Microsoft | Malware Protection Center

Top Exploits of 2011

Holly Stewart
Senior Lead, Response and Threat Intelligence

The MMPC and ME

- Microsoft Malware Protection Center (MMPC)
  - Antivirus research and industry collaboration
  - Threat data from over 600 million systems worldwide
    - Microsoft Malicious Software Removal Tool (MSRT)
    - Microsoft Security Essentials
    - Forefront Endpoint Protection
- Holly Stewart (ME)
  - Manage Response Coordinators
  - Critical response processes
  - Microsoft Active Protections Program (MAPP)
  - Microsoft Security Intelligence Report

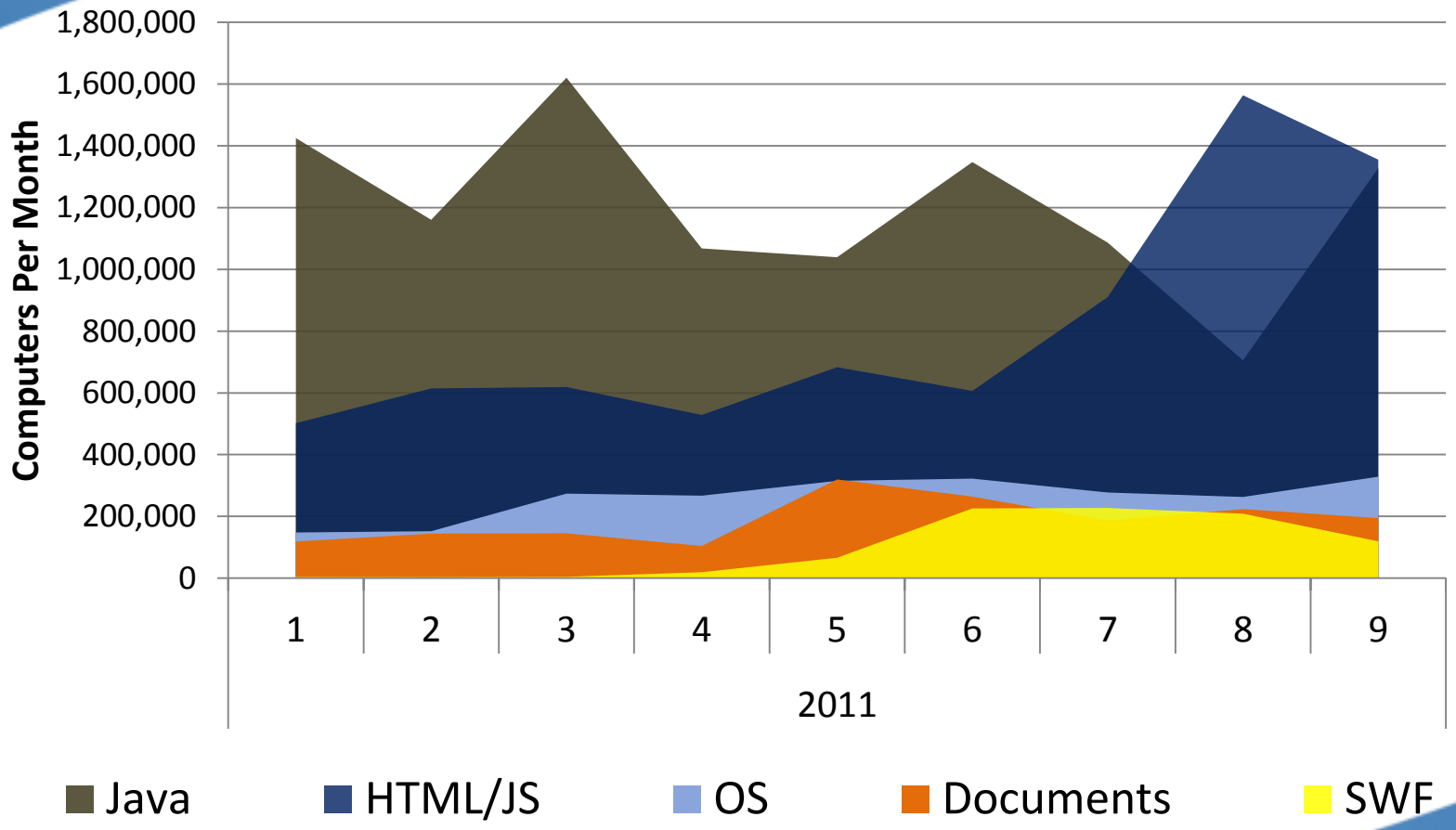
About the Data in this Report

- Tens of millions of real-time endpoint protection installations
  - Forefront & Security Essentials
  - Corporate & Consumer
- Data represents exploitation attempts
  - Not infections!
  - Generally counted monthly by number of unique computers encountering an exploit family
- 100% of the vulnerabilities discussed in this presentation have updates available (now)

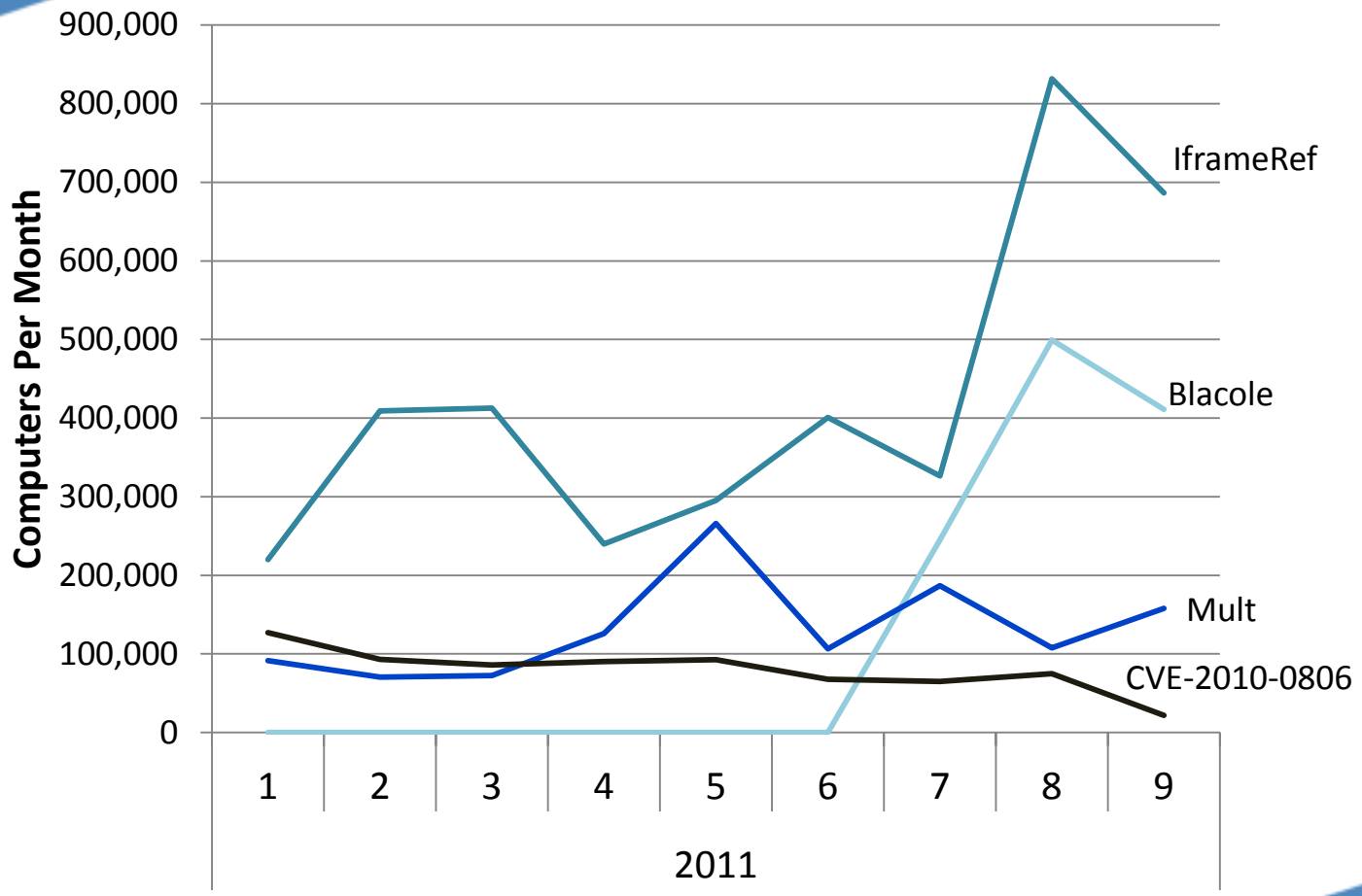
Objectives

- Most frequently targeted class of vulnerability
- Specific vulnerabilities that are most frequently exploited
- Differences in the corporate and consumer environments
- Geographical differences

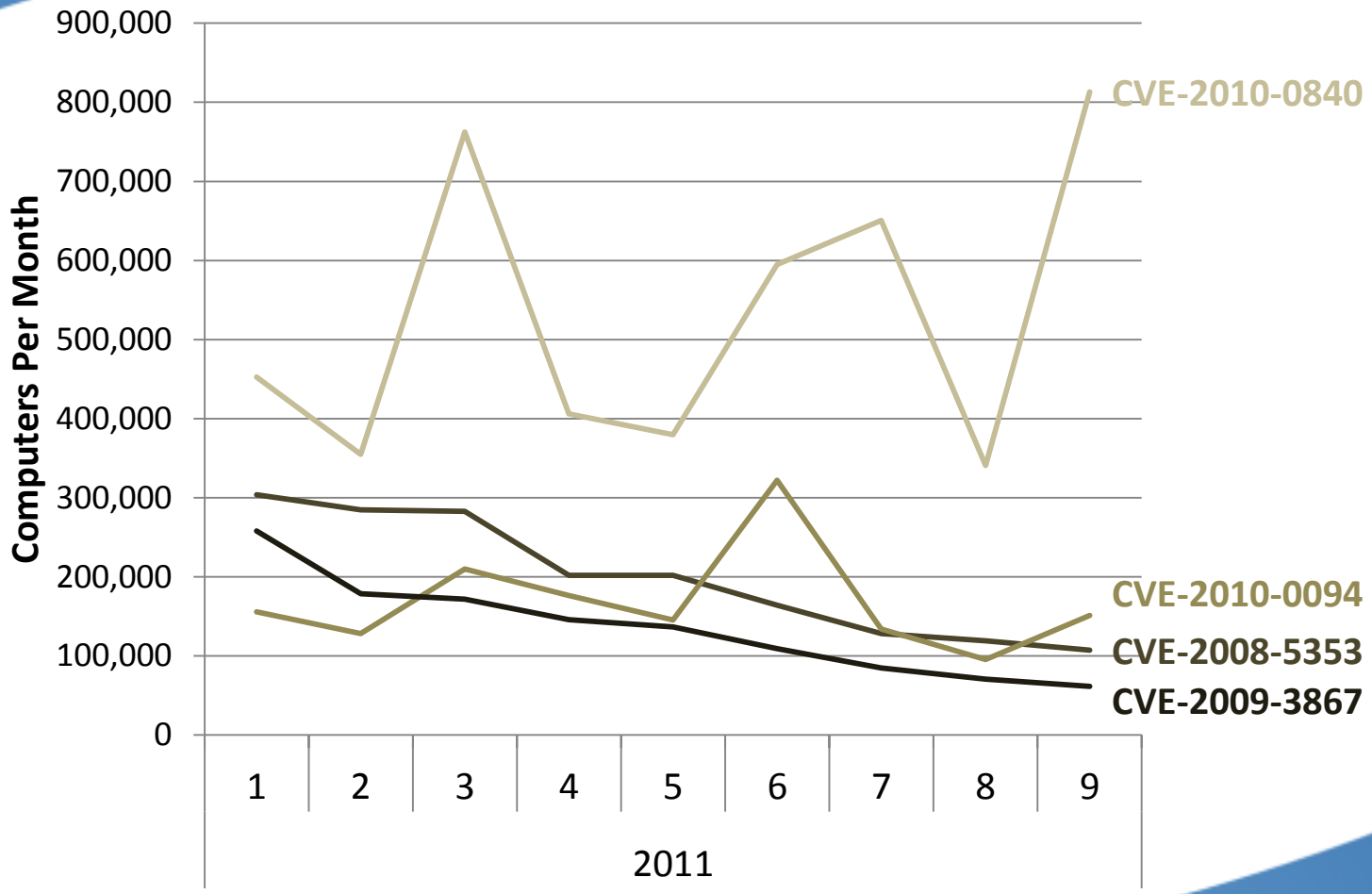
Exploitation Category Trends



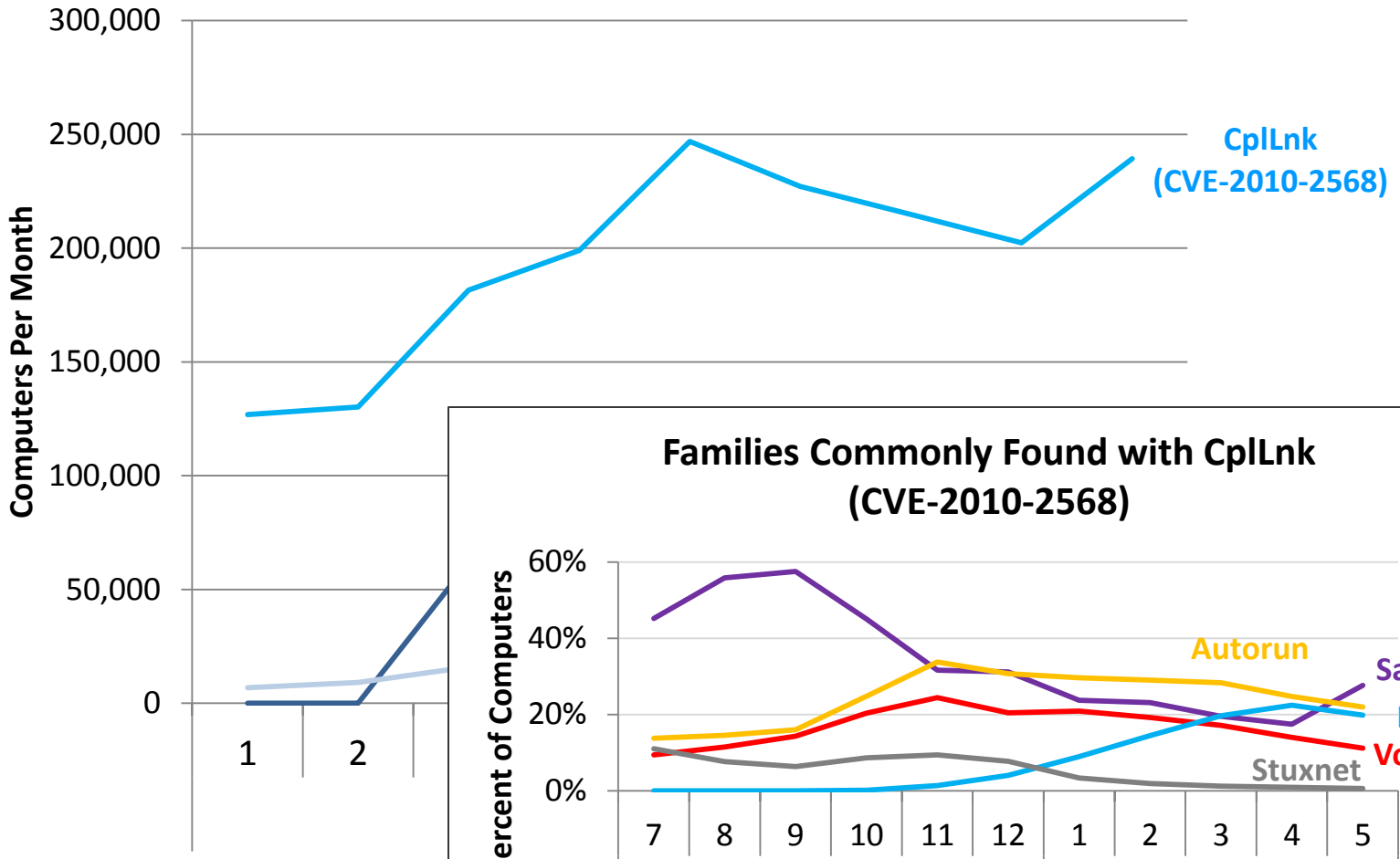
Top Families in HTML/JS (93%)



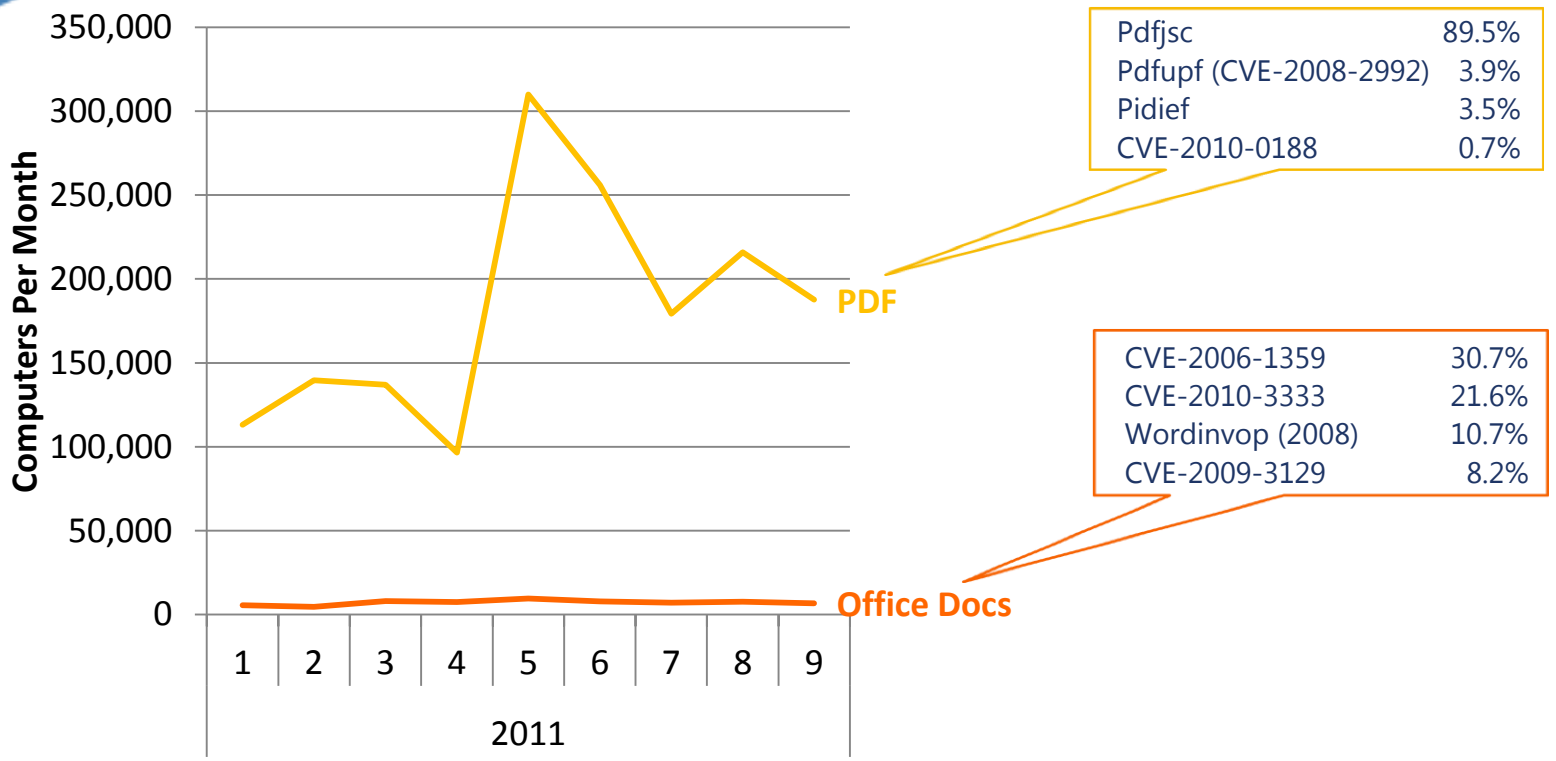
Top Java Exploit Families (86%)



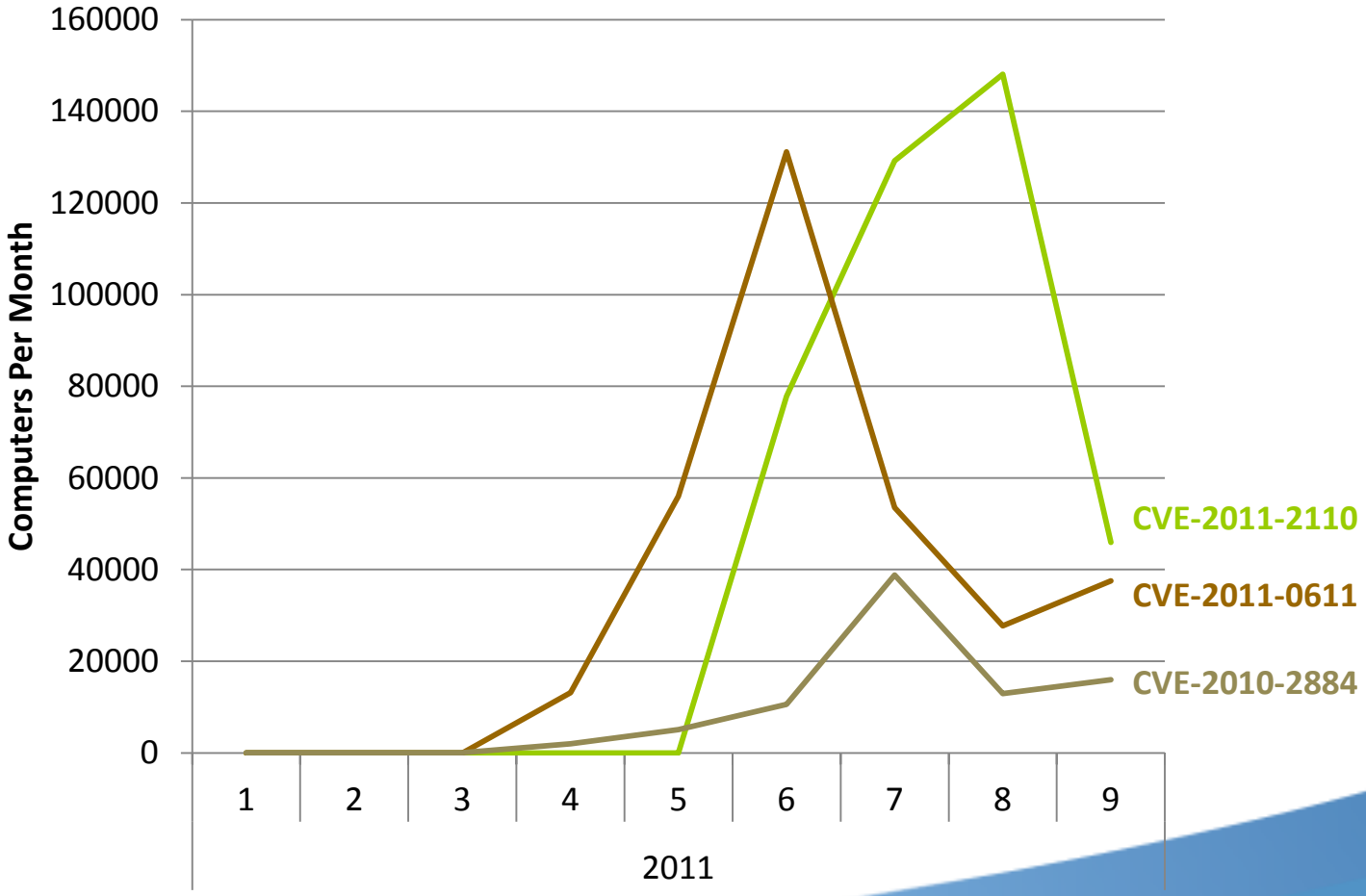
Top Operating System Exploits (93%)



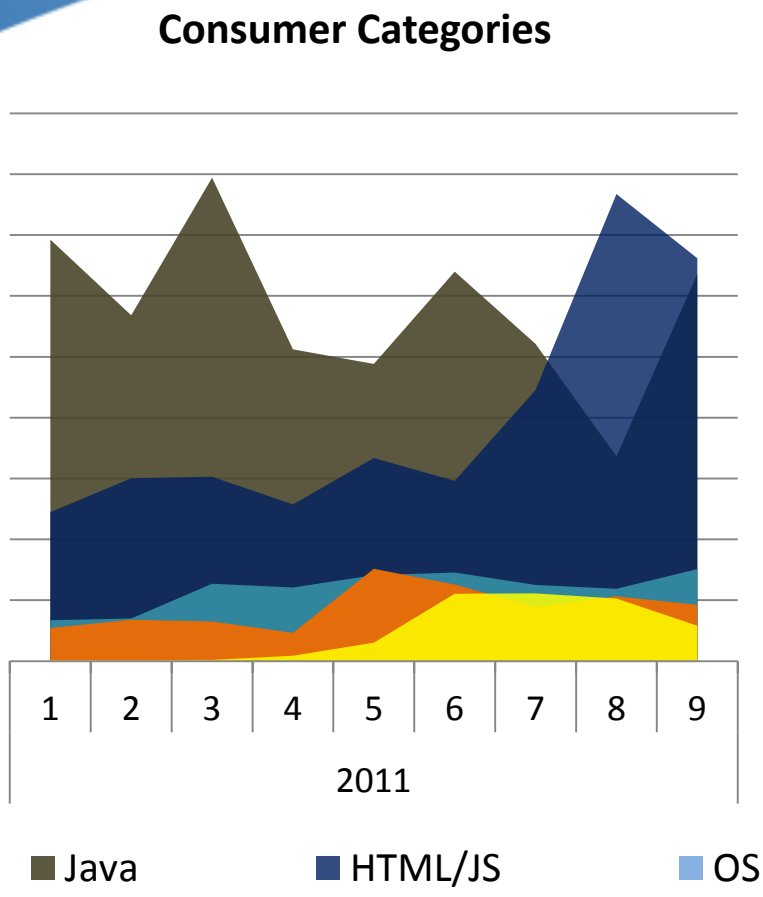
Top Document Exploits (99.9%)

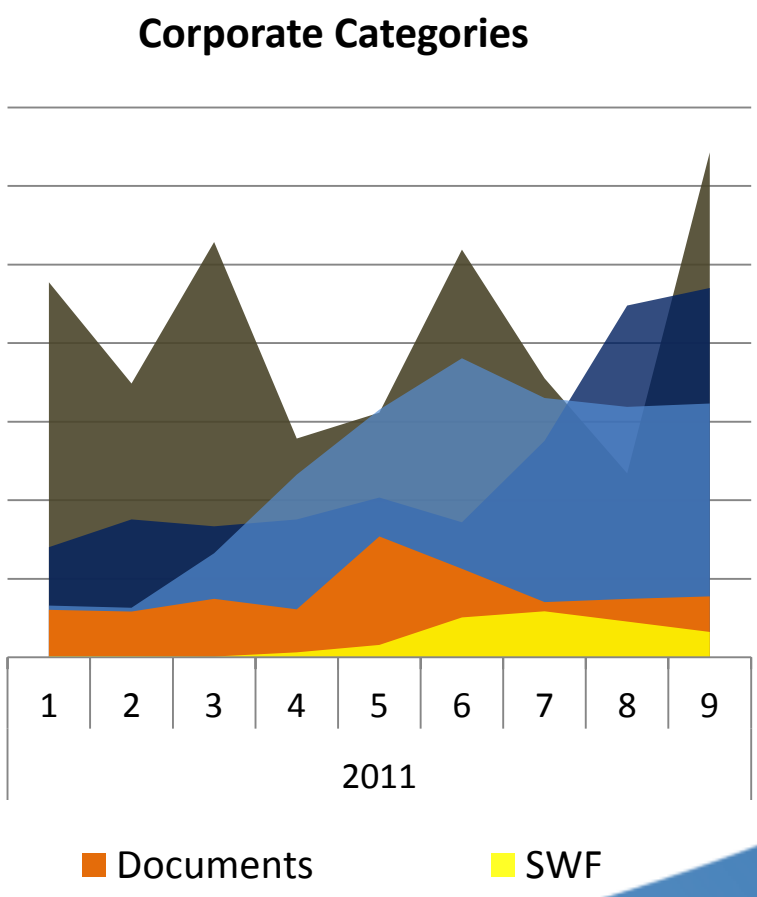


Top SWF Exploits (92%)



Categories: Consumer/Corporate



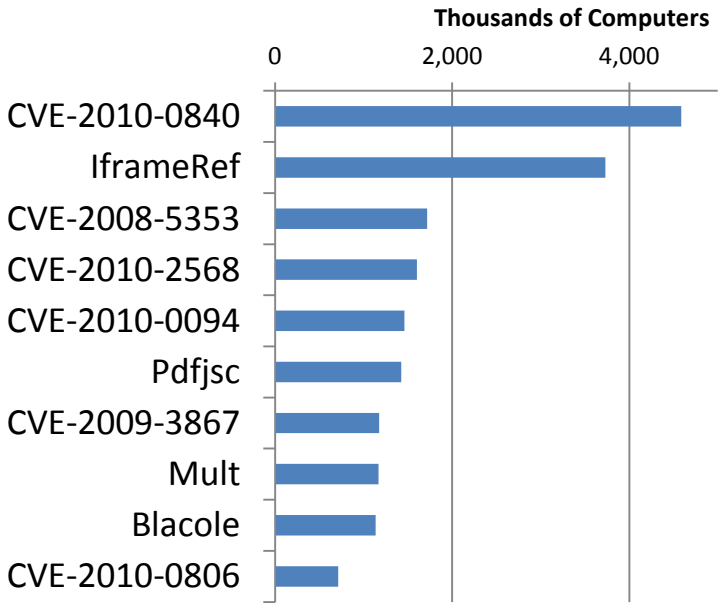


Top Exploits: Consumer/Corporate

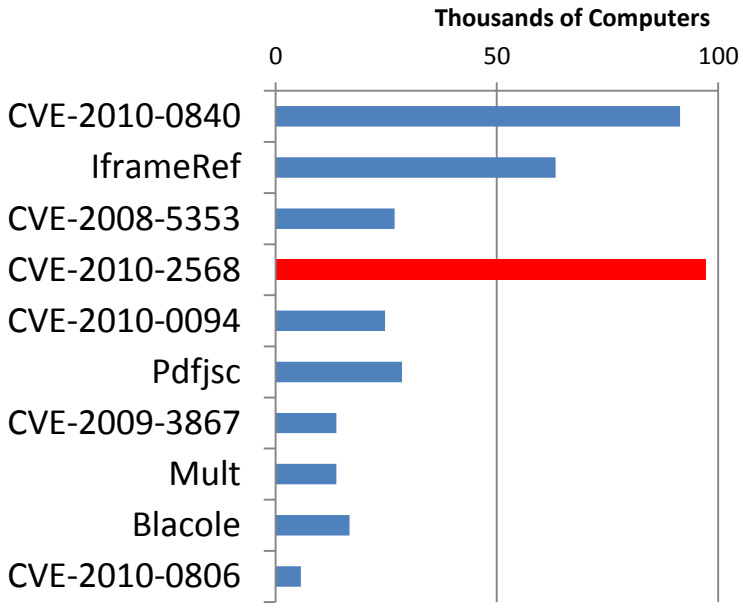
Top 10 Exploits

January – September 2011

Consumer



Corporate



Geographical Differences

- Consumer data
- At least 20k computers per location
- % of computers encountering at least one exploit/month

Location	Average	Location	Average	Location	Average
Worldwide	*3.1%*	Morocco	1.6%	Ecuador	2.6%
Czech Republic	0.8%	Hong Kong	1.6%	Saudi Arabia	2.6%
Japan	0.9%	Chile	1.6%	Iran	2.7%
Slovenia	1.0%	South Africa	1.7%	Turkey	2.9%
Slovakia	1.1%	Malaysia	1.7%	Peru	3.0%
Taiwan	1.2%	Costa Rica	1.7%	Jordan	3.2%
Bulgaria	1.2%	Philippines	1.8%	Canada	3.2%
Argentina	1.3%	Serbia	1.8%	Hungary	3.3%
Finland	1.3%	Kuwait	1.8%	United Kingdom	3.4%
Israel	1.3%	Qatar	1.8%	United States	3.6%
Croatia	1.3%	China	1.8%	Thailand	3.6%
Puerto Rico	1.3%	Colombia	1.8%	Ukraine	3.6%
Poland	1.3%	Greece	1.9%	Nigeria	4.1%
Lithuania	1.4%	Mexico	2.0%	Russia	4.2%
Denmark	1.4%	Belgium	2.0%	India	5.1%
Switzerland	1.4%	Ireland	2.0%	Portugal	5.5%
Austria	1.4%	Dominican Republic	2.0%	Brazil	6.7%
Estonia	1.4%	Spain	2.1%	Vietnam	7.5%
Romania	1.4%	Italy	2.1%	Pakistan	8.6%
Sweden	1.4%	Venezuela	2.1%	Indonesia	17.0%
New Zealand	1.4%	Egypt	2.4%	Korea Rep.	19.8%
France	1.5%	Netherlands	2.4%		
Norway	1.5%	Germany	2.4%		
Singapore	1.5%	Australia	2.5%		
Latvia	1.6%	United Arab Emirates	2.5%		

Geographies Reporting Greatest Exploitation

Location	1	2	3	4	5	6	7	8	9	Average
Worldwide	*3.2%*	*4.2%*	*3.2%*	*2.2%*	*2.6%*	*3.1%*	*2.8%*	*3.1%*	*3.3%*	*3.1%*
Korea Rep.	8.8%	6.9%	10.3%	15.8%	26.9%	27.2%	34.9%	27.9%	19.8%	19.8%
Indonesia	17.8%	26.4%	17.6%	17.5%	18.3%	16.0%	14.7%	12.2%	12.9%	17.0%
Pakistan	9.1%	14.8%	7.4%	7.5%	8.2%	7.8%	7.8%	7.1%	8.1%	8.6%
Vietnam	5.5%	7.0%	7.3%	8.2%	9.3%	8.5%	7.0%	7.0%	7.7%	7.5%
Brazil	4.1%	12.0%	8.3%	4.7%	5.6%	7.9%	5.4%	6.5%	5.4%	6.7%

- Korea – Adobe Flash exploitation
- Indonesia, Pakistan, Vietnam – CplLnk (CVE-2010-2568)
  - + India + Mexico = 52% (AVE) of all computers reporting CplLnk
- Brazil - IframeRef

Geographies Reporting Least Exploitation

Location	1	2	3	4	5	6	7	8	9	Average
Worldwide	*3.2%*	*4.2%*	*3.2%*	*2.2%*	*2.6%*	*3.1%*	*2.8%*	*3.1%*	*3.3%*	*3.1%*
Czech Republic	0.9%	1.2%	0.7%	0.5%	0.6%	0.6%	0.7%	0.9%	1.1%	0.8%
Japan	0.4%	0.7%	0.5%	0.4%	1.4%	2.1%	0.7%	1.1%	0.6%	0.9%
Slovenia	1.1%	1.4%	0.9%	0.8%	0.9%	0.9%	0.7%	1.2%	1.4%	1.0%
Slovakia	1.2%	2.2%	1.0%	0.7%	0.9%	0.7%	0.9%	1.0%	1.1%	1.1%
Taiwan	1.3%	1.5%	1.3%	1.3%	1.1%	1.2%	0.8%	1.0%	0.9%	1.2%

- Lower prevalence of CplLnk (2010-2568) exploitation
  - Czech Republic, Japan, Slovakia, Taiwan
- Japan
  - CplLnk, 2010-0094, 2010-0806
- Slovenia
  - Exploitation profile similar to global average, just less!
- Taiwan
  - CplLnk, 2008-5353, 2009-3867

Key Observations

- Yes, 0-days are scary, but…
  - Vulnerability exploitation continues, and in most cases, increases in immense volumes ***after*** updates have been released.
    (Apply the update available folks!)

- Most targeted technologies are:
  - Java platform software
  - Adobe Acrobat and Adobe Reader
  - Adobe Flash Player
  - Browsers, ActiveX, and plug-ins
  - Some operating systems
    - First time a mobile OS has come to the surface in our data
    - Apply MS10-046 to protect against CplLnk exploitation

Questions?