Lessons from a Zero-Day: The WMF Episode

Jim Voorhees

Windows Metafile Format Vulnerability

- December 2005, blindsided the defense community
- Spawned great controversy, everyone talked about it, but there was no consensus
- As a community we felt helpless, no one had answers

WMF Vulnerability

- 16-bit format for storing vector graphics released in December 1987
- At least 14 WMF functions had vulnerabilities; most likely, not all are fixed today
- The 32-bit Enhanced Metafile Format has replaced WMF
- Problem in December 2005 was with a deprecated subfunction in a superceded format

The Beginning

- Discovered early in December in Russia, Lithuania, or Poland
- Exploits used for ‘Pump and dump’ stock schemes, etc.
- H.D. Moore said it was discussed in the ‘underground’ before we found out about it

Discovery

- Websense and Sunbelt Software found the exploit code early and began to work with Microsoft
- Most people learned about it on December 27 through an email sent to Bugtraq:

```
From: <noemailpls at noemail.ziper>
Date: 27 Dec 2005 20:20:14 -0000

('binary' encoding is not supported, stored as-is) Warning
the following URL successfully exploited a fully patched
windows xp system with a freshly updated norton anti virus.

unionseek.com/d/t1/wmf_exp.htm

The url runs a .wmf and executes the virus, f-secure will
pick up the virus norton will not. (Noemailpls, 2005).
```

And Then...?

Tue.	27 Dec.	Vulnerability and exploits discovered. Microsoft begins SSIRP.
Wed.	28 Dec.	Metasploit module available. Microsoft issues Advisory
Thu	29 Dec.	---
Fri	30 Dec.	Another vector discovered: Lotus Notes.
Sat.	31 Dec.	Second generation exploit and Guilfanov's patch released. –Yet another vector found: IM.
Sun.	1 Jan.	ISC recommends installation of Guilfanov's patch
Mon.	2 Jan.	Metasploit module updated
Tue.	3 Jan.	McAfee discovers WMFMaker, another tool to create exploits
Wed.	4 Jan.	Microsoft's patch leaked and withdrawn
Thu.	5 Jan.	Patch and Bulletin MS06-001 issued.

Microsoft

- Sped into action
  - Activated its Software Security Incident Response Procedure (SSIRP)
    - The patch possibly written the next day
    - An Advisory was issued within hours
      - Included advice and mitigations
- Yet….
  - The patch was expected on Patch Tuesday, January 10

Why So Late?

- Procedure: Test all versions of the software
  - 450,000 test cases
  - 22,000 stress tests
  - 2,000 WMF files in image library were analyzed
- Policy: All versions of the patch must be released at the same time
  - Major customers don't get it early
  - Microsoft even patches its servers when everyone else does

Metasploit

- A tool to craft exploits easily
  - Developed by H.D. Moore
- WMF module appeared hours after the Bugtraq email
- Exploits multiplied exponentially
- Pressure on Microsoft for the patch

No Satisfactory Defense

- The good guys talk, the good guys learn
- But, workarounds sacrificed functionality, required technical skill, did not work
- Most antivirus signatures required frequent updating
- Differences on what worked, on the operating systems affected, on the risk

A Solution that Worked

- Third party patches
  - The first, by Ilfak Guilfanov, issued New Year's Eve
    - Intended to be a temporary solution
    - ISC made it available

The Race to Protection

- Attackers continued to develop new exploits, new vectors, new tools
- A new Metasploit module was released
- Defenders tried to keep up, but they were still ineffective

The Microsoft Solution

- The patch was leaked on Wednesday
- But it was issued January 5
  - A last minute decision
  - Released ahead of schedule
- Adequate protection was now available

Lessons: What Was Done Right

- Much of the communication was good; much was learned
- The third party patch was useful
  - Zeroday Emergency Response Team (ZERT) was created

Lessons: What Needs to be Done

- Microsoft can be more flexible and more informative
- Other vendors also need to be more open.
- We need to know more about what the bad guys do and how effective they are

Lessons: What You Should Do

- Follow best security practices
  - Defense in depth, up-to-date patching
  - Incident response processes in place
  - Know your network
- Consider host-based whitelisting technologies
  - Authentication of software
    - Examples: Savant, SecureWare Sanctuary, Bit9 Parity, CA HIPS
    - Require effective policies, application lockdown
  - Other options include whitelisting devices, scripts
    - Microsoft Server 2008, Firefox NoScript add-on