all systems have Acrobat Reader or another PDF rendering product installed, but often those applications may be vulnerable/not patched up-to-date since they aren't automatically updated via Microsoft Update, etc.
- Urge your users to check and upgrade Acrobat Reader if they aren't already up to date (to do this, while in Acrobat Reader, go to Help ==> Check for Updates Now)
- Another option you may want to consider may be trying a third party PDF viewer such as Foxit Reader (www.foxitsoftware.com), or Preview on Mac OS X.
- If you do ever get a suspicious PDF document, you can check it with Wepawet: http://wepawet.iseclab.org/ (if nothing's found, that does NOT mean the file's safe!)

If Possible, Don't Allow Flash

- Flash is another attack vector which has proven to be very popular with malware authors.
- Flash is virtually universally installed (just like PDF viewing software), but unlike PDF viewers, I'm not aware of any third party viewer options.
- Note that if you deinstall or disable Flash, you can't use YouTube (currently the 4th most popular site on the Internet), and many web sites also won't work (or at least many sites won't work well). Ugh.
- Like PDF files, suspicious Flash files can be analyzed with Wepawet, and some other SWF analysis tools are mentioned at: http://isc.sans.org/diary.html?storyid=2931
- Did you also know that Flash pages can store persistent cookie-like state? See tinyurl.com/check-flash-cookies

Remove Vulnerable Versions of Java

- Another vulnerability routinely exploited by malware targets outdated versions of Java.
- This vulnerability is particularly problematic because:
  -- Java is very widely installed
  -- When you update Java, old vulnerable versions of Java are **not** automatically removed from your system (you need to remove those manually, but few people do)
  -- Users may not recognize that different web browsers may use different versions of Java.
- To fix this issue, perform two key steps:
  -- Make sure you are running the latest version of Java: See www.java.com/en/ at the "Do I have Java?" link
  -- Remove any **old** versions of Java, as described at www.java.com/en/download/faq/remove_olderversions.xml

Check for Other Unpatched Apps/Problems

- Once you've dealt with the major categories of potential problems we've already mentioned, you may want to scan for additional applications which are installed but missing patches.
- An application that works well for this, and which is free for personal use, is Secunia's Personal Software Inspector (PSI), see http://secunia.com/vulnerability_scanning/personal/
- I also like Microsoft's Baseline Security Analyzer 2.1, see technet.microsoft.com/en-us/security/cc184923.aspx

Block Most Advertising Sites via DNS

- Advertising is another major potential vector for badness
- You don't need to view ads (no one ever says, "Gee, I know, let's go out and look at some commercials!")
- No, the sites you use **won't** stop running just because you don't view their ads (there are plenty of other less security aware people who will continue to do so for you)
- Some sites WILL break (e.g., there are some sites that pass clicks through an advertising site; for those, you'll need to learn how to extract the real URL you want)
- One resource listing some sites you may want to block via DNS: http://www.mvps.org/winhelp2002/hosts.htm
- Beware of making your local host file **too** huge, because in some cases that may slow down DNS resolution (the host file may be searched linearly, ugh)

An Example of The Problem With Ads…

Note to Readers

Published: September 13, 2009

Some NYTimes.com readers have seen a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software. We believe this was generated by an unauthorized advertisement and are working to prevent the problem from recurring. If you see such a warning, we suggest that you not click on it. Instead, quit and restart your Web browser. Questions and comments can be sent to webeditor@nytimes.com.

www.nytimes.com/2009/09/13/business/media/13note.html

EMAIL: Don't Send or Accept Attachments

- Another example of a "hard choice" which can dramatically reduce your exposure to malware is deciding to stop using attachments in email.
- **Note:** only accepting attachments from "people you know" isn't sufficient; people you know (or people pretending to be people you know) may send infected attachments too.
- It may help to think a bit about some reasons why people send attachments rather than plain text only:
  -- they may think formatted attachments look "more professional"
  -- they may not know how to create, save, and insert a plain text file into a mail message
  -- they may not know how to create and publish a web page and then just share that URL

Do We Need Back-to-the-Basics Education?

- Should we be offering basic remedial education for our users so they can learn to do simple online tasks we once took for granted, such as:
  -- creating and editing plain text files?
  -- creating simple web pages?
  -- securely moving files from a PC to a web server with scp or sftp?

  Those skills may represent vanishing skill, the cyber equivalent of folk skills from the "Foxfire" books!
- Do we also need to teach critical survival skills for users receiving online documents? Users need to understand that anyone can forge a message using digital "letter head," so trying to judge the legitimacy of a message by its appearance is pointless!

Don't Send or Accept HTML-formated Email

- HTML formatted mail can easily be used to infect your system with malware, while also enabling things like "web bugs" which can be used to spy on you. HTML formatted email is also a primary vector for phishing attacks (what you see as a textual link anchor ^= where the link goes)
- Make sure that **your** email program isn't sending HTML formatted email by default. Check your preferences!
- Discourage correspondents from sending HTML-formatted email to you (ask them to send you plain text email only)
- If you manage any mailing lists, ban it from all your lists (this is usually a configurable option)
- If you control email for an entire system or site, consider defanging dangerous email with Procmail Email Sanitizer (see the next section for more on PES).

Avoiding Infection:
On The Server

Scanning Server Traffic With An A/V Product

- Even if your users have a desktop antivirus product, you should also be scanning incoming email with a server-side antivirus product, too, for "protection in depth."

- To maximize malware detection, you may want to use two different antivirus products, one on the desktop and another on your servers. This will give you overlapping coverage footprints, so even if one A/V product misses a malware threat, the other product may catch it.

- For example, at the University of Oregon we use ClamAV, a free anti-virus product, on our servers, but McAfee on our desktops.

File Extension Attachments to Sanitize

- Another approach which can help avoid some malicious attachments is to block/"poison" executable attachments using a product like Procmail Email Sanitizer (see www.impsec.org/email-tools/procmail-security.html)
- While many computer users know that filenames ending in .exe or .com are (usually) executable programs, files with many other extensions may also represent executable programs including files ending in .ade, .adp, .app, .asd, .asp, .bas, .bat, .cer, .chm, .cil, .cmd, .cpl, .crt, .csh, .dll, .fxp, .hlp, .hta, .inf, .ins, .isp, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .msc, .msi, .msp, .mst, .nws, .ocx, .ops, .pcd, .pif, .prg, .pst, .reg, .scf, .scr, .sct, .shb, .shs, .tmp, .url, .vb, .vbe, .vbs, .vsmacros, .vss, .vst, .vsw, .wmf, .ws, .wsc, .wsf, and .wsh plus others

File Extension Attachments to Sanitize (2)

- Sites can decide to:
  -- quarantine (or drop outright) all messages with potentially dangerous executable file extensions
  -- delete all potentially dangerous attachments while delivering the rest of the message, perhaps with a note about the deleted attachment
  -- rename all files with potentially dangerous file extensions (e.g., by postpending .txt onto potentially dangerous executable file extensions)
- Sites also should decide what they want to do with .zip files and other archives. Should the zip file be unzippped and each of the resulting files scrutinized? Should zip files be blocked outright (like other dangerous file types)?
- Another policy choice: what about passworded zip files?

Don't Make It Impossible To Report Malware

- When blocking or otherwise managing potentially dangerous email content, be sure you exempt your site's abuse reporting addresses (abuse@, postmaster@, whois point of contact addresses, etc.) from that filtering.

- If you don't exempt those key addresses from malware-related filtering, you may make it impossible for people to report malware originating at your site!

Coping With Infections If/When They Do Occur

How Do You Know You're Infected?

- Most people become suspicious that they've become infected when their system begins to perform erratically, crash, pop up unexpected content, or loses net access.
- A better way to find issues with a system running Microsoft Windows is MyNetWatchman's SecCheck (see http://www.mynetwatchman.com/tools/sc/)
- Over time, SecCheck has accumulated a library of binaries that it has seen, and it now routinely tracks how often each of those binaries is seen.
- This strategy allows SecCheck to focus its attention on new or unusual programs or modules, disregarding the programs or modules that are common and well known.
- This is one of the best tools to use on a system which you suspect may be infected.

Monitoring Critical Files for Changes

- Another approach to detecting unwanted changes is through monitoring of critical files. In the Unix world, one of the more well known products of this sort is Tripwire, see http://www.tripwire.com/
- A product that may help you with this under Windows is WinPatrol 2009, see http://www.winpatrol.com/

Trusting An Infected Sytem To Inspect Itself

- Beyond a certain point, however, you need to understand that you really can't trust an infected system to monitor or inspect itself for infection -- one of the things malware may do is to intentionally interfere with your scans (malware of this sort is referred to as a "rootkit")
- Anti-rootkit tools are available, including:
  -- www.sophos.com/products/free-tools/sophos-anti-rootkit.html [URL split due to length]
  -- www.trendmicro.com/download/rbuster.asp
- If you suspect a system is infected and things like your normal antivirus program, SecCheck, or even rootkit detection and removal tools don't find anything, the next step is to remove the potentially infected hard drive(s) and mount/check them on another operating system.

What To Do If Your System Is Infected

- Sometimes, all best efforts to the contrary notwithstanding, a user will get infected with malware.
- The question then becomes, "What should (s)he do?"
- Wishful thinking may be, "Oh, I'll just remove the malware using one (or more) antivirus products."
- In many cases, however, it may **not** be possible to successfully remove all malware and return the system to a known-safe and stable configuration.
- Among security professionals, the expert advice is usually: **"nuke-and-pave."** That is, format the system and then reinstall the sytsem from scratch (or from a known-good backup).
- This generally correct advice may be hindered by a variety of factors, including a lack of system backups

What Should You Be Backing Up?

- If you end up with an infected system, a clean backup of critical files can be critical to your ability to recover.
- Increasingly large hard drives (e.g., 500GB and TB-class drives are now common) can make it awkward or time consuming for users to backup "everything."
- If you simply allow users to speculate about what they should be backing up, they will likely miss key files or back up other stuff they really don't need.
- Some commercial products (e.g., Norton 360) attempt to describe basic categories such as documents, pictures, music, video, email, contact info, financial files, and Internet favorites (but that may not be a complete list).
- Are you providing any backup-related recommendations to your users? If not, maybe you should be?

Some Additional Backup-Related Thoughts

- Backing up to a removable hard drive may be faster and more convenient than trying to back up to CD or DVD or tape, but be sure you don't get in the habbit of using (and reusing!) a single external hard drive for all your backups; you want to have multiple generations of backups available in case one backup hard drive fails or gets contaminated with infected files, etc.
- Would a network-based backup service for all campus servers, desktops and laptops be worth considering?
- Will all your backups be encrypted? if not, why not?
- You may want to clean up cached web pages and other temporary files before doing a backup. Ccleaner (see http://www.ccleaner.com) is one product which can help with that cleanup process.

Maybe You're Not Really Infected: Hoaxes

- Some of the "malware" you may hear about is not really malware
- A classic example of a "malware" hoax was the "jdbgmgr.exe" "warning" which urged people to find and remove jdbgmgr.exe from their computer. (That file is actually the Java Debug Manager used by Java coders) A nice summary of this hoax can be found online at http://www.snopes.com/computer/virus/jdbgmgr.asp
- Note that while the jdbgmgr.exe hoax didn't delete an essential system component, a malicious person might target something which is critical and whose removal might leave systems non-functional. Users should be taught to be skeptical of email virus warnings and should also be told to never participate in any chain letter!

Specific High Profile Malware
You May Have Been Hearing About

Before We Look At These Specific Examples

- Let me emphasize that this section is a "snapshot in time" and what's true now will likely be out of date in just a matter of weeks or months from now
- Rather than getting "stuck" on the details of any particular piece of malware, note the major themes these examples illustrate, including:
  -- the rise of malware targeting financial information
  -- spambots continue to be prominent
  -- spammers are exploiting new technologies right alongside users (e.g., Koobface's "Web 2.0" focus)
- We'll try to make this section less "dry"/"mind numbing" by including some "fun factoids" for at least some of these malware families (but don't let those "fun factoids" mislead you -- these are very serious threats)

Financial and Identity Theft Malware

Clampi

- Aka Ligats, Ilomo, Rscan
- Financial malware: steal banking credentials from SMBs
- www.secureworks.com/research/threats/clampi-trojan/
  "One of the largest and most professional thieving operations on the Internet"
- Interesting factoids (from http://www.symantec.com/security_response/writeup.jsp?docid=2008-011616-5036-99&tabid=2 [URL split due to length]):
  -- "When the Trojan is executed, it queries the locale of the compromised computer and exits if the country name begins with the letter "R". [Only three countries start with "R:" Romania, Russia Federation, and Rwanda];
  -- A list of domain names and IP addresses used by this malware threat are available from the Symantec page.

ESB claims Western Beaver was responsible for security breach

TEXT SIZE

By: Bob Bauder - Beaver County Times

Tuesday September 22, 2009 08:04 PM

BEAVER — An Ellwood City bank contends that Western Beaver School District is responsible for a computer security breach that permitted a hacker to siphon more than $700,000 from district accounts over the Christmas break last year.

Western Beaver has sued ESB Bank for the return of nearly $450,000, the amount that remains missing.

According to the suit, someone infected the school's computer system with a virus, triggering 72 electronic fund transfers from Western Beaver's tax and general fund accounts managed by ESB. A total of $704,610 was transferred from Dec. 29 through Jan. 5 into bank accounts of 42 individuals from California to Puerto Rico.

The FBI is investigating, but did not return a phone call on Tuesday from The Times.

The bank was able to reverse transfers totaling $263,413, leaving Western Beaver at a loss for $441,197.

Western Beaver has sued, asking Beaver County Court to enter a judgment against ESB for the outstanding amount.

In recent court filings, ESB claims that contracts with Western Beaver guarantee the bank indemnity against losses suffered by the school district through unauthorized fund transfers. It contends the district is responsible for such transfers.

The bank says the virus infected Western Beaver's computer system, an indication that the district failed to comply with security procedures outlined in the contracts.

Zeus (Zbot)

- Aka Zbot, WSNPOEM, NTOS, PRG
- Zeus is financial malware, stealing banking credentials and potentially modifying HTML content so as to be able to actively request additional confidential information
- Widely undetected by antivirus products (see http://www.trusteer.com/files/Zeus_and_Antivirus.pdf)
- Has been seen in conjunction with email claiming to be from the "IRS:" http://garwarner.blogspot.com/2009/09/irs-version-of-zeus-bot-continues.html
- Blocklist of Zeus domains and IPs: https://zeustracker.abuse.ch/blocklist.php
- "Fun factoid" (from http://www.abuse.ch/?p=1327): This malware includes a "kos" command ("kill OS"), oh great... :-(

Koobface

- "Largest Web 2.0 botnet" ("The Real Face of Koobface," http://blog.trendmicro.com/the-real-face-of-koobface/) with variants targeting Facebook, Myspace, Twitter, and other "Web 2.0" sites.
- "When it comes to information harvesting and financial and identity theft, the most dangerous botnets were Koobface, Zeus and Clampi." www.itpro.co.uk/615364/infected-computers-compromised-for-300-days
- The Koobface payload is adaptive and can be tailored in real time, including ad delivery components, fake AV components, Captcha breakers, data stealing malware, DNS changers, search hijackers, click fraudware, etc.
- "Fun factoid:" "Koobface" is an anagram/jumble for "Facebook"

Spambot Malware

Grum

- "[...] the most active botnet in terms of spam distribution is now the little-known botnet, Grum. Both Grum and another botnet called Bobax have overtaken Cutwail as the most active spam-sending botnets, currently responsible for 23.2% and 15.7% of all spam respectively." See http://www.symantec.com/connect/blogs/evaluating-botnet-capacity

Rustock

- Spambot and rootkit. Estimates as of Sept. 29th, 2009 are that it is 1.3-1.9 million bots in size (see http://www.messagelabs.com/resources/press/38345), largest of all [spam?] bots according to Messagelabs.
- Responsible for 35% of spam as of March 5th, 2009 (m86security.com/TRACE/traceitem.asp?article=882)
- Rustock was closely studied by researchers:
  -- Kaspersky: "Rustock and All That," http://www.viruslist.com/en/analysis?pubid=204792011
  -- Sandia: "Case Study of the Rustock Rootkit and Spam Bot," http://www.usenix.org/event/hotbots07/tech/full_papers/chiang/chiang_html/
- "Fun factoid:" Rustock apparently only works from Midnight to 4PM Pacific time according to Messagelabs.

Cutwail

- Aka Pushdo or Pandex. Spambot, malware dropper, etc. Spam campaigns include "Canadian Pharmacy" spam.
- 39 pp. writeup at "A Study of the Pushdo / Cutwail Botnet," http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/pushdo-external.pdf :

  > "While it does not grab as many headlines as its attention-seeking peers such as Storm or Conficker, according to recent reports it is the 2nd largest SPAM botnet on the planet - sending approximately 7.7 Billion emails per day"

- Recently associated with fake IRS letters using dot eu domains (see http://blogs.zdnet.com/security/?p=4260)

Xarvester

- Spambot capable of 600K spam/day/bot although usual delivery rates may be lower; nice analysis at m86security.com/trace/i/Xarvester,spambot.886~.asp

- www.secureworks.com/research/threats/botnets2009/?threat=botnets2009 describes Xarvester as "one of the top spamming botnets, sending pitches for pharmaceuticals, diploma mills, replica watches and a fair amount of Russian-language spam"

Mega-D (Ozdok)

- "Mega-D accounts for 32% of spam," [at that time] www.m86security.com/TRACE/traceitem.asp?article=510 : "The spam is almost always promoting male enlargement pills, and several brand names are used including MaxHerbal, Express Herbals, **Herbal King**, and VPXL."
- "FTC Shuts Down, Freezes Assets of Vast International Spam E-Mail Network," October 14th, 2008, http://www.ftc.gov/opa/2008/10/**herbalkings**.shtm
- June 2009: Mega-D now responsible for 9.3% of all spam, see http://www.messagelabs.com/mlireport/MLIReport_2009.06_June_FINAL.pdf at page 1
- "Fun factoid:" Ozdok would secretly grab screenshots (http://www.secureworks.com/research/blog/index.php/2009/01/20/ozdok-watching-the-watchers/)

Waledac

- Spambot (with additional capabilities) known to have spammed for "Canadian Pharmacy" and other pillz sites.

- Uses encrypted peer-to-peer command and control technology, and fast-flux hosting. Fond of mailing around holiday times with holiday themed spam.

- Excellent 67 page writeup entitled, "Infiltrating the WALEDAC Botnet," June 2009, available at us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/infiltrating_the_waledac_botnet_v2.pdf

Donbot

- Aka Buzus, Bachsoy. Spambot.
- "[...] in August [2009], another prolific botnet called Donbot continued to use shortened URLs in its spam runs, peaking at distributing ten billion emails in just one day." [www.marketwire.com/press-release/Messagelabs-Now-Part-Of-Symantec-NASDAQ-SYMC-1035112.html]
- Nice writeup at www.m86security.com/trace/i/Donbot,spambot.899~.asp mentioning

  > "Donbot concentrates mainly on pharmaceutical spam, but has also been observed sending material relating to replica watches and adult dating."

- Fun factoid: "Donbot" is called that because of the string "Don" in the malware

Other Notable Malware

Conficker/Downadup

- Not yet clear what this malware will ultimately be used for -- but it is important simply because of its level of penetration -- http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking shows over 5-6 million unique infected IP's each day.
- Excellent writeups from SRI and CAIDA are available at mtc.sri.com/Conficker/addendumC/index.html and www.caida.org/research/security/ms08-067/conficker.xml
- "Fun factoids" for Conficker: (1) "Microsoft has announced a US$250,000 reward for information that results in the arrest and conviction of those responsible for illegally launching the Conficker worm. [...] Microsoft [...] Reward Hotline, 1-425-706-1111, [...] avreward@microsoft.com" and (2) Conficker-A wouldn't infect hosts using Ukranian keyboards.

Taterf

- Worm.
- Taterf spreads via mapped drives, and captures Internet gaming credentials for World of Warcraft plus a variety of games popular in East Asian countries.
- #1 on Microsoft's list of the ten most prevalent malware samples spotted during August 2009, accounting for over half a million malicious threats during the month. [see http://blogs.technet.com/mmpc/archive/2009/08/27/msrt-august-top-detection-reports.aspx].
- Earlier, in 2008, Microsoft reported removing Taterf from 1,269,098 distinct machines during just one week [see http://blogs.technet.com/mmpc/archive/2008/06/20/taterf-all-your-drives-are-belong-to-me-1-one.aspx]

Some Malware-Related Tools and Resources

Site Advisor

- Site Advisor is a McAfee product that reviews web sites for potential threats.

- Wonderful resource if you have a colleague or family member who's always asking, "I'm tempted to try website <foo>. Do you think it's safe for me to do so?"

- Site Advisor also accepts "nominations" for sites you're curious about, but which it may not have yet visited.

Sample SiteAdvisor Report

internet2.edu | McAfee SiteAdvisor Software - Website Safety Ratings and Secure Search

http://www.siteadvisor.com/sites/internet2.edu

Google

internet2.edu

Advertisement

We tested this site and didn't find any significant problems.

Are you the owner of this site? Leave a comment

Contact information: | Country: United States | Popularity: Many users

AUTOMATED WEB SAFETY TESTING RESULTS FOR INTERNET2.EDU

E-MAIL TESTS FOR INTERNET2.EDU:

DOWNLOAD TESTS FOR INTERNET2.EDU:

19 green downloads

In our tests, we found downloads on this site were free of adware, spyware, and other potentially unwanted programs.

View detailed analysis

Submit a download for analysis

Downloads we found on this site:

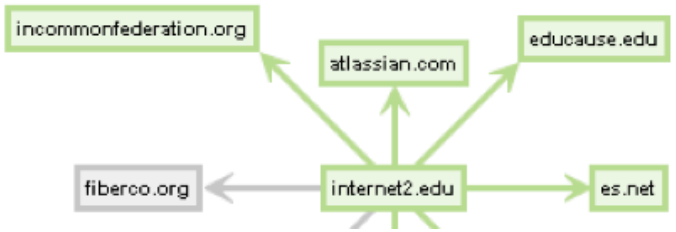
Download	Analysis
msorun.cab	
Windows-web100clt.zip	
detective3.1-mswin.zip	
perfSONAR-1.0.jar	
signet-1.0-bin.zip	

19 total downloads. See more.

ONLINE AFFILIATIONS FOR INTERNET2.EDU:

Linked to green sites

When we visited this site, we found that most of its links are to sites which are safe or have only minor safety/annoyance



Google Safebrowsing Site Diagnostic Report

- Another site reputation review site is Google's Safe Browsing project.

- For an example of what they think of uoregon.edu or our ASN (3582), see:

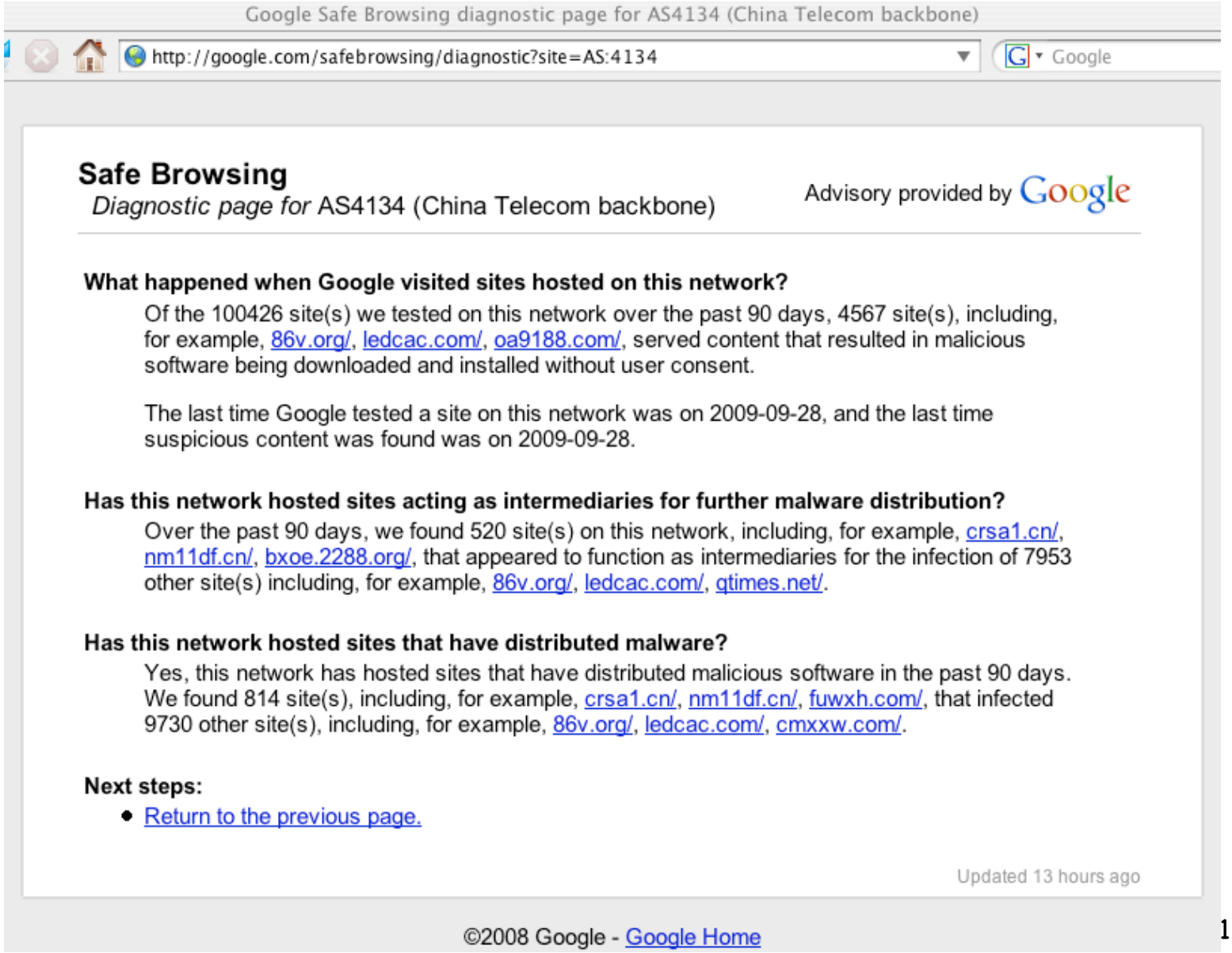
  -- google.com/safebrowsing/diagnostic?site=uoregon.edu

  -- google.com/safebrowsing/diagnostic?site=AS:3582

  or substitute your own domain or ASN.

- For more information about the data used to drive these reputation summaries, see "All Your iFRAMEs Point to Us," Google Technical Report provos-2008a, http://research.google.com/archive/provos-2008a.pdf

Google Safebrowsing Report for AS4134



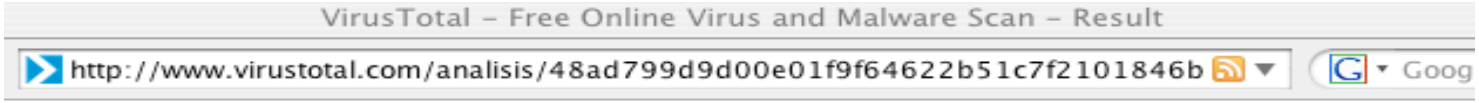
Virustotal

- Virustotal is a wonderful resource if you have a suspicious executable and you'd like to know how a variety of antivirus products think about that file.

- By submitting a file to Virustotal, you can get a report for virtually all common antivirus products, and you can also help fight malware (submitted files are shared with antivirus vendors)

- In addition to antivirus reports, you'll also get the file's MD5 checksum, SHA1 and SHA256 checksums, and other valuable information about your submission.

Sample (partial) Virustotal Output



File **postcard.exe** received on **2009.10.05 04:09:29 (UTC)**
Current status: **finished**
Result: **33/41 (80.49%)**

Compact Print results

Antivirus	Version	Last Update	Result
a-squared	4.5.0.24	2009.10.05	-
AhnLab-V3	5.0.0.2	2009.10.03	mIRC/Zapchast
AntiVir	7.9.1.33	2009.10.05	TR/Dropper.Gen
Antiy-AVL	2.0.3.7	2009.10.05	Backdoor/IRC.Zapchast
Authentium	5.1.2.4	2009.10.04	REG/Zapchast.H
Avast	4.8.1351.0	2009.10.04	VBS:Malware-gen
AVG	8.5.0.420	2009.10.04	Zapchast
BitDefender	7.2	2009.10.05	Backdoor.Zapchast.PF
CAT-QuickHeal	10.00	2009.10.03	-
ClamAV	0.94.1	2009.10.03	Trojan.IRC.Zapchast-16
Comodo	2515	2009.10.05	Backdoor.Win32.mIRC-based
DrWeb	5.0.0.12182	2009.10.05	-
eSafe	7.0.17.0	2009.10.04	Win32.mIRC-based
eTrust-Vet	31.6.6774	2009.10.02	-
F-Prot	4.5.1.85	2009.10.04	REG/Zapchast.H

Sandboxes

- "Sandboxes" are controlled environments where malware can safely be run in an instrumented environment for analysis.
- Three popular malware sandboxes are:

  -- Anubis (Analyzing Unknown Binaries)
  http://anubis.iseclab.org/

  -- CWSandbox
  http://www.sunbeltsecurity.com

  -- Threat Expert
  http://www.threatexpert.com/

hosts-file.net

- Strangely enough, some times you may want to know the neighborhoods where malware can be found on the web. If that's the case for you, you may be interested in the Ur I.T. Mate Group hpHosts RSS feed. See: http://hosts-file.net/rss.asp

- For information about what the various hosts-file,net classifications mean, see the decoder sheet at http://hosts-file.net/?s=policy

What's Next? One Emerging Trend: The Automated Abuse of Websites

You're Probably Helping Spammers Right Now, Without Knowing It

- Since spammers no longer have much luck with email, they've turned to the web, where defenses are weaker.
- When you get a minute, Google your web site for commonly spammed products or services; in many cases you may be surprised by what you find. Example Google search:

  hydrocodone no prescription site:edu

  (or you can be more specific by specifying your top level domain instead of just "edu")

- This web defacement is occurring via automated tools

The Big Guys Are Being Killed By This Too...

- Miscreants are freely distributing software products which are designed to automate the creation of free web email accounts at major providers, including products (or inexpensive services) which defeat Captchas.
- Those mass-produced accounts are then used to send spam, including plenty of 419 (advance fee fraud) spam.
- This is one of the fastest growing sort of abuse out there...

What Should You Be Doing to Counter This?

- Patch your wikis, blogs, guestbooks and other web apps!
- Watch for abuse of pages at your web site; Google and other search engines are key to spotting malicious pages.
- Scan your systems for strangely named files. "Dot directories" on Unix systems in strange places are one example of a sort of "strangely named" file or directory you should be paying attention to
- Consider eliminating anonymously writable pages such as guestbooks, or at least supress the display of comments until they've been approved by a moderator/reviewer.
- Be aware that some web pages may be scripted to return an innocuous page to you, but completely different content to remote viewers or to search engines. Check suspicious files directly via the file system, not via http.

Thanks For The Chance To Talk Today!

- Are there any questions?