



The Evolving Malware Threat:

Guarding Against Criminal Malware

Roger A. Grimes, InfoWorld security columnist/Microsoft Sr. Computer Consultant

June 26, 2007

Old Malware Model

Historic Hacking and Malware Trends

- From 1999 to late 2006, about 90% of malware attacks arrived via email
 - Malicious file attachments
 - Rogue embedded links
 - Spam
 - Ad-ware
 - MIME-type mismatches
 - Social-engineering methods

Current Malware Landscape

New Malware Model

- Bots
- Professionally written
 - Development forks, teams
- Client-side Attacks
- Criminally-motivated
- Designed To Get Money
 - Steal passwords, identity info
 - DDoS attacks

Current Malware Landscape

New Malware Model (con't)

- Self-healing bot nets
- Intended to live only a few hours
- Auto-updating, Design To Hide
- Infects users through (mostly innocent) infected web site
 - Infected site
 - Banner advertisements
 - Borrowed code

Current Malware Landscape

Today's Bots and Malware

- Message Labs reports 10 completely new bot programs detected a day
- Google detected 200,000 new unique malicious executables in 1 year
- Most malware programs are “packed”
 - A large percentage (25%-60%) of all new malware programs are going past scanners undetected

Current Malware Landscape

Attack Methods

- Client-side attacks still very prevalent on Windows
 - In most cases, spreads because end-user interacts with malicious link, web site, program, or file attachment
 - Usually unpatched apps or OS
 - High percentage of W2K, XP SP1
 - Growing number of zero days

Current Malware Landscape

Today

- **Millions of PCs “owned” on the Internet**
- **For the most part, we aren’t doing much to stop them**
- **We aren’t catching many of the criminals**
- **End-user education is harder than it first appears**
- **Users/admins not doing the simple things they should be doing to stop malicious attacks**
- **Attackers don’t need complex, hypervisor attacks to do damage; current attacks doing just fine**

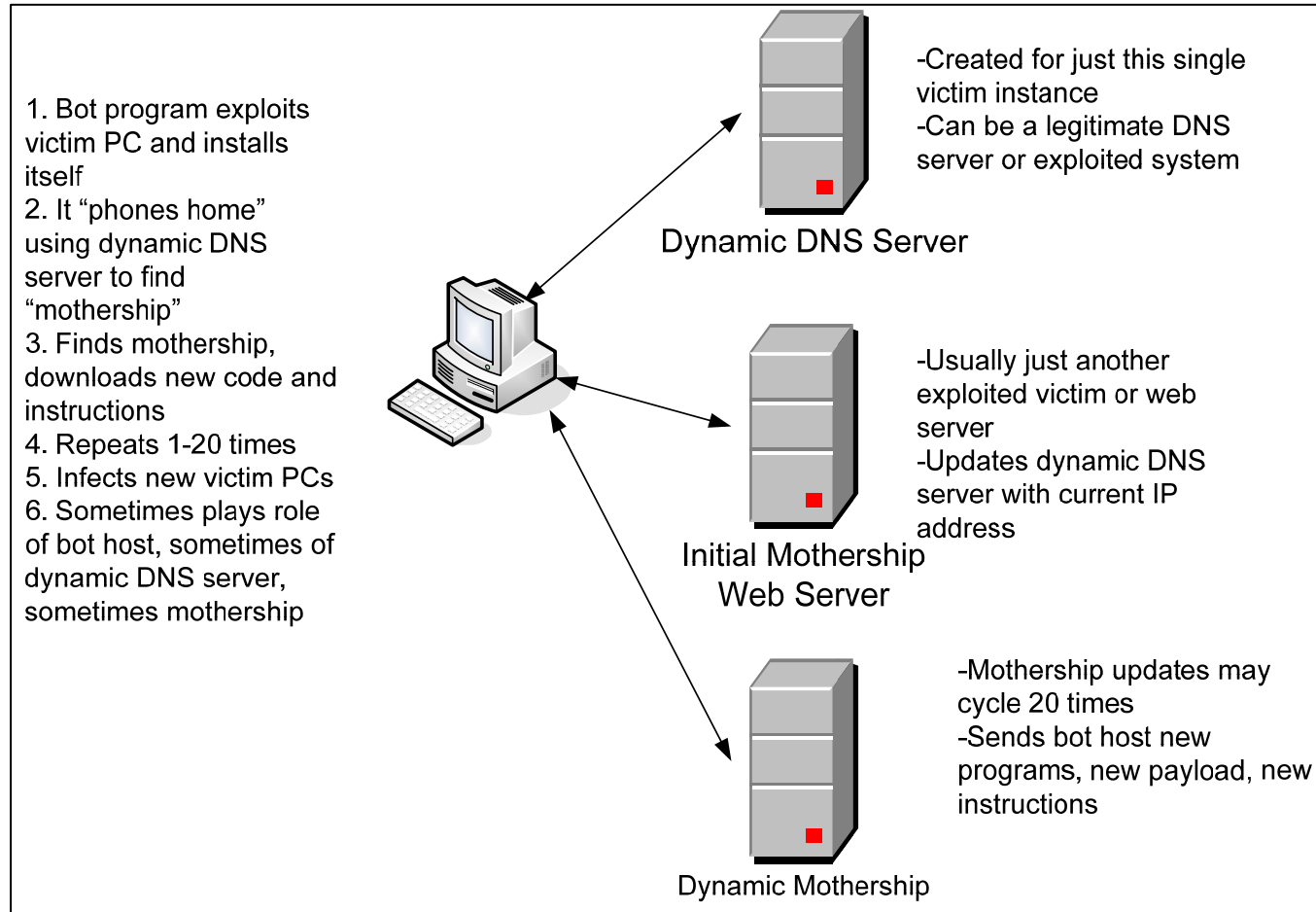
Current Malware Landscape

New Malware Model Steps

1. Infect or Exploit
2. Modify system to gain control
3. Phone “home” to get code update
Repeat this step 1-20 times
4. Modify host and spread to create bot net
5. Steal information-financial, passwords, etc.
6. Able to bypass any authentication method
7. When finished, self-delete, cover up tracks

Current Malware Landscape

New Malware Model Steps



Current Malware Landscape

Initial Activation

- Infected web site
- App-based Social Engineering
 - File Attachment
 - Trojan Installation
 - Embedded URL Link
 - Malformed Media Content
- Buffer Overflow
- Boot Code or Auto-Run Modification

Current Malware Landscape

Infection or Exploit

- “Zero-day” exploits becoming more common
- One attack program can have 20 exploit vectors
- DNS tricks
 - Poisoning, hosts file manipulation
 - Sound-alikes

Current Malware Landscape

Bot Nets

- Many commercial bot net kits
 - 24 x 7 tech support
 - Bypass any authentication
 - Made to order
- To defeat bot nets, defenders must find and take down C&C servers or disrupt their communication channels (e.g. IRC)

Current Malware Landscape

Bot Nets-”Spam-Thrus”

- Bot net creators have made “self-healing” C&C nets
- C&C servers monitor each other in a port 80/443 peer-to-peer network
- Uses “keep-alive” packets
 - If keep-alive packet isn’t rec’d, peer notifies other peers, and bots are instantly updated
 - Single bot allows entire C&C structure to be rebuilt
- Roving, rarely staying one place longer than a few hours

Current Malware Landscape

Web Attacker Toolkit

- User visits compromised, legitimate, web site and gets bot/trojan infected
- Perl-based CGI script
 - PHP launched, obfuscated JavaScript
- Web Attacker is a program that can be downloaded from Russia for as little as \$15
 - \$300 for ultra edition
 - \$25 extra gets you 24 x 7 tech support
- Currently, responsible for 30% to 80% of all client-side attacks

Current Malware Landscape

Web Attacker Toolkit

- GUI-based, and good documentation
- Updated frequently with latest zero-day and known exploits
- Updated to evade detection
- Detects visiting user's browser and infects them with one of a few dozen exploits
 - Infects both IE and Firefox
- Been out about 2 years now

Current Malware Landscape

Web Attacker Toolkit

- Point-n-Click GUI Configs



Current Malware Landscape

Web Attacker Toolkit

- Infected web sites often host GUI statistics
- Infected hosted will have a remote, password-protected control panel page for owner to use
- Report break down by:
 - Type of exploits used successfully
 - Visitor OS
 - Visitor Browser

Current Malware Landscape

Web 2.0 Malware Example

Mespam Trojan

- Initially spread by Stormworm/Peacomm botnet
- Injects itself into Windows as a Layered Service Provider (LSP)
- When infected user post web content (e.g. blog comments, web-based mail, etc.),
- Trojan injects malicious links into any outgoing HTML-network packet
- User and antivirus program has no idea
- Indexed and showing up on search sites within minutes

Current Malware Landscape

Bank Stealing Trojans

- Infects client through normal means, then waits for user to authenticate to financial web site
 - Bank, ebay, egold, etc.
- Then launches a hidden browser session and steals all the money
 - Except leaves enough so that “close your account?” wizards aren’t set off.
 - Changes your email address and mailing address

Current Malware Landscape

Bank Stealing Trojans

- Cannot be stopped by any in-band authentication (e.g. SSL, smart cards, two-factor authentication, etc.)
- It is a “man-in-the-end-node” attack
- Doesn't steal passwords or logon information because it already has all your money
- Be around for about 3 years

Current Malware Landscape

Web-based Malware Report

- *May 2007-The Ghost In The Browser Analysis of Web-based Malware*
- Based on searching for malicious links in over 7 billion web pages over 12 months (ending March 2007)
- Found 450,000 infected web pages
 - 0.06% hit rate
 - Included many popular web sites

Current Malware Landscape

McAfee Web Report

- May 2007 analysis
- (www.siteadvisor.com/studies/search_safety_may_2007.html)
- Found that 4% of returned web links from an Internet search engine query contain malware or risky mechanisms (many in sponsored links)
- 0.03% returned attack malware
- AOL returned the safest web pages
- Yahoo returned the most risk
- 20% of the web results from searches for digital music and tech toys returned risky sites

Current Malware Landscape

Web-based Malware Report

Web sites were infected 1 of 5 ways:

- Poor web site security
- Vulnerable applications (e.g. PHP, CGI, ASP, SQL, etc.)
- User contributed content (e.g. cross site scripting)
- Malicious advertising inclusion
- Malicious third-party software component (i.e. widget) inclusion

Current Malware Landscape

Web-based Malware Report

Malicious Advertising

- Many web sites are being paid to include roving advertising banners and pop-ups.
- While these services are often maintained by legitimate, respected, web advertisers, the actual ad content is often sub contracted to a sub contractor of a subcontractor. E
- The top level owner has no idea that their legitimate advertising banner service has been co-opted by malware criminals.

Current Malware Landscape

Web-based Malware Report

User Contributed Content

- Many web sites, especially blogs, allow users to contribute content
- If web site's software is not appropriately configured, will allow cross-site scripting exploits
 - Malicious person posts a malicious Javascript instead of text
 - Readers then execute Javascript

Current Malware Landscape

Web-based Malware Report

User Contributed Content (con't)

- Attackers, of course, have automated programs that check for vulnerable web sites and blogs
- When the automated program finds a vulnerable site, it posts 1 to more than a 1000 malicious scripts

Current Malware Landscape

Web-based Malware Report

Malicious Widgets

- Many web sites borrow free widgets (e.g. traffic counter), and for months or years, the widget functions just as intended.
 - The widget code is often hosted on another external server.
 - But at a later date the “free” widget code is maliciously manipulated to inject malware links.
- It appears in many cases, the bad guys are giving away free widgets and encouraging widespread adoption so they can use them as infection vectors later on.

Current Malware Landscape

Web-based Malware Report

Misc

- Some infected web sites install up to 50 malicious programs from a single visit
 - Good luck in cleaning that one up
- Many malware programs were 2X or 3X obfuscated, bypassing most AV and IDS detectors
- One URL handed over 1,100 binaries
- Report concludes, “... that a large fraction of computer users is exposed to web-based malware every day

Current Malware Landscape

Web-based Malware Report

Not All Web Sites Are Innocent

- Web sites are often paid to look the other way
- www.iframe.money.org offers web sites \$7 per 10,000 unique views
- 33% of the over 8000 web sites that 9 IPOWER web servers host contain malware, for years
 - Bad case of neglect or something else?

Current Malware Landscape

Malware Is Hiding Better

- Traditional Anti-virus scanning is becoming less accurate
- So much malware coming out each hour
- Most of it is “morphed” or obfuscated copies of existing malware
 - Still, the trick is working
- Many studies report AV detection rates under 25% for daily malware

Current Malware Landscape

Malware Is Hiding Better

Known Malware Detection Rates Not Bad

www.av-test.org study (May 2007)

- 29 AV engines run against 606,901 known current (last 12 months) malware files
- Average detection rate was 87%
 - Low detection rate was 62%
 - High detection rate was 99.83%

Current Malware Landscape

New Malware Is Hiding Even Better

www.av-comparatives.org study

- Test 20 scanners in heuristics mode against 20,000+ previously unknown malware samples
- Heuristic accuracy ranged from 8% to 71%
- Three AV products were around 70%
- 2/3rds of AV products detected at 30% or less

VirusTotal (www.virustotal.com) Detection Failures

- 96% of submitted malware samples were missed by one or more AV engines
- Only 4% of submitted samples were detected by all AV engines

Current Malware Landscape

Malware Is Hiding Better

How Does Malware Hide?

Early Techniques:

- Encrypted – hide the malware so it can't be scanned
- Oligomorphic- multi. encryption/decryption engines
- Polymorphic- random encryption/decryption
- Metamorphic- mutates malware body, looks for compiler on host and re-compiles malware on-the-fly

Current Malware Landscape

New Malware Is Hiding Even Better

How Does Malware Hide?

Today's Techniques:

- HTML Encoding/Obfuscation
- Character set (e.g. UTF-8, UTF-7, Unicode) encoding
- Compression (e.g. multi-compressed zip files)
- Packers, Multi-packers
- SSL/TLS/encryption for travel and communications

Current Malware Landscape

New Malware Is Hiding Even Better

How Does Malware Hide?

Today's Techniques:

- Language encoding (e.g. simplified Chinese)
- Transfer encoding (e.g. *chunked*, *token-extension*)
- Packet fragmentation, time-outs
- Password protected files
- Embedded code (e.g. RTF links)
- Embedded in thick content (e.g. Flash objects)

Current Malware Landscape

New Malware Is Hiding Even Better

How Does Malware Hide?

Today's Techniques:

- Dynamic DNS names
- Dynamic IP addressing
- One-time URLs (unique per victim)
- Self-deleting malware
- Delete and come back when needed

Current Malware Landscape

New Malware Is Hiding Even Better

How Does Malware Hide?

Today's Techniques:

- ***Exploit morph engines*** (“on-the-fly” creations, unique per user)
 - Changes exploit
 - Changes obscurity mechanism
 - Changes shell code
 - Changes script components
 - Delivered malware will never exist again

Current Malware Landscape

New Malware Is Hiding Even Better

Complicating AV Vendors Lives

- Malware designed to not work in VMs
- Malware downloads blocked by IP address and domain name (e.g. never to MS domains)
- Time-based approaches (e.g. malware only available for 10 minutes every two days)
- Use of invisible HTML
 - Real user would never click on it, only automated honeyclient

Current Malware Landscape

Forming a Defense

Lessons To Take Away

- Malware is trending away from malicious emails to innocently infected web sites
 - Visiting only “trusted” web sites still good advice, but users need to be aware
- You need to make sure all client OS and applications are patched (and not just the OS)
- Consider investing more in technologies that can mitigate these types of threats
- Educate end users about the evolving malware threat

Current Malware Landscape

Forming a Defense

Best End-User Defenses

- Don't be logged in as Administrator all the time
- Be fully patched-OS and applications
 - Check yourself, www.secunia.com, Software Inspector
- Convert incoming email to plain-text
- Use strong passwords (8 char. or longer)
- Don't click on things you shouldn't

Current Malware Landscape

Forming a Defense

Best Web Commerce Defenses

- Secure your web site
- Check for and close any hidden browser sessions (tell user no other browser session allowed)
- Monitor back-end transactions for malicious behavior
 - Like VISA and Mastercard do
 - Let users determine the threshold of “pain”
- Send clean VM to end-user

Current Malware Landscape

Forming a Defense

Best Web Commerce Defenses (con't)

- Change the post-successful-logon page URL time to time (and put anti-malware warnings in its place)
- Don't allow end-user to change email address or mailing address without confirmation to original location or verified call to customer support
- Don't allow large transactions to strange locations without additional verification

Current Malware Landscape

Questions

- e: rogrim@microsoft.com