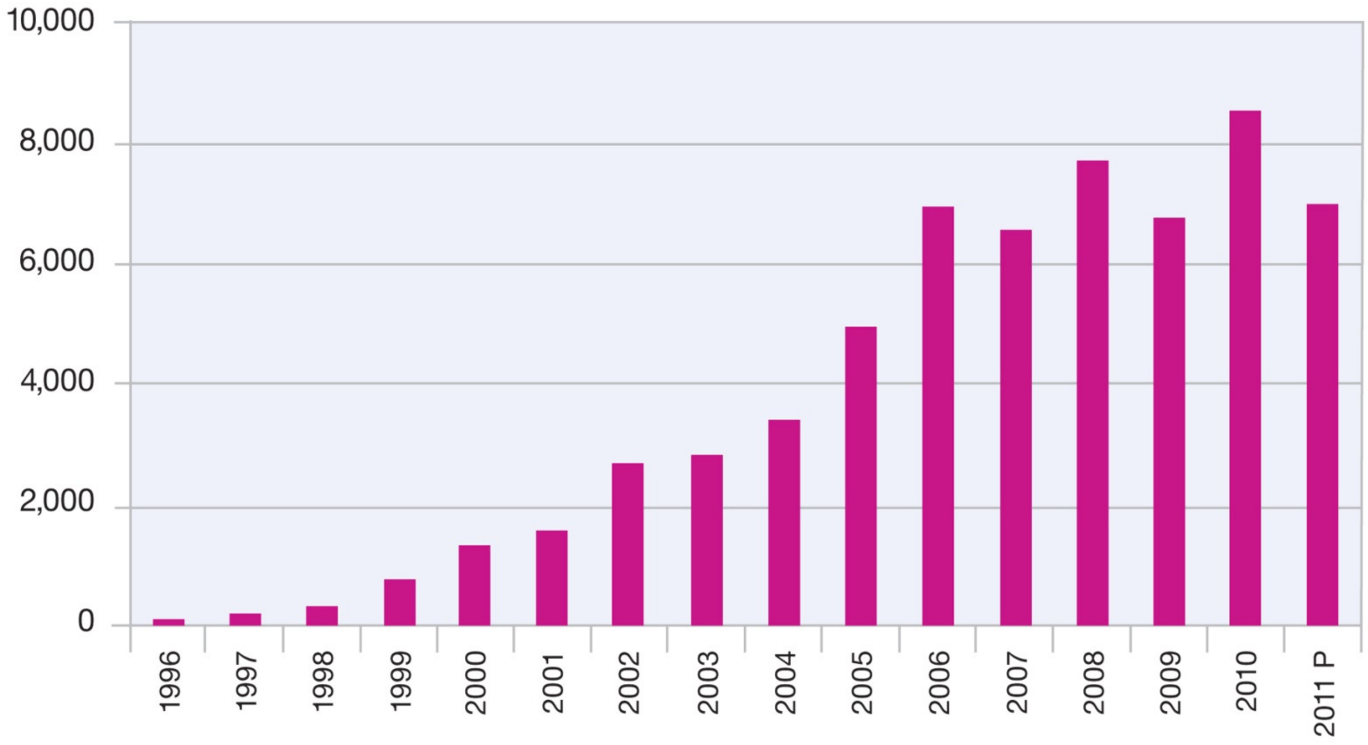
The State of Security Vulnerabilities in 2011

Tom Cross, IBM X-Force

Chris Valasek, Accuvant Labs

There are about 7,000 software vulnerability disclosures every year…



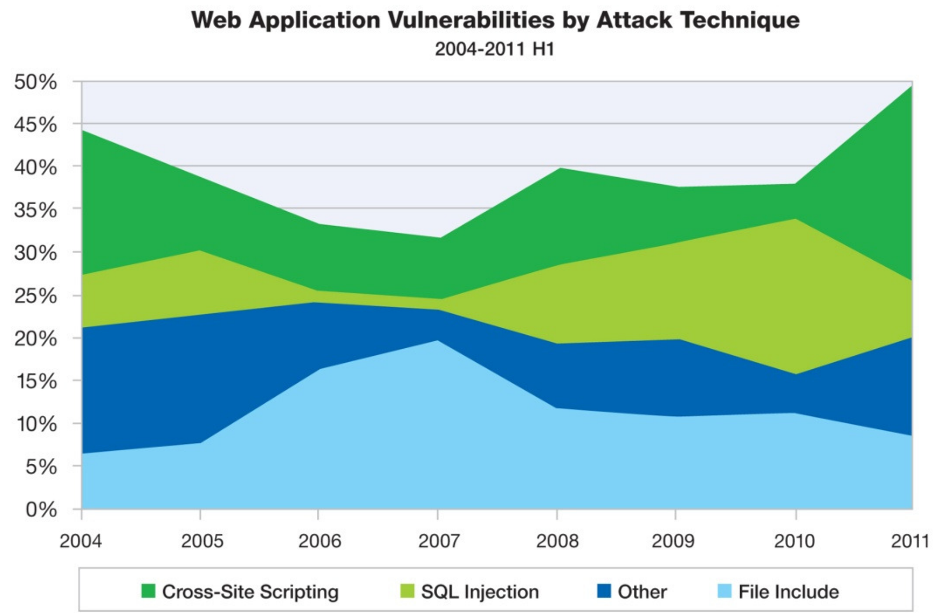
Vulnerability Disclosures Growth by Year

1996-2011 (2011 Half-year Projection)

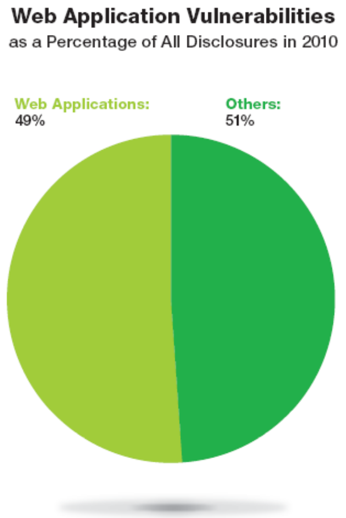
Source: IBM X-Force® Research and Development

Decline in web application vulnerabilities in H1 2011

- In 2010 49% of security vulnerabilities affected web applications.
- In 2011 41% affected web applications.
- Big decline in SQL Injection vulnerabiliites.

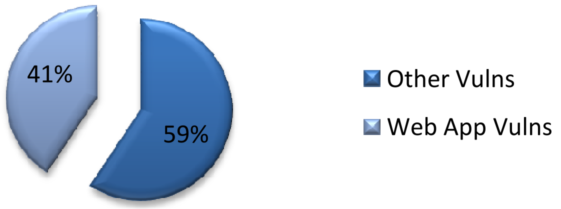


Source: IBM X-Force® Research and Development



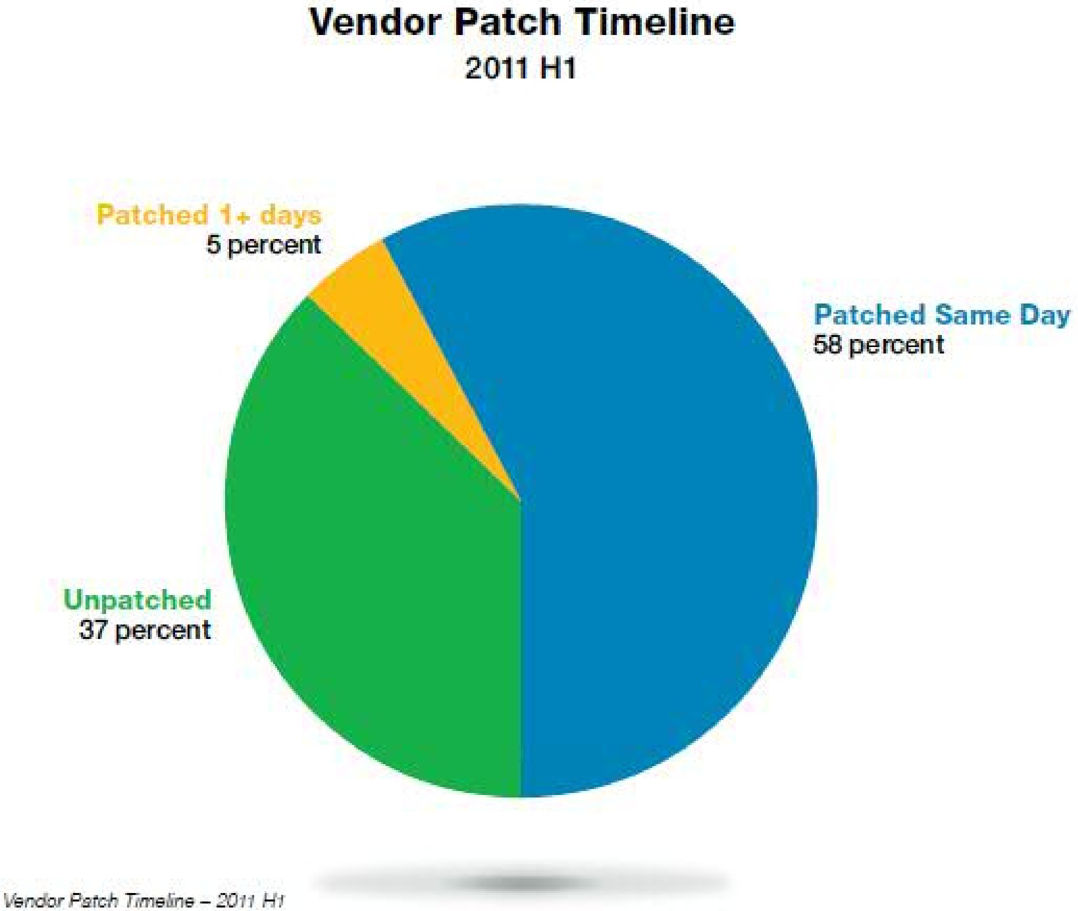
Web Application Vulnerabilities

as a Percentage of All Disclosures in 2011



Patching

- Significant improvement in unpatched vulnerabilities
- Hasn’t dropped below 44% in over five years

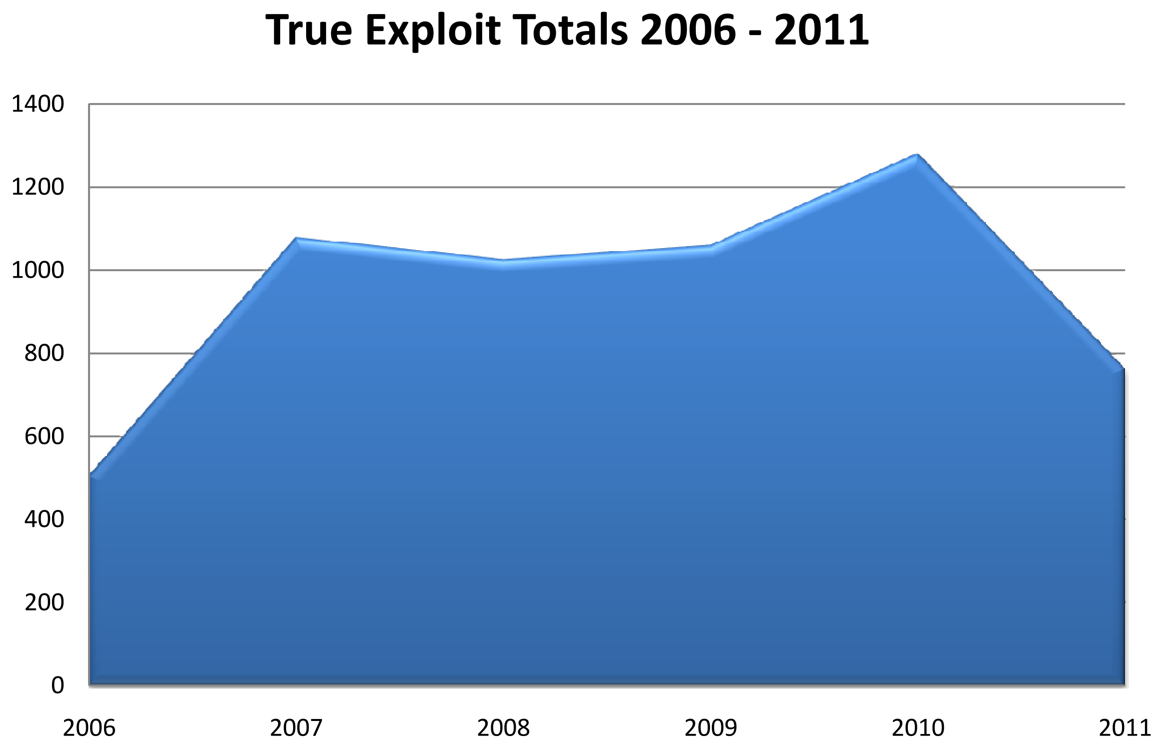


Vendor Patch Timeline
2011 H1

Fig. 33: Vendor Patch Timeline – 2011 H1

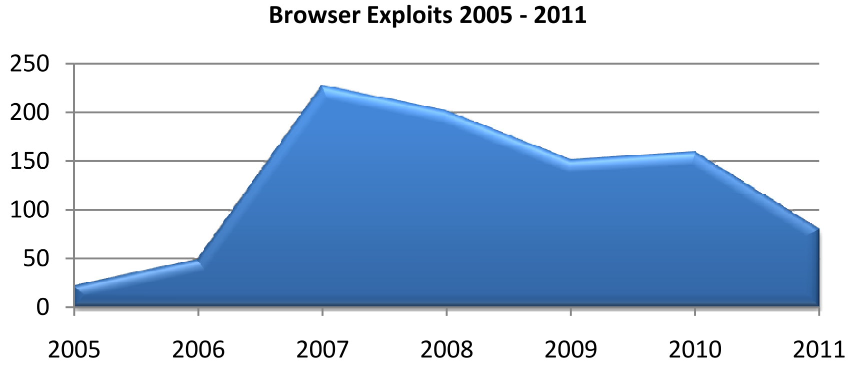
Public Exploit Disclosures

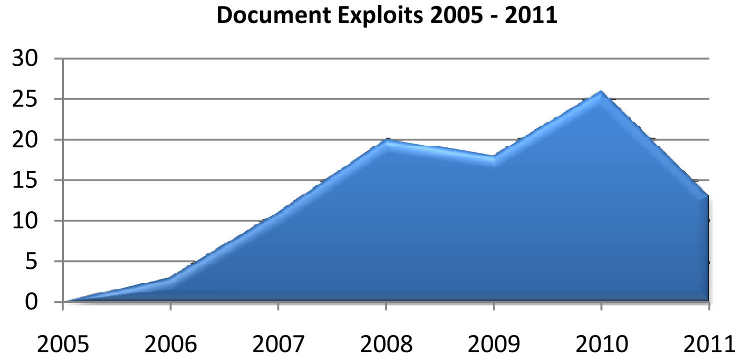
- Fewer exploits released so far this year since 2006
- Down as a percentage of vulnerabilities as well

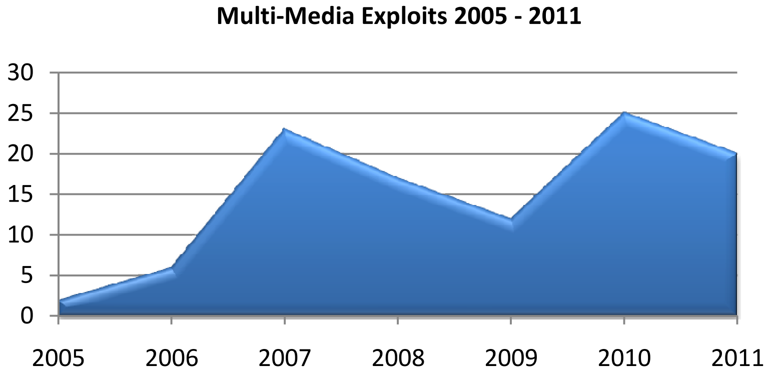


	2006	2007	2008	2009	2010	2011
True Exploits	504	1078	1025	1059	1280	762
Percentage of Total	7.3%	16.5%	13.3%	15.7%	14.7%	10.8%

Public Exploits

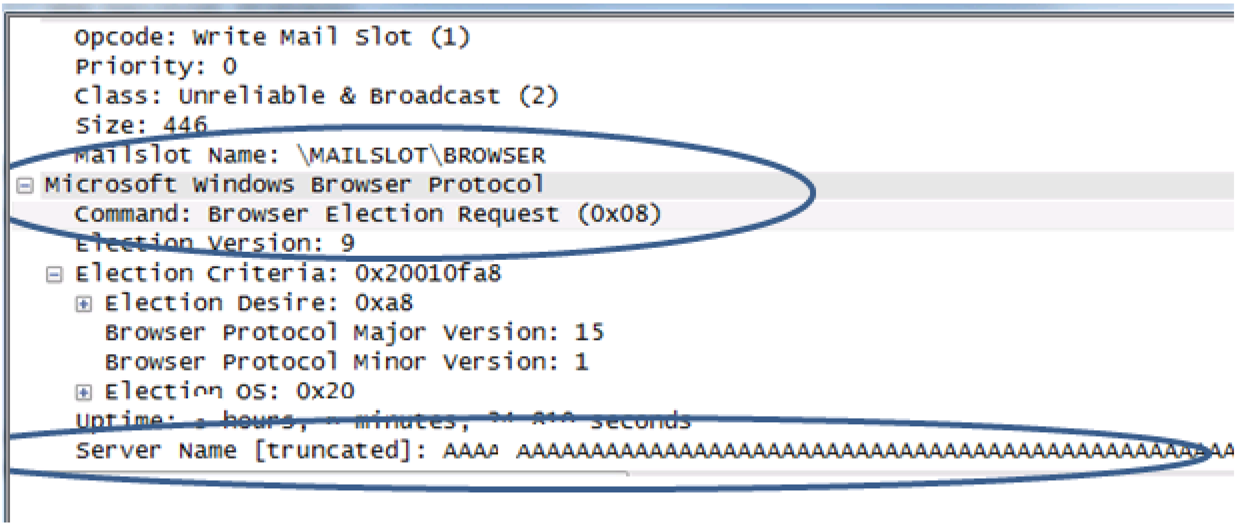






CVE-2011-0654 - MS11-019 - SMB Browser Election Request Overflow

- 0-day POC release in February 2011
- Large string length is 0ed, and then subtracted from, resulting a negative length, which is then used in a memcpy
- Results in a 4 Gig Memcpy



```
  Opcode: Write Mail Slot (1)
  Priority: 0
  Class: Unreliable & Broadcast (2)
  Size: 446
  Mailslot Name: \MAILSLOT\BROWSER
⊟ Microsoft Windows Browser Protocol
  Command: Browser Election Request (0x08)
  Election Version: 9
⊟ Election Criteria: 0x20010fa8
  ⊞ Election Desire: 0xa8
    Browser Protocol Major Version: 15
    Browser Protocol Minor Version: 1
  ⊞ Election OS: 0x20
  Uptime: [illegible] hours, [illegible] minutes, [illegible] seconds
  Server Name [truncated]: AAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

CVE-2011-1966 – MS11-058: Windows DNS Server RCE

MSRC:

The issue is a sign-extension vulnerability where a small negative number is expanded to a larger type without proper checks. Later, this large negative number is used as a memcpy count to populate a heap buffer. The copy length will always be at least 0x80000000 bytes long so the copy operation itself will likely fail in the absence of 2+ GB of memory available to be copied.

Even if an attacker is able to successfully populate memory for the copy to succeed and massage the heap to gain control of the process, the platform mitigations of ASLR, DEP, and the heap metadata protection must still be overcome before malicious code could be run.

DNS service will no longer restart it after it crashes three times.

Microsoft Exploitability Index: “3 – Functioning Exploit Code Unlikely”.

CVE-2011-2013 – MS11-083 – UDP Refcount Overflow

- MSRC Exploitability index of 2.
- When UDP Packets are received, some data structures are initialized and a reference counter is incremented, but the data structures are never dereferenced.
- By sending 2^32 UDP Packets, attacker can cause the reference counter to wrap.
- If the memory is then dereferenced, this can create an unstable condition, if it is referenced again.
- A different request is required to cause the dereference (as obviously the dereference was missing from the UDP handler).
- An ICMP Echo request can cause the dereference to occur.
- Then there is the matter of getting attacker controlled data into that memory location…
- prdelka released an exploit: “I calculated that it would take approximately 52 days for the host to enter a condition where this vulnerability is triggerable.”
- Todd Manning at BreakingPoint was able to trigger in 8 hours in a lab.

CVE-2010-4701 – MS11-024: Windows Fax Cover Page Editor

- Public POC disclosed in December 2010.
- Microsoft gave this an exploitability index of 3 – patched in April, 2011.

```
0:000> !load ./winext/msec.dll
    ...
    (20d4.2728): C++ EH exception - code e06d7363 (first chance)
    (20d4.2728): Access violation - code c0000005 (first chance)
    First chance exceptions are reported before any exception handling.
    This exception may be expected and handled.
    eax=00c6f118 ebx=00c6f118 ecx=41414141 edx=00c90d08 esi=00c6f110 edi=00270000
    eip=7c83e790 esp=0006f084 ebp=0006f148 iopl=0 nv up ei ng nz na po cy
    cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010283
    ntdll!RtlAbsoluteToSelfRelativeSD+0x5cd:
    7c83e790 8901 mov dword ptr [ecx],eax ds:0023:41414141=????????
  User mode write access violations that are not near NULL are exploitable.
    ...

    at a first look this seems exploitable, we can write four bytes into an arbitrary location.
    I'm posting a proof-of-concept written in php which creates a malformed .cov file.
    Results may vary if the buffer is modified. Full exploit is in stage of developing.
    */
```

CVE-2011-0661 - MS11-020: SMB Server RCE

- Wormable! RCE in Windows SMB Stack
- MSRC Exploitability Index of 1
- SANS: PATCH NOW!

- No POC – No Exploit - Nada

CVE-2010-3972 - MS11-004 – IIS FTP IAC Overflow

- Originally disclosed in December 2010 by Matthew Bergin as a 'denial of service'

- Microsoft claimed that exploitation would be near impossible
  - http://blogs.technet.com/b/srd/archive/2010/12/22/assessing-an-iis-ftp-7-5-unauthenticated-denial-of-service-vulnerability.aspx

- Attacker controllable number of 0xFF bytes written sequentially past the end of a heap buffer.

CVE-2010-3972 - MS11-004 – IIS FTP IAC Overflow

- Why no public, real-world exploits?
  - Intricate knowledge of IIS FTP server, FTP protocol, Windows 7 heap internals and exploitation techniques
  - Very time consuming to develop an actual, precision exploit (more RCE than DoS)
  - Massive amounts of heap massaging to get memory in a deterministic state
  - Quite hard on single core processor, would be increasingly difficult w/ more cores
    - I don’t believe it would be impossible, but reliability would go down substantially

- This is typical of this type of vulnerability (and many vulnerabilities). You need strong knowledge of memory management, operating system, application and weird machines

- http://prezi.com/irrl_vrs7dva/modern-lfh-exploitation/?auth_key=9f87b988d7f5276e121f472322ea4693a1c39f79

Comments:

- Exploitation is much harder now than it used to be: ASLR, DEP, Stack Cookies (/GS), Heap Mitigations, Sandboxing
- If you look at www.exploit-db.com you'll see many exploits for code injection, stack overflow on non-ASLR / non-GS applications
- A lot of public exploits end up being for client side applications
- Many claim to be selling exploits, hence no reason to publicly release them
  - While the price may be disputed, NSS labs has a program offering small amounts of money for non-0day exploits
  - https://www.exploithub.com/

CVE-2010-3970 – MS11-006

- Windows thumbnail rendering engine
- CMP ECX, 0x100; JG ERROR;
- Stack overflow
- A Vulnerability in My Heart – Moti & Xu Hao
- Bugs like this are still out there

Multi-media & document vulnerabilities

- Significant increases in both categories
- Attackers have zeroed in on software that consumers are running regardless of the browser
- Recent efforts to sandbox these applications are not perfect

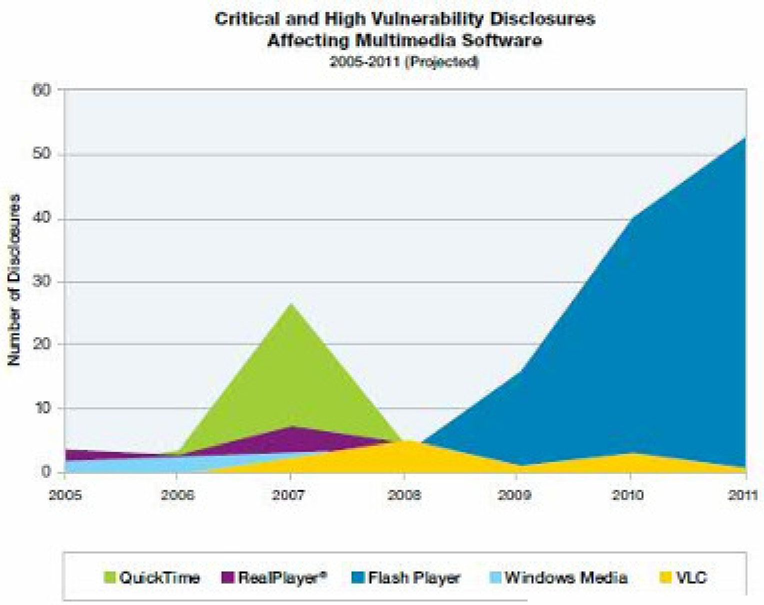

Critical and High Vulnerability Disclosures
Affecting Multimedia Software
2005-2011 (Projected)

Figure 37: Critical and High Vulnerability Disclosures Affecting Multimedia Software –2005-2011 (Projected)

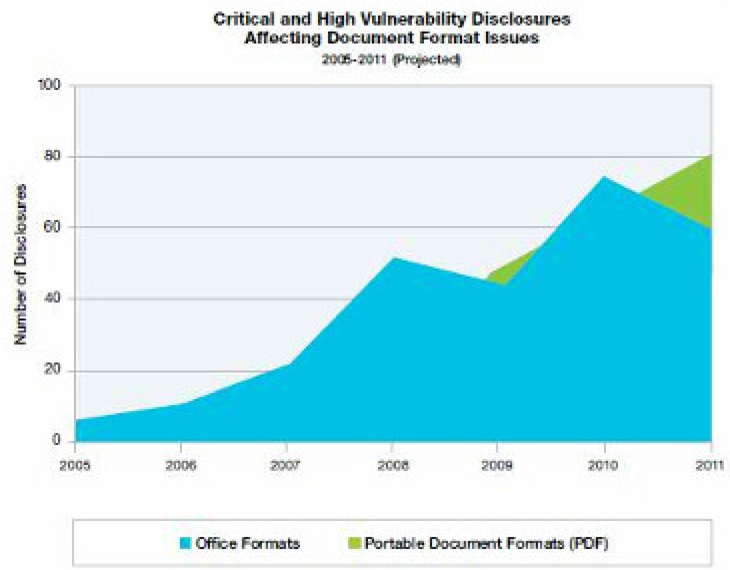
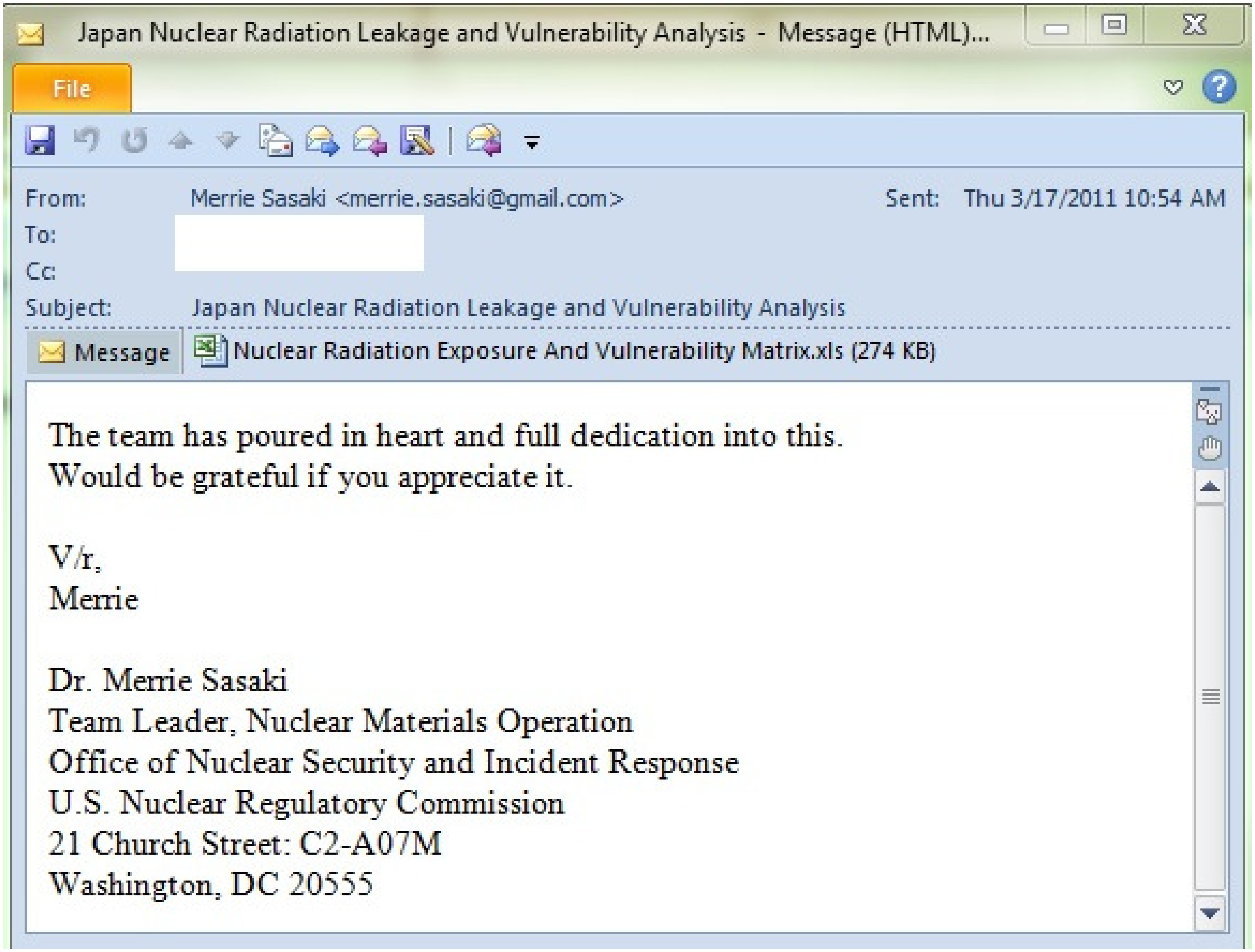

Critical and High Vulnerability Disclosures
Affecting Document Format Issues
2005-2011 (Projected)

Figure 38: Critical and High Vulnerability Disclosures Affecting Document Format Issues – 2005-2011 (Projected)

CVE-2011-0609


Japan Nuclear Radiation Leakage and Vulnerability Analysis - Message (HTML)...
File

From: Merrie Sasaki <merrie.sasaki@gmail.com>

Sent: Thu 3/17/2011 10:54 AM

To: [redacted]

Cc:

Subject: Japan Nuclear Radiation Leakage and Vulnerability Analysis

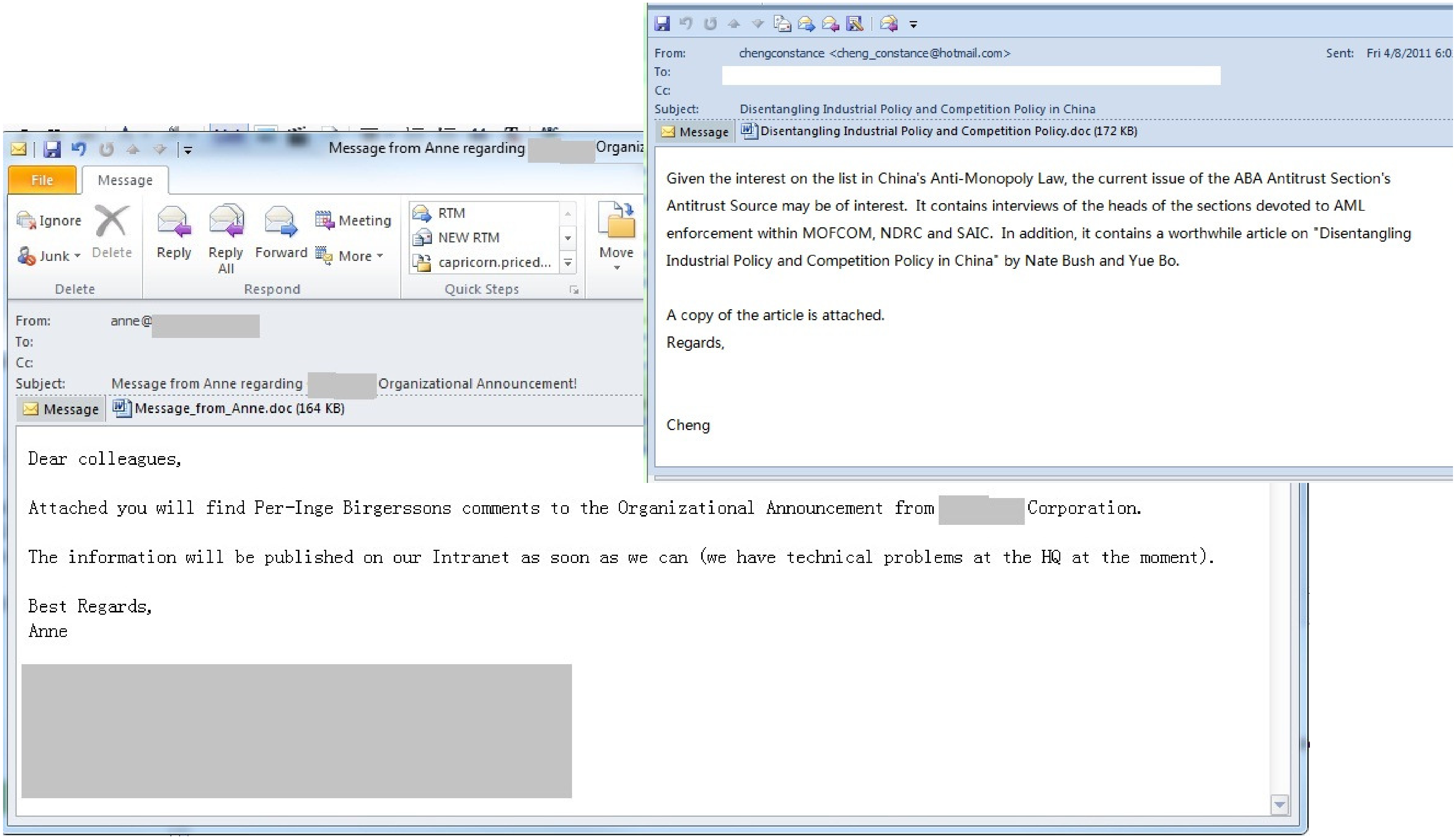
Message | Nuclear Radiation Exposure And Vulnerability Matrix.xls (274 KB)

The team has poured in heart and full dedication into this.
Would be grateful if you appreciate it.

V/r,
Merrie

Dr. Merrie Sasaki
Team Leader, Nuclear Materials Operation
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
21 Church Street: C2-A07M
Washington, DC 20555

CVE-2011-0611



From: chengconstance <cheng_constance@hotmail.com> Sent: Fri 4/8/2011 6:0

To: [redacted]

Cc:

Subject: Disentangling Industrial Policy and Competition Policy in China

Message | Disentangling Industrial Policy and Competition Policy.doc (172 KB)

Given the interest on the list in China's Anti-Monopoly Law, the current issue of the ABA Antitrust Section's Antitrust Source may be of interest. It contains interviews of the heads of the sections devoted to AML enforcement within MOFCOM, NDRC and SAIC. In addition, it contains a worthwhile article on "Disentangling Industrial Policy and Competition Policy in China" by Nate Bush and Yue Bo.

A copy of the article is attached.

Regards,

Cheng

From: anne@[redacted]

To:

Cc:

Subject: Message from Anne regarding [redacted] Organizational Announcement!

Message | Message_from_Anne.doc (164 KB)

Dear colleagues,

Attached you will find Per-Inge Birgerssons comments to the Organizational Announcement from [redacted] Corporation.

The information will be published on our Intranet as soon as we can (we have technical problems at the HQ at the moment).

Best Regards,
Anne

[redacted]

CVE-2011-0609 & CVE-2011-0611

- Errors in ActionScript Just in Time compiling
- At least one of these bugs was fuzzed
- Exploitation via Heap Spray
- Stealth (sort of)
  - SWF files delivered in Office Documents
    - SWF called from SWF
  - "Drive-by Caching" A/V evasion
- Lots of activity – still in use

Mobile OS Vulnerabilities & Exploits

- Continued interest in Mobile vulnerabilities as enterprise users bring smartphones and tablets into the work place

- Attackers finally warming to the opportunities these devices represent

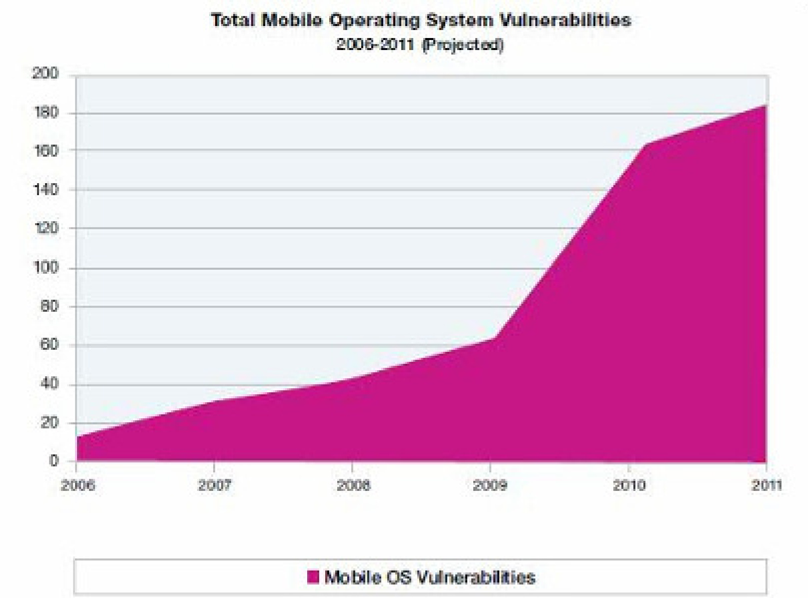


Figure 39: Total Mobile Operating System Vulnerabilities – 2006-2011 (Projected)

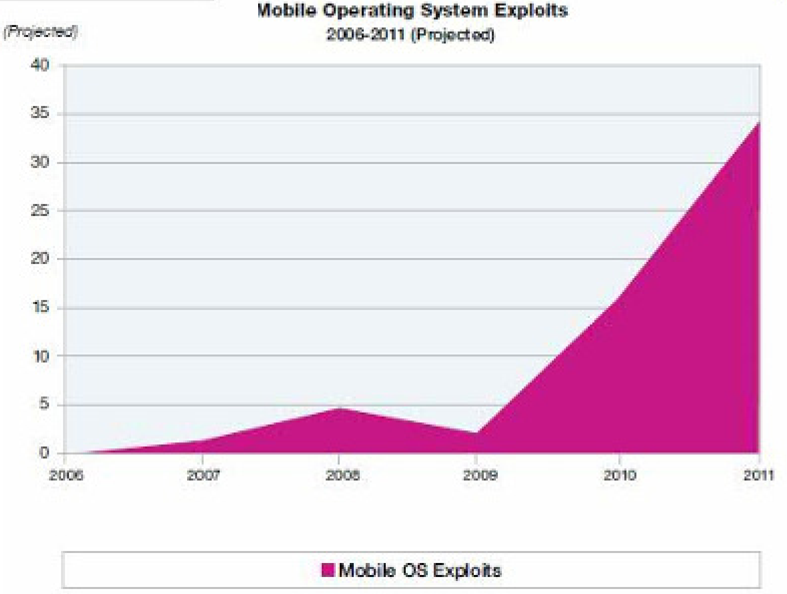


Figure 40: Mobile Operating System Exploits – 2006-2011 (Projected)

SSL

- The BEAST
  - Java vulnerability enabled violation of SOP
    - Fixed
  - Weakness in CBC
    - **Some** browser workarounds shipped
- Multiple SSL Certificate Authority Problems
  - Diginotar
  - DigiCert Sdn Bhd (issued weak certs)
- Ongoing dialog about “fixing” the Certificate problem
  - Moxie Marlinspike’s Convergence Firefox Plugin
  - Sovereign Keys

Denial of Service

- RefRef – Select Benchmark
  - Pentesters use this.
- THC SSL renegotiation issue
  - Use of a single connection could foil some DDOS protections
- Apache ByteRange
  - KingCope – public exploit

The Day that SQL Slammer Disappeared

- January 25, 2003 SQL slammer began a mass infection of Internet connected servers
- Using random IP addresses, 90% of infected servers were infected within 10 minutes of release
- So ubiquitous, techies used its packets to test for Internet connectivity
- On March 10th &11th, 2011 it all but dissapeared

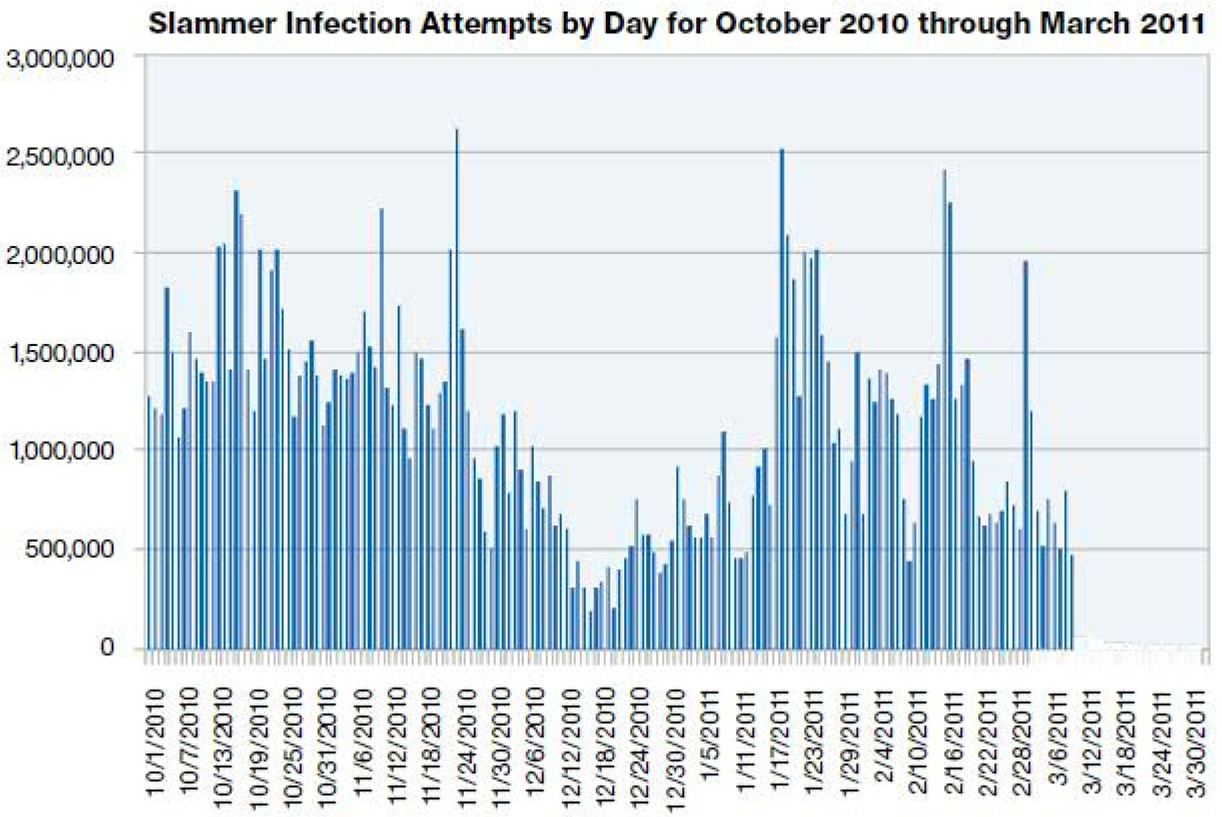


Figure 6: Slammer Infection Attempts by Day for October 2010 through March 2011

SQL Slammer Disappearance Analysis

- Dramatic drop-off not a naturally occurring phenomenon
- Phased draw down over a 20 hour period points to clock-based shut off issued by the same coded trigger
- Geo-adjusted timing data falls off quicker than non-adjusted points to a trigger set to occur between 11AM and Noon

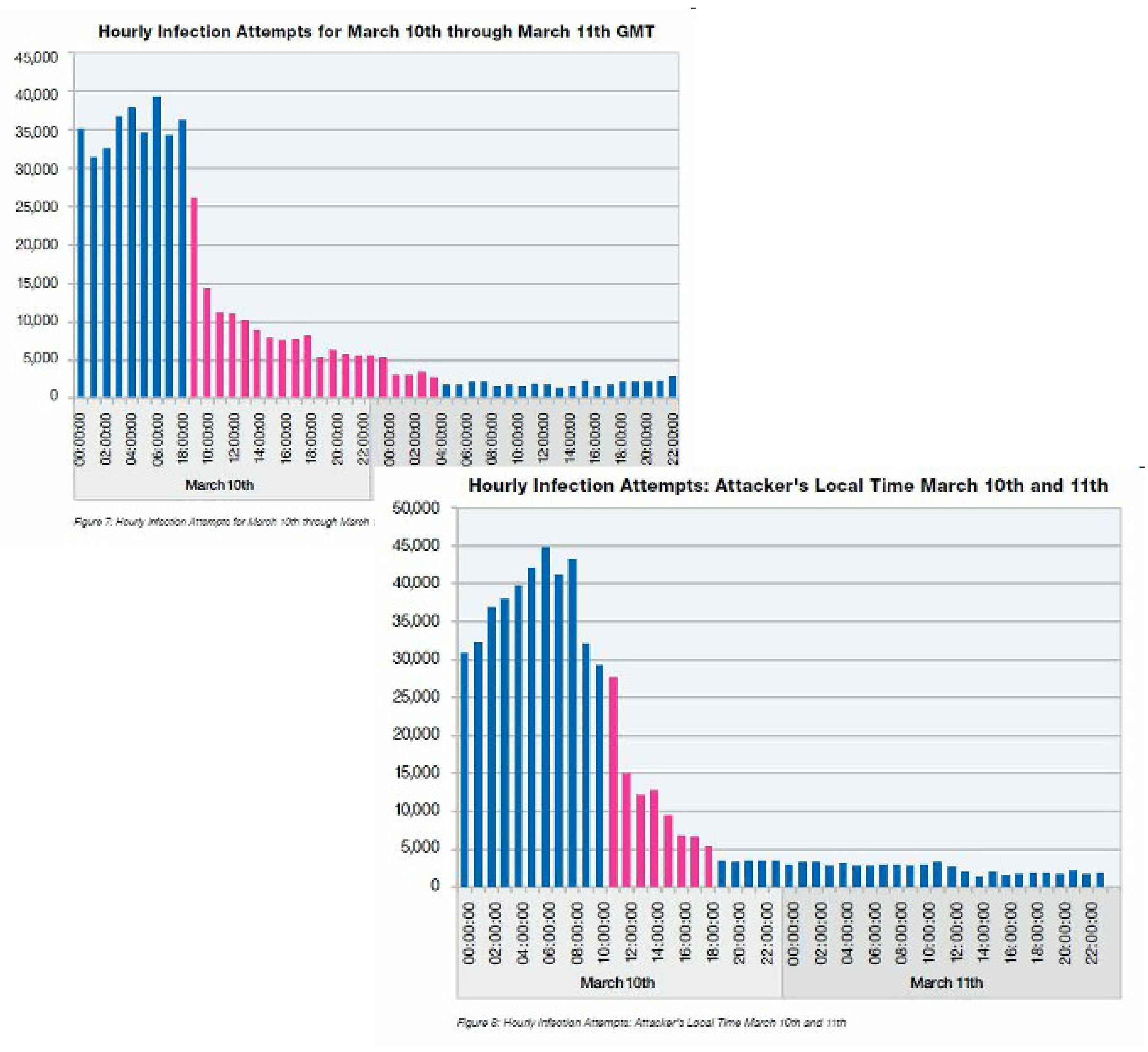


Figure 7: Hourly Infection Attempts for March 10th through March

Figure 8: Hourly Infection Attempts: Attacker's Local Time March 10th and 11th

Black or a White Knight?

- Attack packets gave map to easily exploitable machines.
  - Did a bad actor compromise these machines to create a botnet?
  - Automatic patch and reboot to stop giving themselves away

- Or did a White Knight decide to rid the world of Slammer with the exact methodology
  - Without the botnet

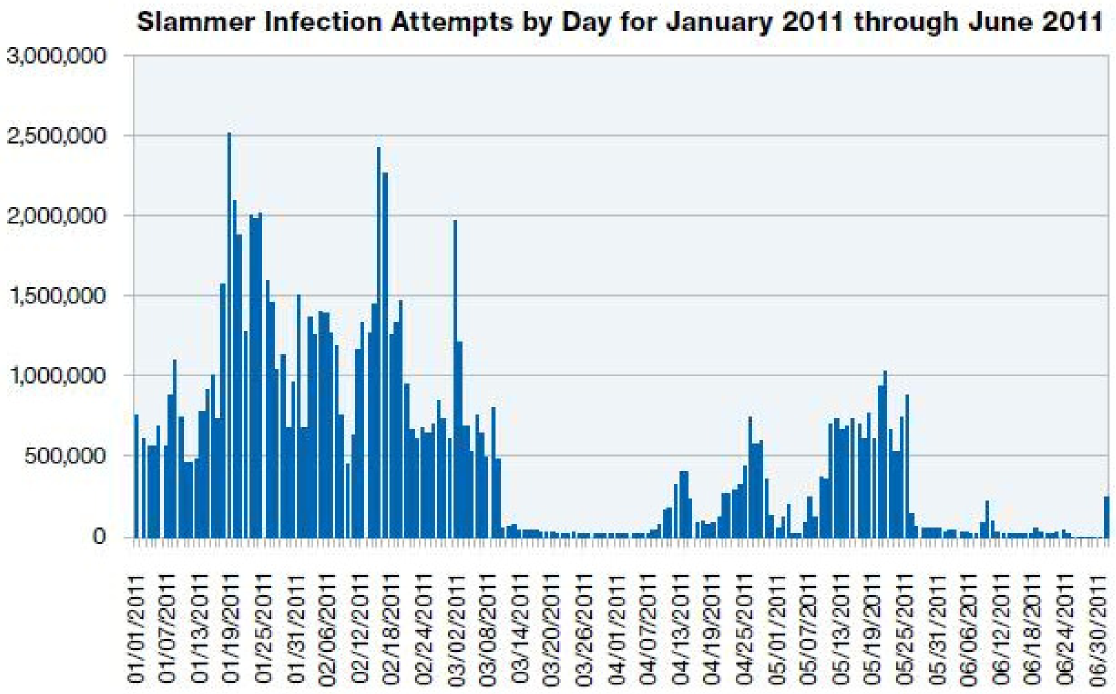


Figure 9: Slammer Infection Attempts by Day for January 2011 through June 2011

Security community trying to figure this out?