RSACONFERENCE2013

Security in knowledge

Real Time Forensics: Uncover the culprit while the body is still warm

Bruce Snell
McAfee

Session ID: SPO2-W23B

Session Classification: General Interest

What do we accomplish with Forensics?

- Find out what was damaged/stolen
- Find out what attack was used
- Find out where data was sent
- Recovery of compromised systems

What do we accomplish with Forensics?

- Find out what was damaged/stolen
  - Know who we need to notify
  - Recover lost/damaged systems
  - Better prepare defense for next time

Well, next time someone uses that attack we will certainly be prepared!

What do we accomplish with Forensics?

- Find out what was attack was used
  - Reporting
  - Otaku factor

Hey, that was actually the Citadel worm that ripped through our systems...isn't that cool?

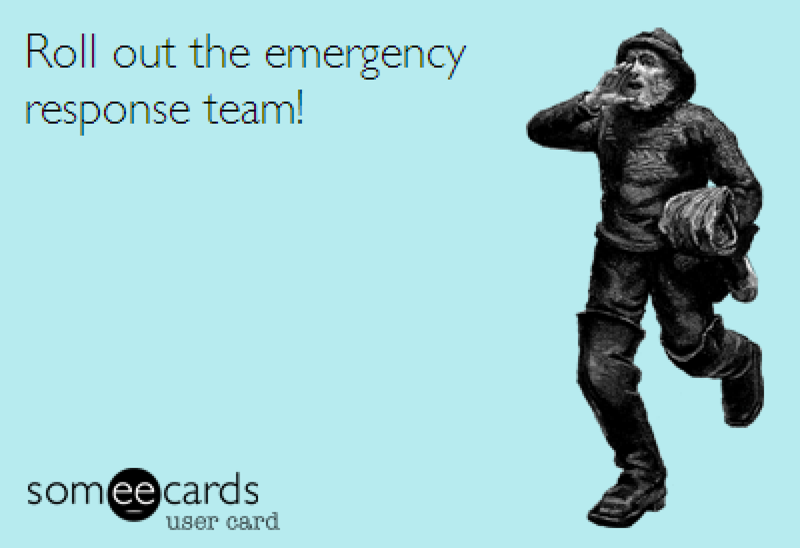
What do we accomplish with Forensics?

- Find out where the data was sent
  - Aid in investigation by authorities
  - Strengthen defense against future attacks

Hang on, let me start a report running so we can figure out who we should block, should only take an hour or so

What do we accomplish with Forensics?

- Recovery of compromised systems
  - Identify which systems are impacted
  - Costly physical recovery typically needed



What would it take…

- …to provide real time forensics?

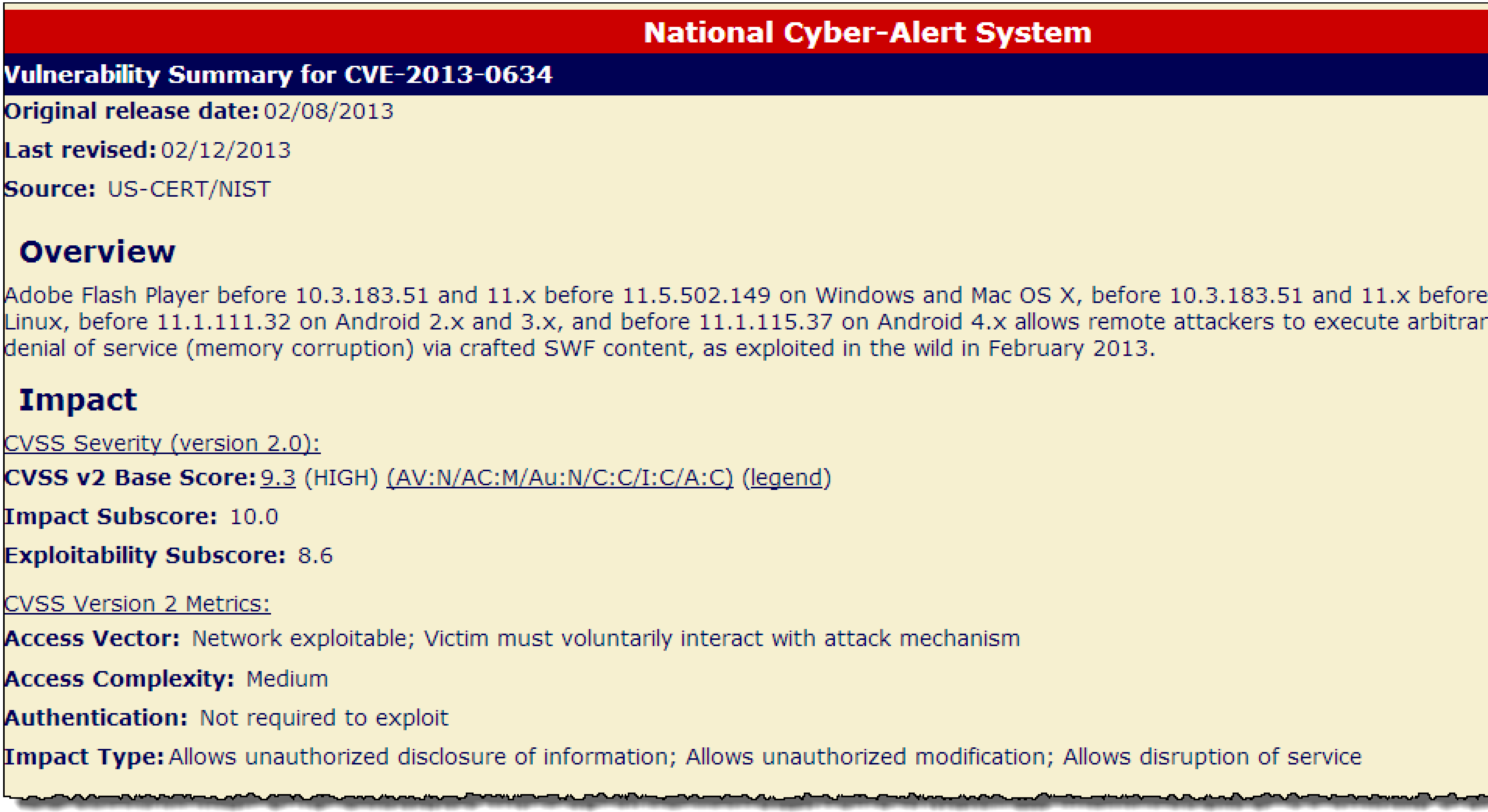
Can you grab data from…

- Every machine?
  - In your entire Enterprise
    - With the exact state information?
- Go!

Scenario…

- Multiple vulnerabilities exposed in Adobe Flash
  - CVE-2013-0633
    - Used in targeted attacks, disguised as Word email attachment
    - Contains malicious Flash content
    - Buffer overflow
  - CVE-2013-0634
    - Exploit reported by Lockheed Martin, MITRE and others, suggesting targeted industrial espionage
    - Memory corruption

How do you react?



National Cyber-Alert System

Vulnerability Summary for CVE-2013-0634

Original release date: 02/08/2013

Last revised: 02/12/2013

Source: US-CERT/NIST

Overview

Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before
Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrar
denial of service (memory corruption) via crafted SWF content, as exploited in the wild in February 2013.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

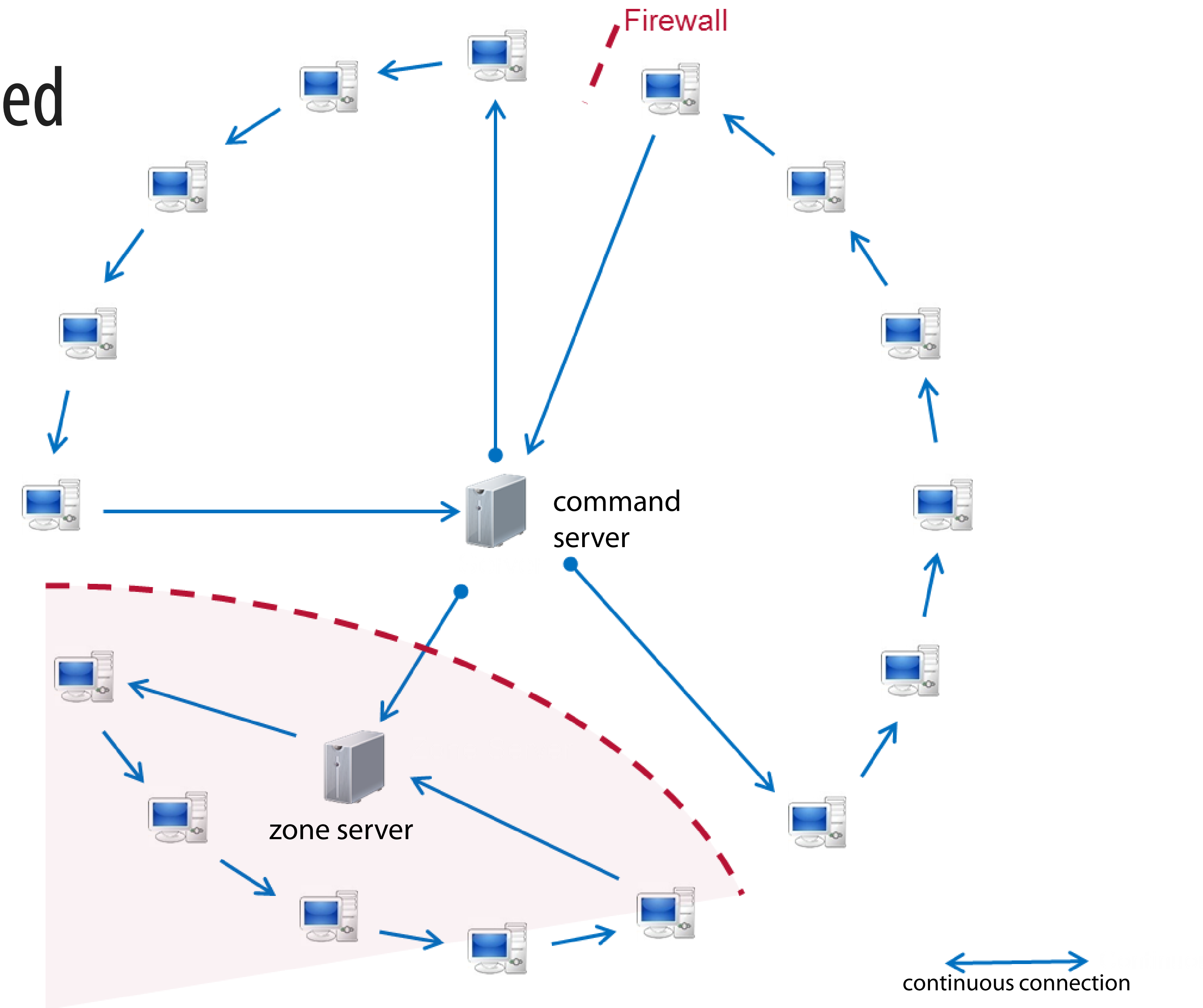
Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Demo

P2P Speed


Firewall
command server
zone server
continuous connection

Questions?