Lessons Learned:
Can alerting the public about exploitation do more harm than good?

About Us

- Tom Cross, IBM X-Force
  - Vulnerability tracking, analysis, and response
  - IPS signature delivery
  - MAPP (Microsoft Active Protections Program) partner
  - X-Force Trend and Risk Report
- Holly Stewart, Microsoft Malware Protection Center (MMPC)
  - Coordination for MMPC as a MAPP partner
  - Communication and response for emerging issues (exploits, malware, etc.)
  - Intelligence reports
  - Not a part of Microsoft Security Response Center (MSRC)

Overview

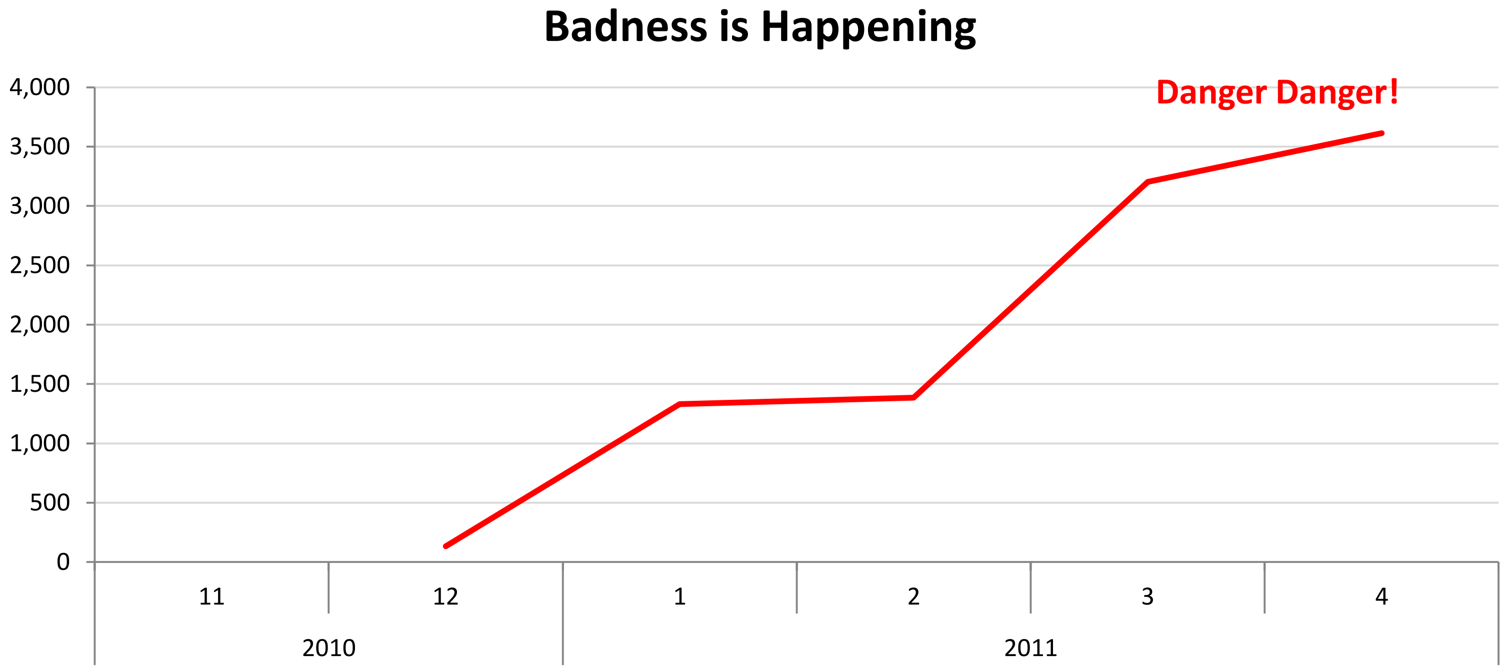
- Exploitation disclosure
  - Define exploitation disclosure
  - How is it different from vuln disclosure?
- What are the risks associated with disclosing exploitation too early?
- What impact does in the wild exploitation have on vulnerability disclosure timing?
- Use cases, examples, lessons learned
- Guidance

A lot of ink has been spilled on Vulnerability Disclosure.

- Vulnerability Disclosure is public disclosure of the fact that a vulnerability exists.
- In general, its preferable if vulnerability disclosure happens in ***coordination*** with the vendor of the vulnerable product, in ***conjunction*** with the release of fix information.
- In some rare cases, it may be necessary to disclose a vulnerability before a fix is available…
  - One such case may be the case where there is exploitation in the wild.

What is exploitation disclosure?

Public disclosure of the fact that a vulnerability is being exploited in the wild.



Why is Exploitation Disclosure important?

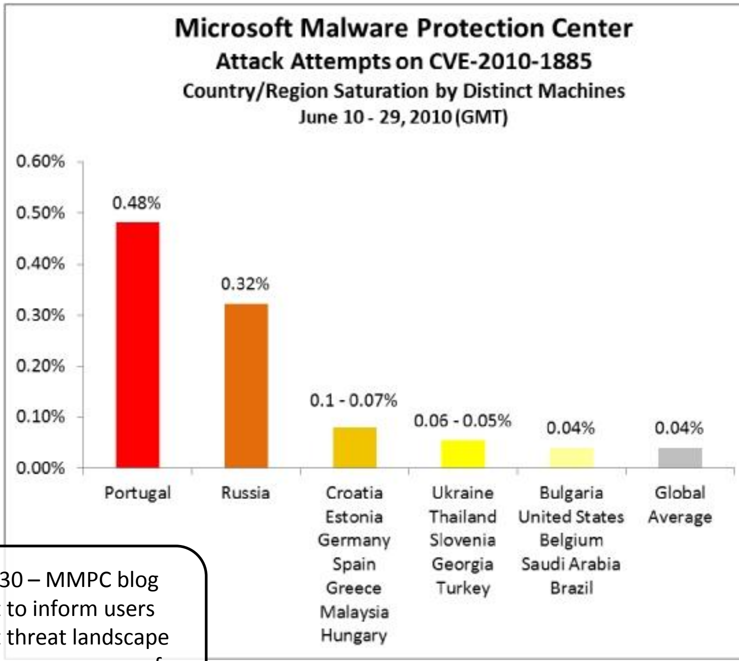
- Software vendors and IT professionals need to understand how to prioritize vulnerability remediation – Exploitation can motivate faster remediation.

- Security product vendors need access to real world exploit samples so they can validate coverage.

- Network managers need to know what attacks are taking place in real time, so they can be prepared and focus their attention on the right warning signs and mitigations.

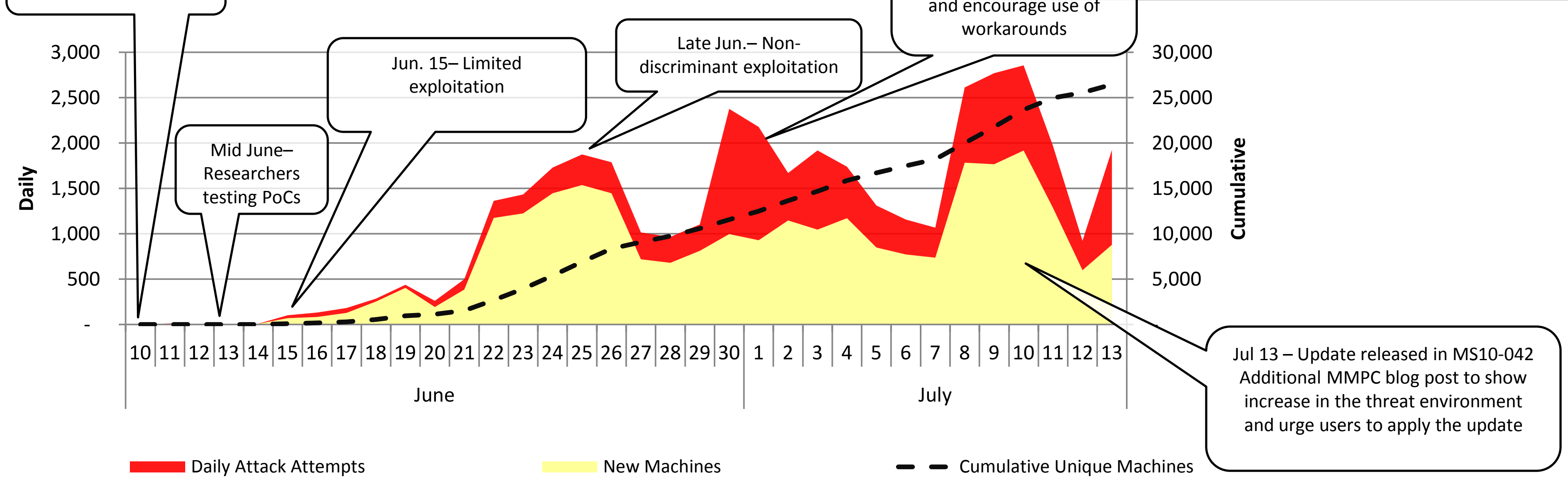
- End users need to know what the overall threat environment is on the Internet

Example: Public knowledge of exploitation can motivate faster deployment of mitigations CVE-2010-1885



Microsoft Malware Protection Center
Attack Attempts on CVE-2010-1885
Country/Region Saturation by Distinct Machines
June 10 - 29, 2010 (GMT)

Microsoft Malware Protection Center
Attack Attempts on CVE-2010-1885
as of midnight July 13, 2010 (GMT)



Jun. 10 – Full Disclosure + PoC

Mid June– Researchers testing PoCs

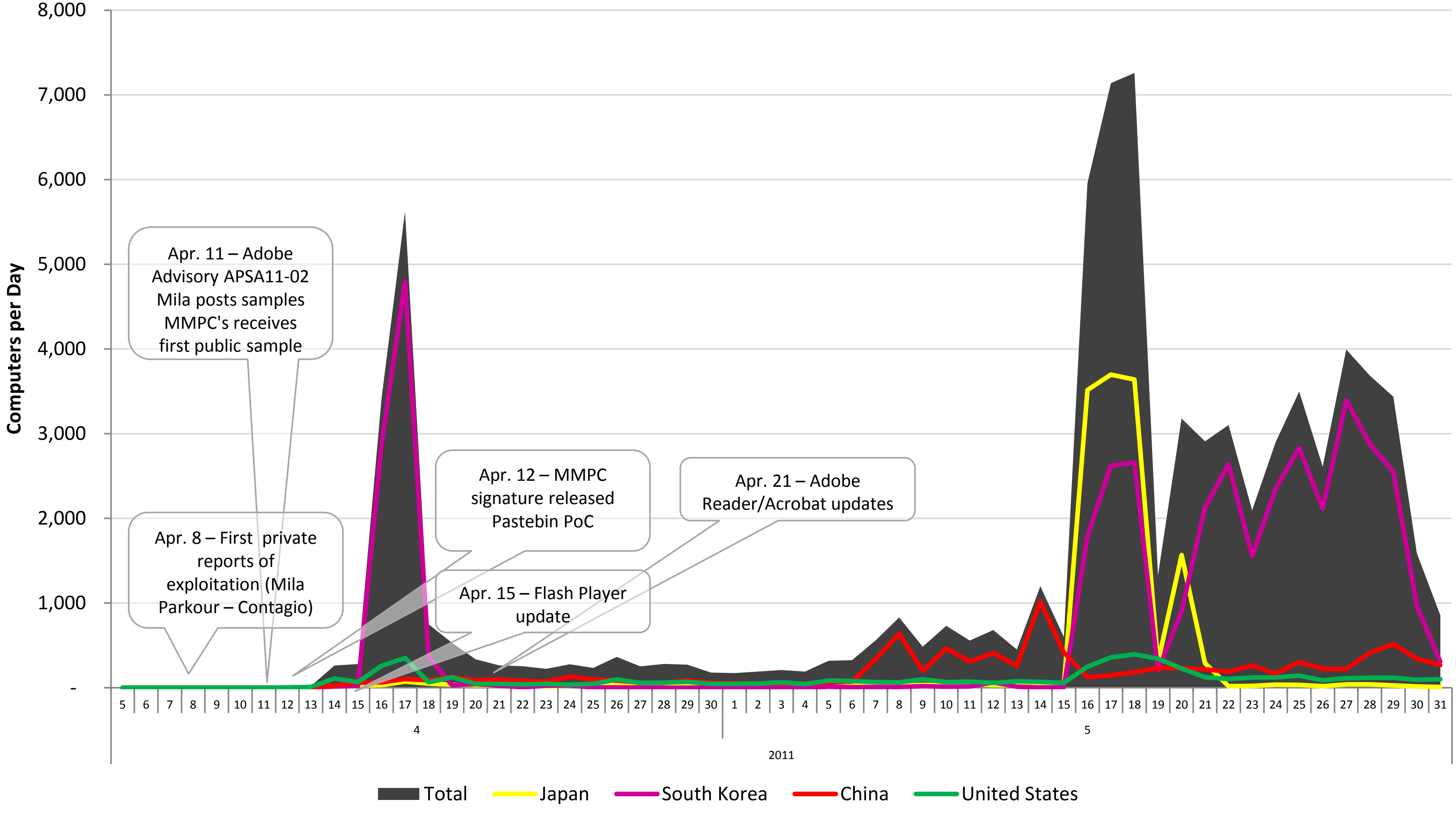
Jun. 15– Limited exploitation

Late Jun.– Non-discriminant exploitation

Jun. 30 – MMPC blog post to inform users about threat landscape and encourage use of workarounds

Jul 13 – Update released in MS10-042 Additional MMPC blog post to show increase in the threat environment and urge users to apply the update

Example: Coordinated disclosure helps the affected vendor prioritize the update CVE-2011-0611



Apr. 11 – Adobe Advisory APSA11-02
Mila posts samples
MMPC's receives first public sample

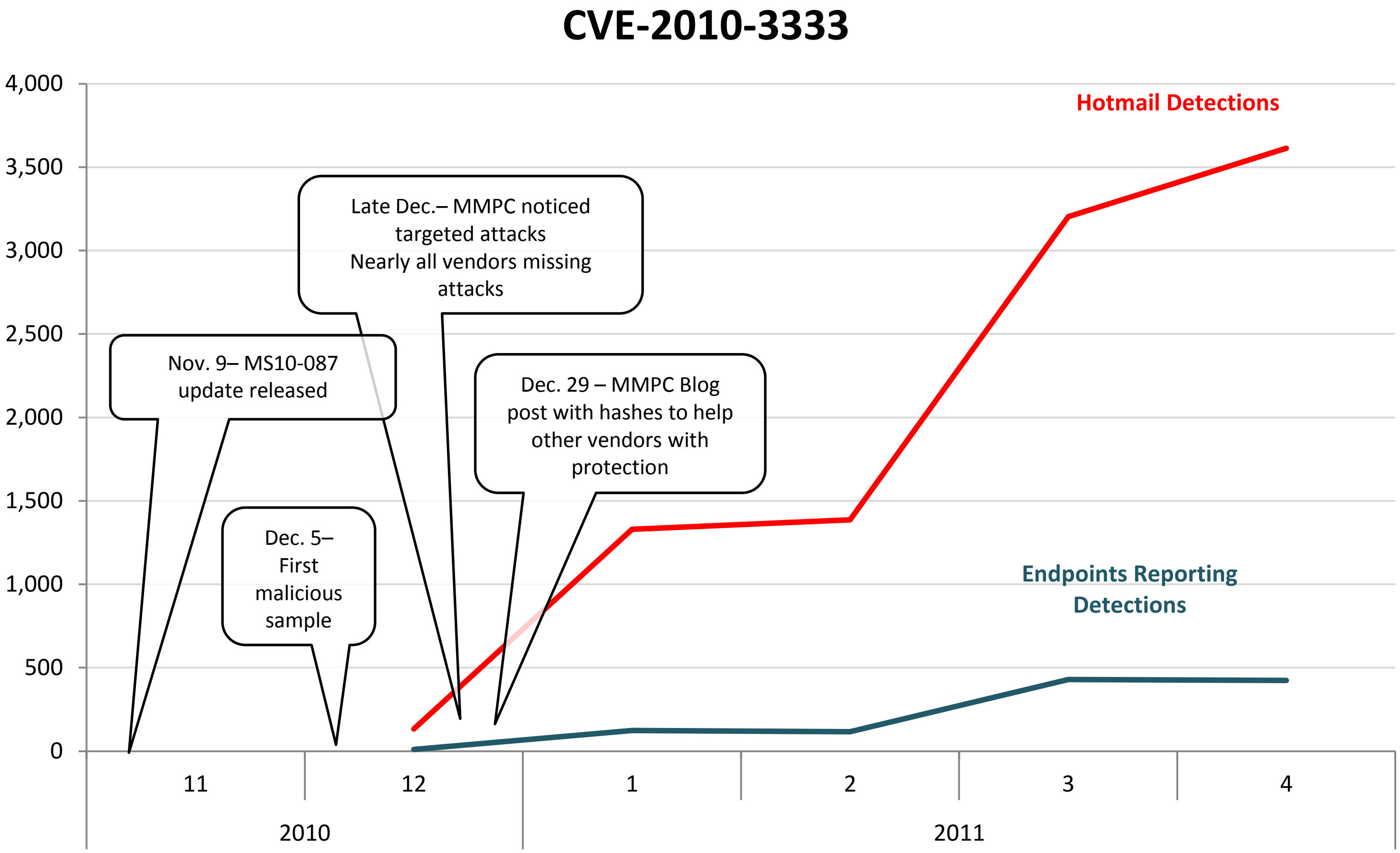
Apr. 8 – First private reports of exploitation (Mila Parkour – Contagio)

Apr. 12 – MMPC signature released
Pastebin PoC

Apr. 15 – Flash Player update

Apr. 21 – Adobe Reader/Acrobat updates

Example: Real-world samples sometimes evade security product coverage CVE-2010-3333



When to disclose exploitation?

- The hard part isn’t deciding whether to disclose, but when.

- Disclosure can happen in one of three ways:
  - Before disclosure of the vulnerability.
  - In conjunction with disclosure of the vulnerability.
  - After the vulnerability has been disclosed.

- Let’s consider each case…

Exploitation disclosure BEFORE vulnerability disclosure

Before

- Many breaches are disclosed without indicating whether or not a new vulnerability was involved.
  - Breaches involving APT or other sophisticated attackers are often associated with 0-day vulnerabilities but this may not be explicitly stated to the general public.
  - This isn’t terribly useful…

Before

- Saying “there is a bad vulnerability and people are exploiting it but we won’t tell you what it is” can create PANIC.
  - People know there is a problem
  - They don’t know what to do about it
  - So they freak out…

Before

- Breaches disclosed with **actionable** information about what happened are helpful to security practitioners.
  - Pilots regularly read NTSB accident reports. Do most IT security pros regularly read breach post mortums?
- Your mitigation advice might not be trusted if you aren’t planning to disclose the vulnerability in the future.
  - People have a legitimate need to know why you are suggesting the mitigations you are suggesting, so that they can evaluate whether or not your mitigations make sense in their environment.

Therefore…

- It probably doesn’t make sense to disclose that a new vulnerability is being exploited BEFORE vulnerability disclosure unless some actionable advice can be provided.
- The more specific the advice, the closer this is to plain old vulnerability disclosure.

Exploitation disclosure IN CONJUNCTION with vulnerability disclosure

OK, we’re going to simultaneously disclose both the fact that a new vulnerability exists and the fact that it is being exploited in the wild.

The question is, when?

Immediately?

- Usually, if we knew about a new vulnerability, we’d wait for the vendor to release updates before disclosing it, but if exploitation is going on in the wild, that changes things.

- People need to know that they might be hit with these attacks.

- The bad guys already have the information, so disclosing the vulnerability right away only helps the good guys, right?

Why Wait?

- The “bad guys” are not all working together!

- General publicity about a vulnerability without actionable information can attract more attackers to the opportunity.

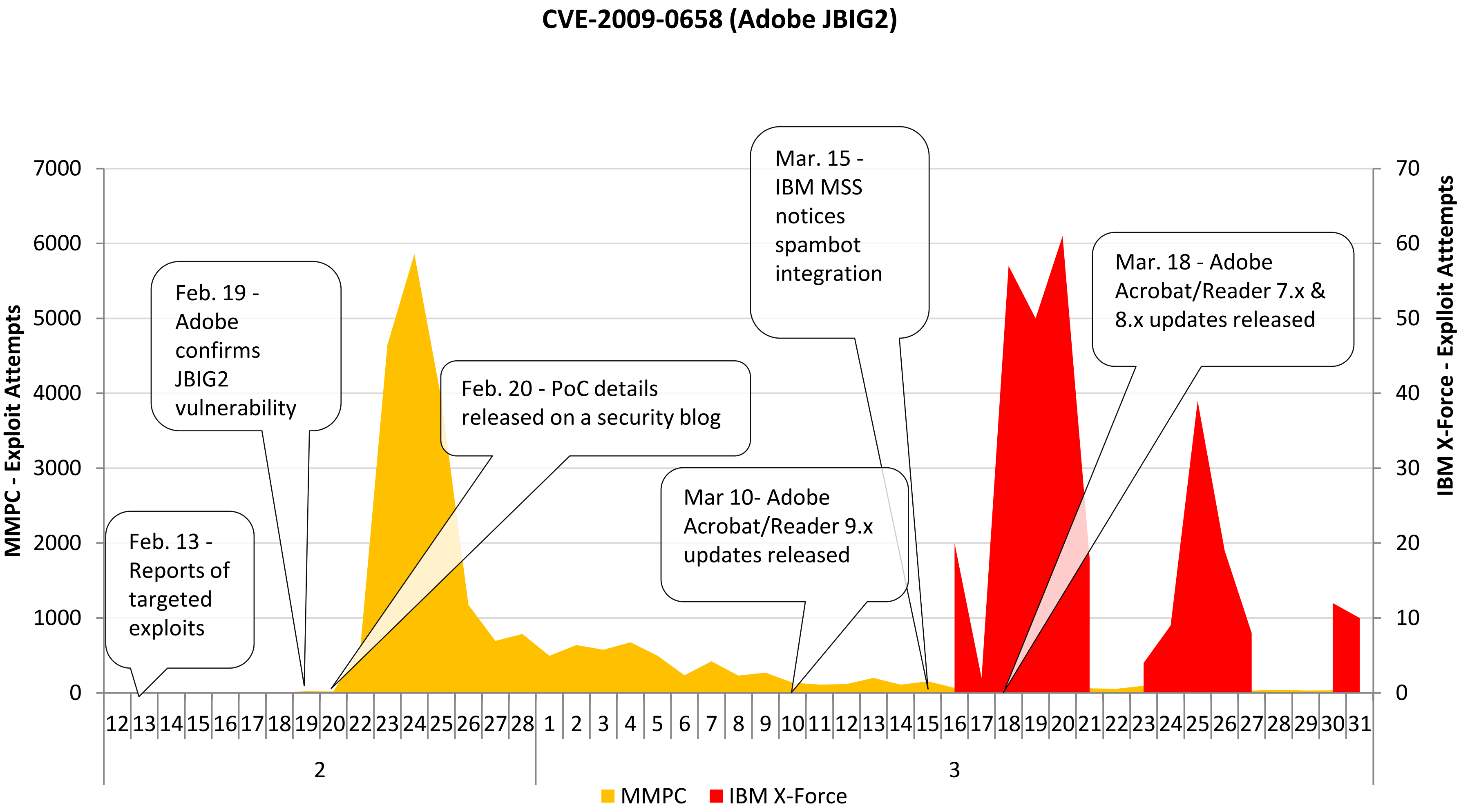
- Scope of attacks can move from targeted to limited to broad.

Defining Exploitation Levels

- Real Exploitation can be…
  - Targeted – Focused on a specific organization or perhaps a small collection of specific entities.
  - Limited – Low in number, could be predominantly affecting one region or industry.
  - Broad – Indiscriminate targets crossing geolocations

0-day Examples

Example: Publicity and PoC details draw attention to lucrative targets CVE-2009-0658



Feb. 13 - Reports of targeted exploits

Feb. 19 - Adobe confirms JBIG2 vulnerability

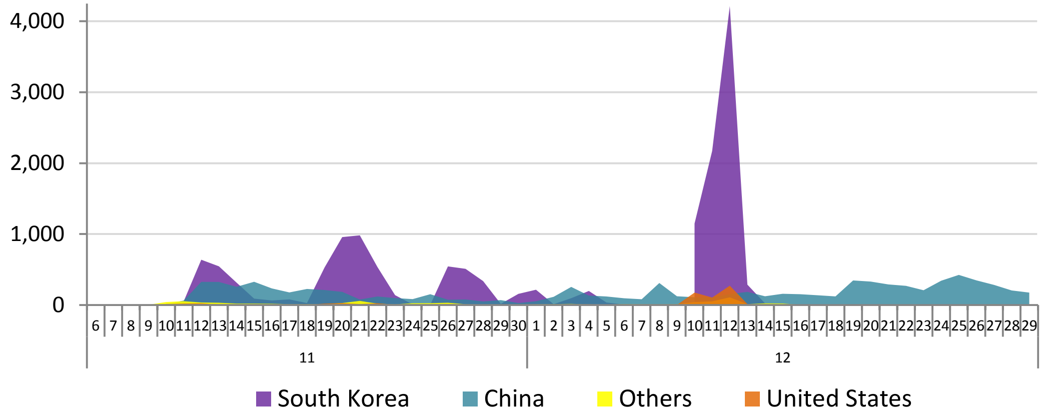
Feb. 20 - PoC details released on a security blog

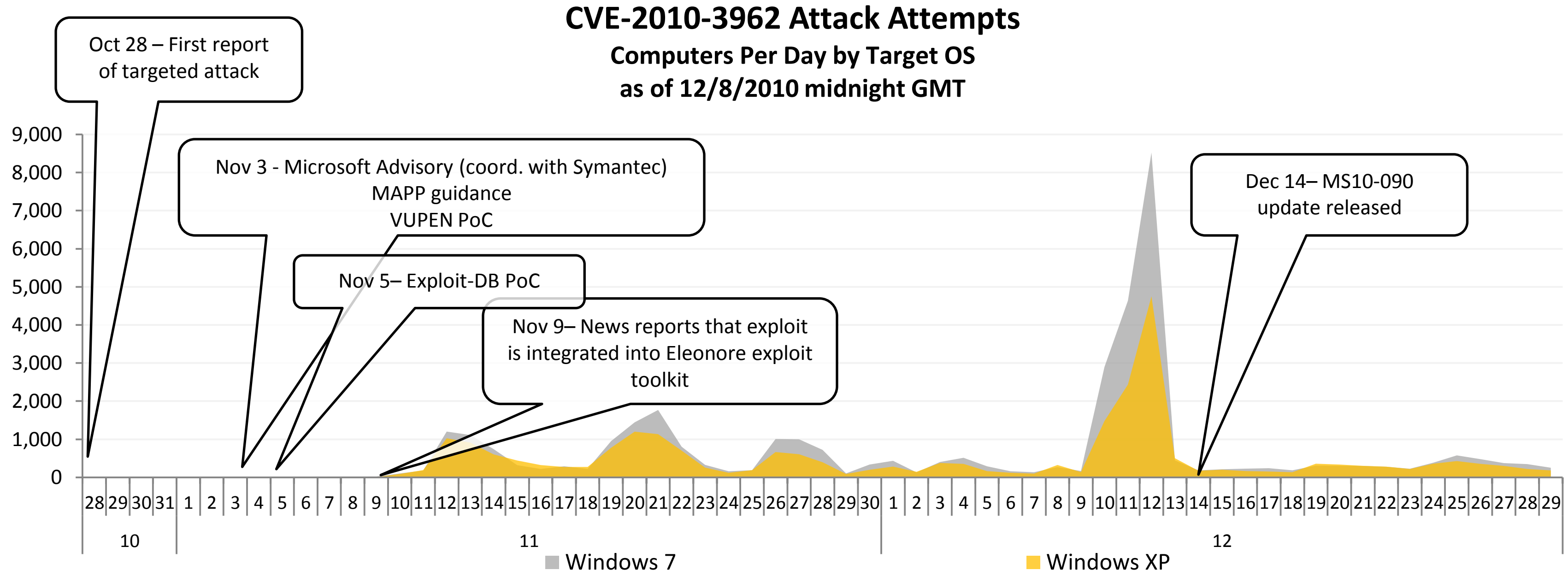
Mar 10- Adobe Acrobat/Reader 9.x updates released

Mar. 15 - IBM MSS notices spambot integration

Mar. 18 - Adobe Acrobat/Reader 7.x & 8.x updates released

Example: Coordination helps good guys. Exploit details may not (CVE-2010-3962)




CVE-2010-3962 Attack Attempts

Computers Per Day by Target OS

as of 12/8/2010 midnight GMT

Oct 28 – First report of targeted attack

Nov 3 - Microsoft Advisory (coord. with Symantec)
MAPP guidance
VUPEN PoC

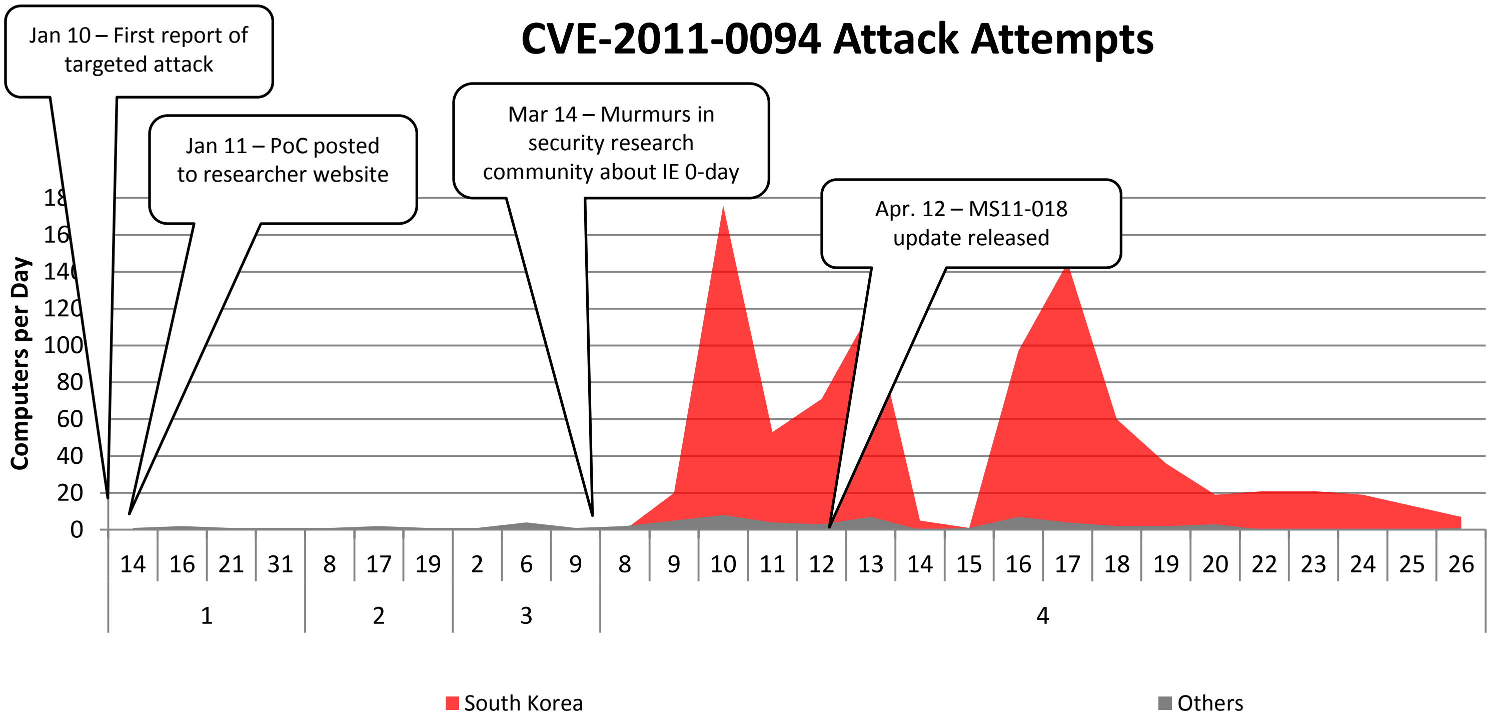
Nov 5– Exploit-DB PoC

Nov 9– News reports that exploit is integrated into Eleonore exploit toolkit

Dec 14– MS10-090 update released

Example: Quiet coordination for targeted attack may delay copycat attacks (CVE-2011-0094)

- One reported target in Jan.
- All quiet until weekend before update



Why Coordinate?

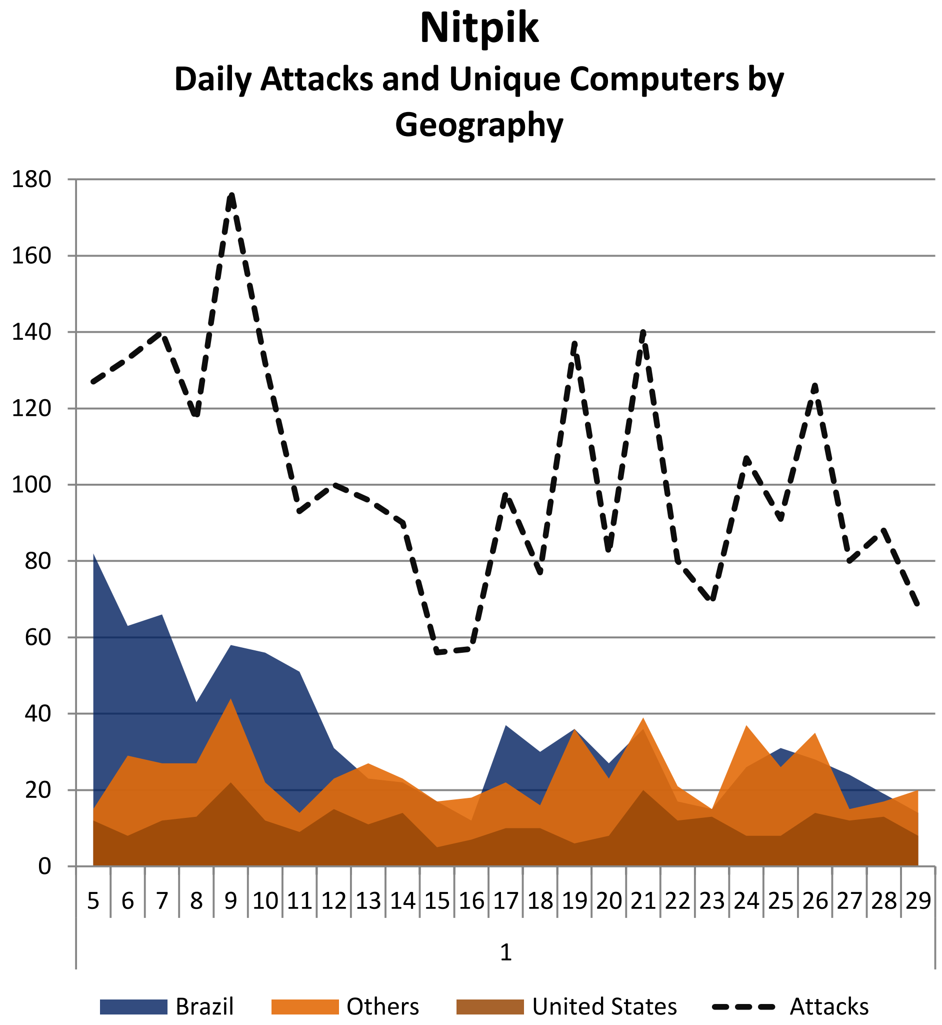
- The point of disclosing is to provide **actionable** advice to potential victims.
- Even if you can’t wait for a long time, the software vendor can help develop higher quality advice.
- The vendor is best positioned to ensure that the users of the product are informed about that advice.
- The vendor may be best positioned to ensure that the exploitation is **real.**

Real Exploitation is NOT…

- Researchers testing PoCs
- Unintentional exploitation
  - Malformed packets
  - Malformed documents
  - Fuzzed files found to exploit the vulnerability
  - Poorly-written code

Example (Non-Malicious): the Unintentional Exploit

- "Exploit" was the result of bad code, didn't execute code
- Paired with successful, but older vulnerability (update already available)



Exploitation disclosure AFTER vulnerability disclosure

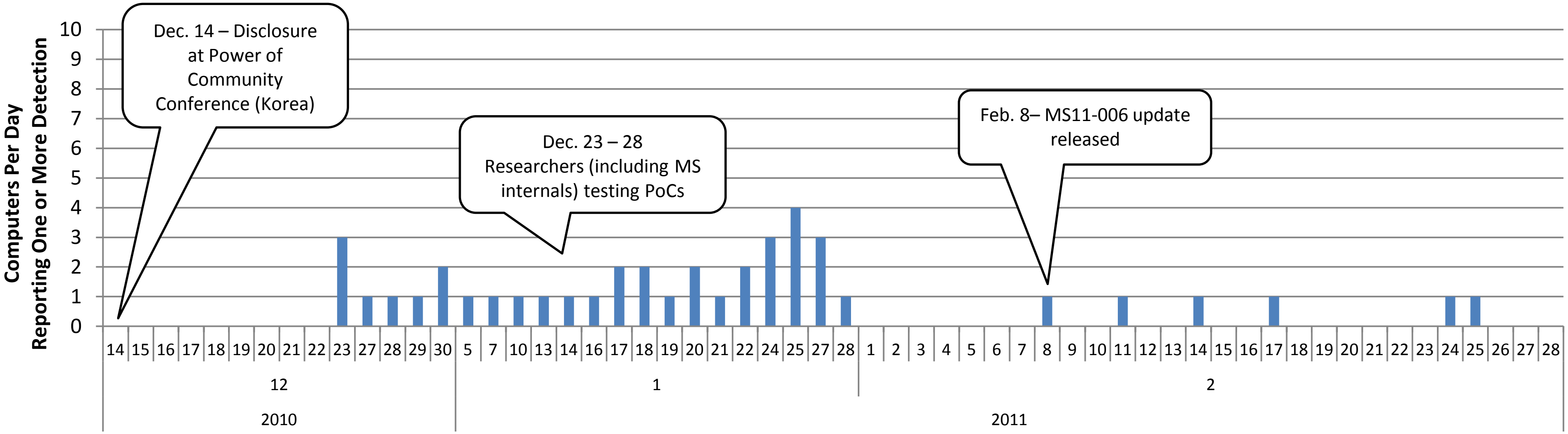
Hey, the vulnerability has already been disclosed, so disclosing the fact that exploitation is occurring can’t hurt, can it?

If a fix is not yet available, reports of exploitation may draw attention to a vulnerability.

Example (Non-Malicious): Researchers

- CVE-2010-3970
  - “Public disclosure” of a vulnerability sometimes results in little or no exploitation because the disclosure wasn’t prominent enough.
  - “If a tree falls in a forest…”

CVE-2010-3970



Dec. 14 – Disclosure at Power of Community Conference (Korea)

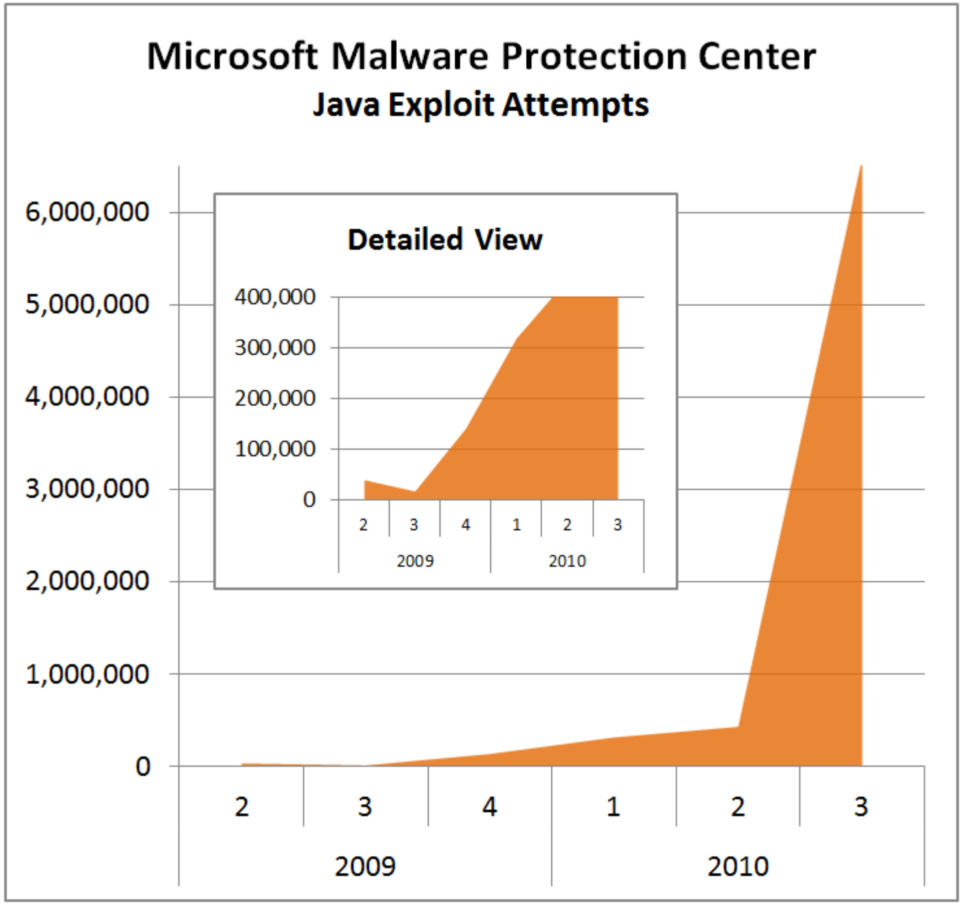
Dec. 23 – 28 Researchers (including MS internals) testing PoCs

Feb. 8– MS11-006 update released

When a fix IS available, coordination can help ensure that public reports make reference to the correct fix information.

Example: Coordination is beneficial even when vulns are well-known

- Analysis of security intelligence data revealed large spike
- Journalists had noted success rate of Java exploits in some toolkits
- Exploits were for known, updated Java vulnerabilities
- There is a need to include the right update information in exploitation reports.



Got a Workaround instead of a fix? Is it really actionable?

- Sometimes it makes sense to disclose a workaround when a fix is not yet available, in particular when exploitation is taking place.
- Consider
  - How easy is it for organizations of different sizes to deploy?
  - Does it cripple functionality?
- If its hard to deploy or breaks something, some organizations won’t be able to deploy it.
- Premature disclosure could increase the risks faced by those organizations.

Conclusions

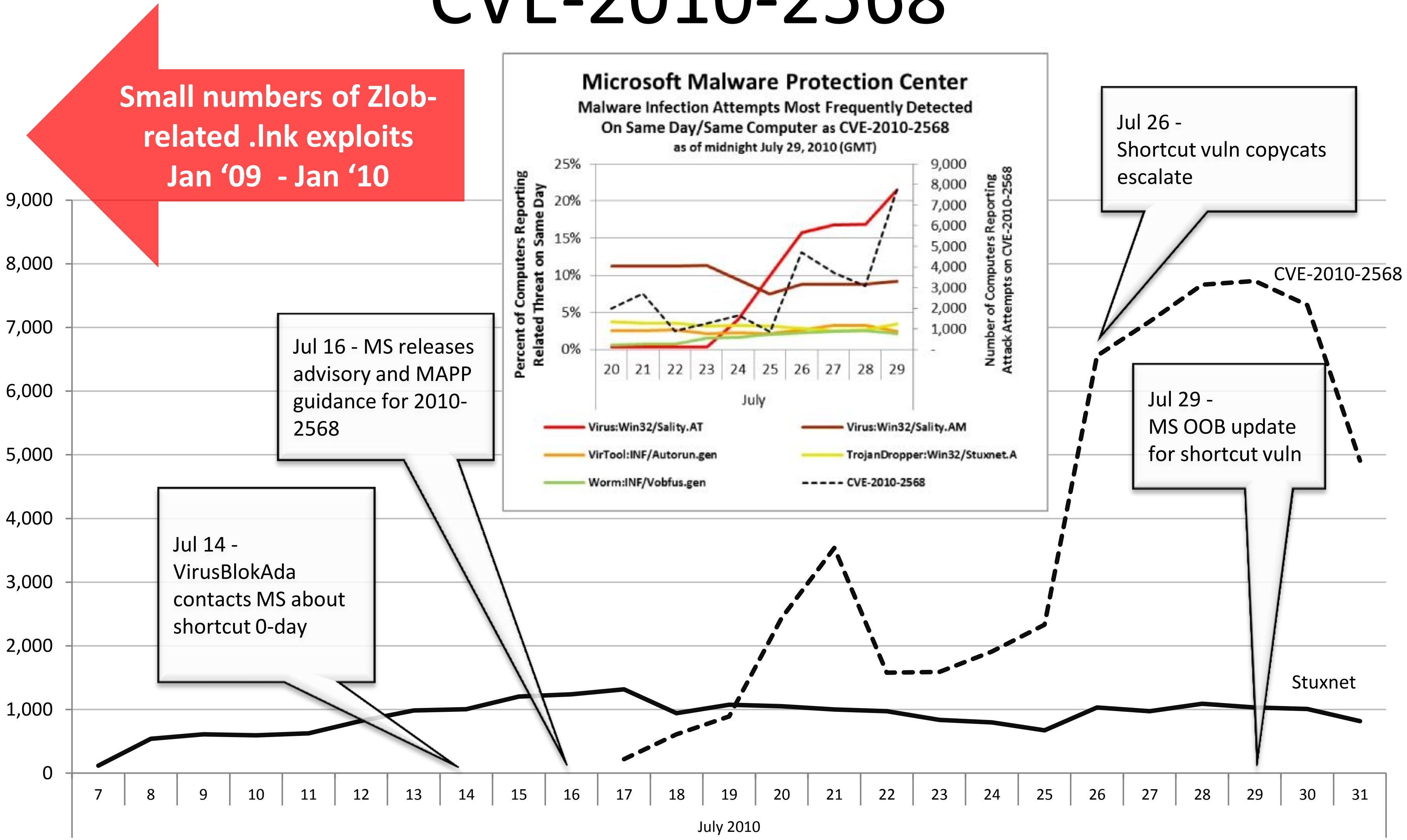
When to disclose exploitation?

- Disclosure can accelerate exploitation.
- Disclosure is most beneficial when it is coupled with **actionable** information.
- The moment to disclose is when the benefit of attracting attention to that actionable information exceeds the harm of attracting attention to the opportunity represented by the vulnerability.

Balancing the Exploitation Disclosure Variables

- Vulnerability is known or unknown?
- Availability of an update or workaround?
- Is the workaround widely actionable?
- Level of exploitation
  - Targeted – Focused on a specific organization or perhaps a small collection of specific entities.
  - Limited – Low in number, could be predominantly affecting one region or industry.
  - Broad – Indiscriminate targets crossing geolocations
- Exploitation is confirmed malicious and not just a POC circulating
- Detection levels associated with circulating exploits

Example: Variables can be complicated CVE-2010-2568


Small numbers of Zlob-related .lnk exploits Jan ‘09 - Jan ‘10

Jul 14 - VirusBlokAda contacts MS about shortcut 0-day

Jul 16 - MS releases advisory and MAPP guidance for 2010-2568

Jul 26 - Shortcut vuln copycats escalate

Jul 29 - MS OOB update for shortcut vuln

General Guidelines for Exploitation Disclosure

	0-Day (Vuln Unknown, No Update)	Known, No Update or Workaround	Known, Workaround available but no Update	Known, Update available
Targeted	Coordinate and wait for updates	Coordinate and wait for updates	Coordinate and wait for updates	Coordinate, but don’t wait
Limited	Coordinate and confirm it	Coordinate, maybe wait	Coordinate, maybe wait	Coordinate, but don’t wait
Broad	Coordinate, but don’t wait	Coordinate, but don’t wait	Coordinate, but don’t wait	Coordinate, but don’t wait

These are general guidelines but the specifics of a particular situation may require different actions, particularly in cases where only a workaround is available and depending on how actionable that workaround really is.

Vendor coordination is always beneficial

- Talk to the affected vendor before you post
  - They may provide remediation and workaround information you don't have.
  - They can be prepared to provide guidance to their customers.
  - Your telemetry data helps prioritize updates
- Be patient
  - Some vulnerabilities can be difficult to remediate
  - There are many factors influencing prioritization of remediation
  - Vendors can build trust by
    - Communicating the factors impacting their remediation schedule
    - Publicly crediting organizations who cooperate with them in coordinating vulnerability and exploitation disclosure

When you publish

- Put hashes (MD5, SHA1, etc…) of the malware samples you've seen in blog posts to help vendors with identifying samples and sample detection

- Avoid providing exploit details that might help copycat attackers

- Include the CVE or go back and add it later if it is not assigned at the time that you publish

- Reference the specific product updates or workaround information for the vulnerabilities in question

Call to Action

- If you are or work with researchers
  - Coordinate!
- If you were the target of an 0-day
  - Coordinate! (and urge any involved security vendors to do the same)
- If you are blogging, writing, publishing details about exploitation
  - Coordinate!
  - Include all the relevant details in your post (hashes, CVEs, availability of updates)

Thank You

- Questions?