BLADE:

An Attack-Agnostic Approach for Preventing Drive-By Malware Infections

Long Lu[1], Vinod Yegneswaran[2], Phillip Porras[2], Wenke Lee[1]

[1] *Georgia Tech*

[2] *SRI International*

Oct. 6th, 2010

17th ACM Conference on Computer and Communications Security

Malware Propagation Facts

- One common path: the Internet

- Two fundamental approaches:
  - Drive-by download Vs. Social engineering

- Drive-by Download
  - most favored by today's attackers
  - Counts for more than 60% malware infections [ISC09, Dasiant10, Google10]

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

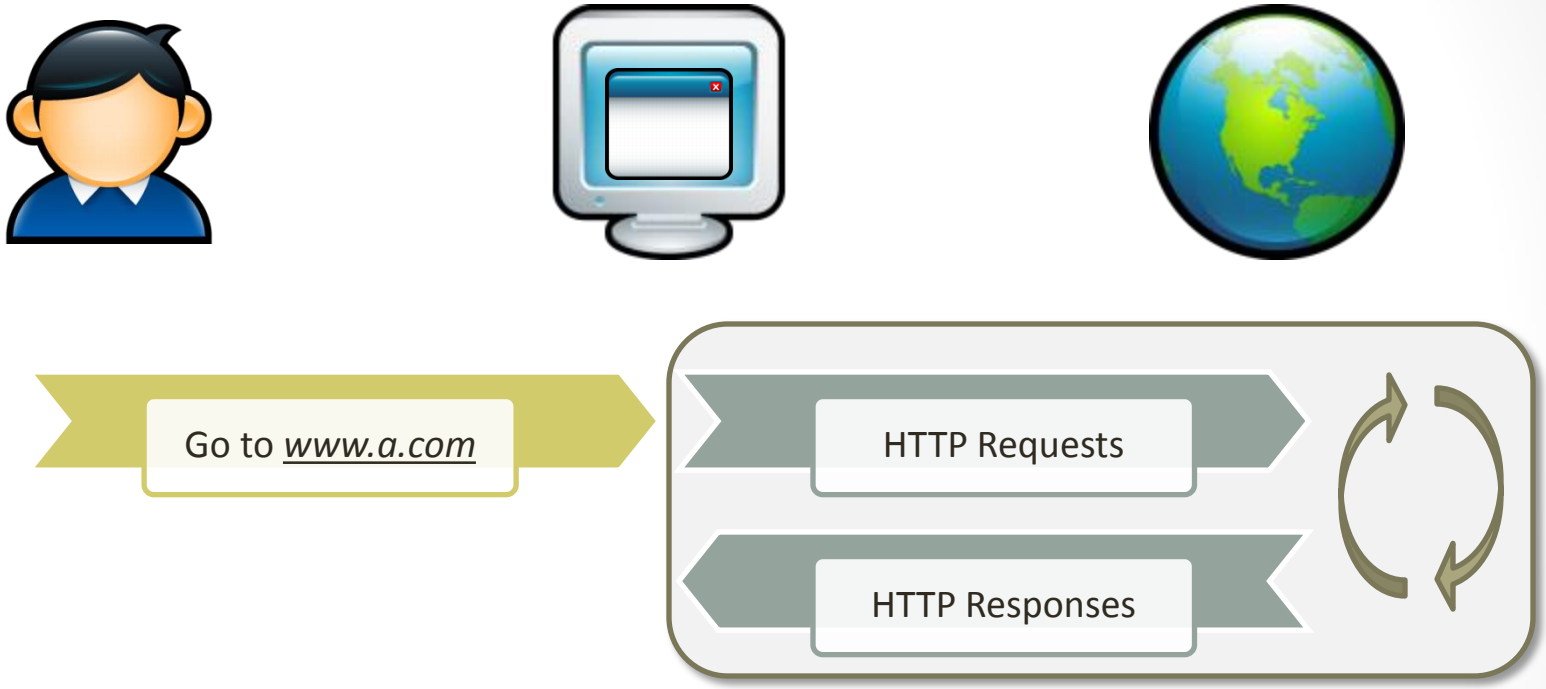
Drive-by Download

- **Definition:** ***Drive-by Download*** - *An attack in which the mere connection to a website results in the installation of a binary executable without the web-user's authorization.*

  - A click-then-infect scheme
  - Exploiting client-side vulnerabilities

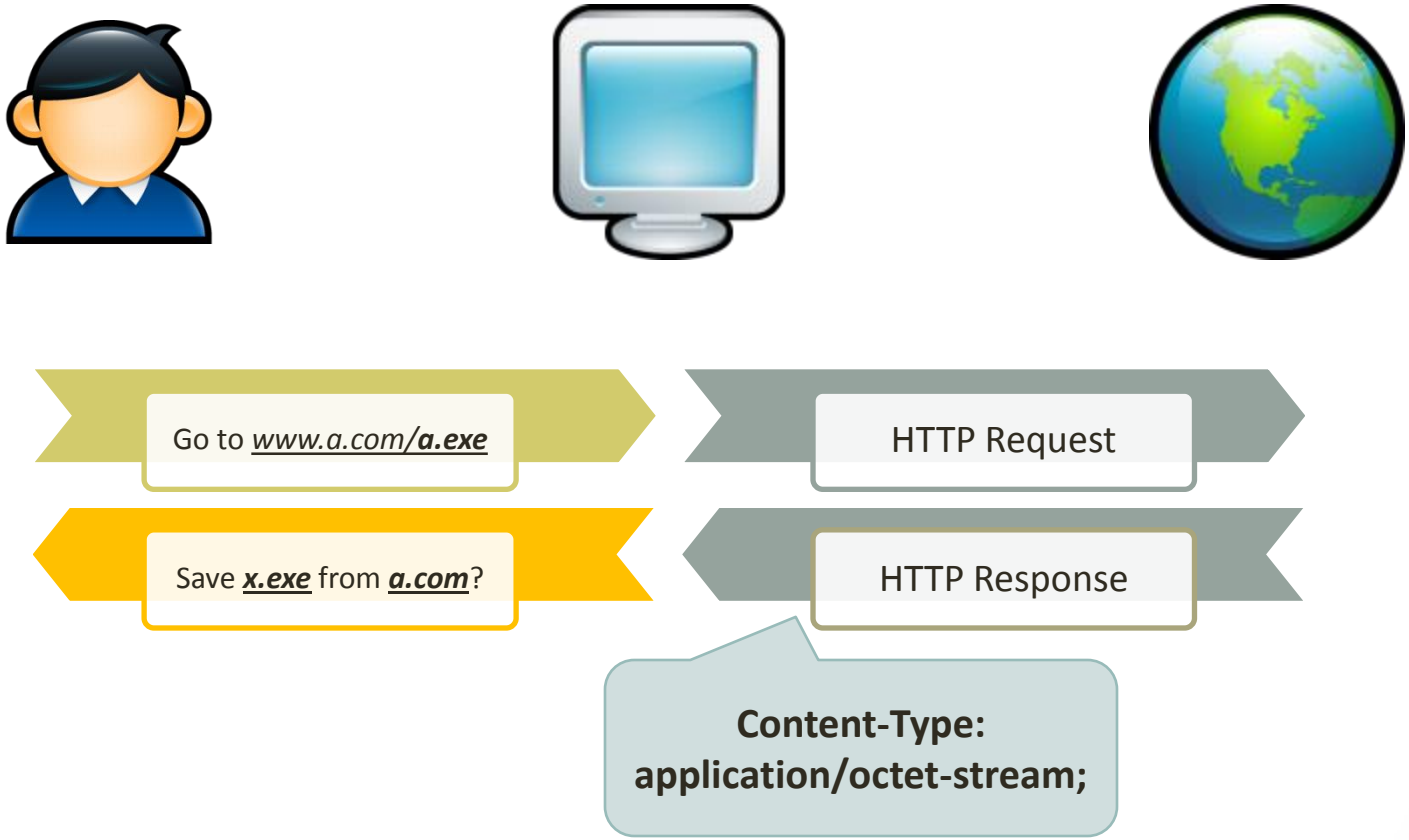
BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Regular browsing & downloading



Browser automatically saves and renders ***supported*** file types (*.html, *.js, *.jpeg, etc.)

Regular browsing & downloading



Browser asks for user consent before saving ***unsupported*** file types (*.exe, *.zip, *.dll, etc.)

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Drive-by download attack

Go to *www.compromised.com*

HTTP Requests

HTTP Responses

Requests without user's consent

Response from malware host

Essential steps:

1. **Exploit**
2. **Download**
3. **Execute**

No user consent required!

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Observations

Browsers handle

- ***supported content*** automatically
- ***unsupported content*** based on user's permissions

Golden Rule: *Browsers should never automatically download and execute binary files without user consent.*

All drive-by downloads inevitably break this rule.
No drive-by download will succeed if this rule holds.

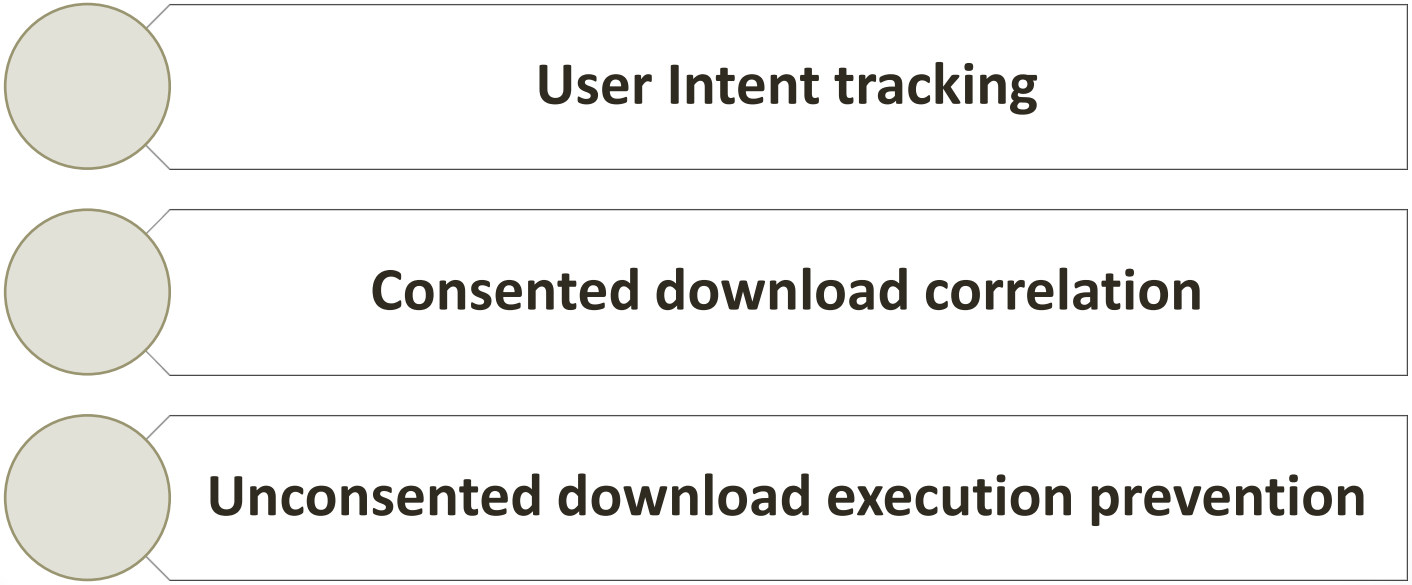
BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

BLADE Approach

- **Goal:** to eliminate drive-by malware infections
- **Approach:** unconsented execution prevention
  - Exploit and vulnerability agnostic
  - Browser independent

Essential steps:

1. **Exploit**
2. **Download**
3. ~~**Execute**~~



BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

BLADE Design

Assumptions

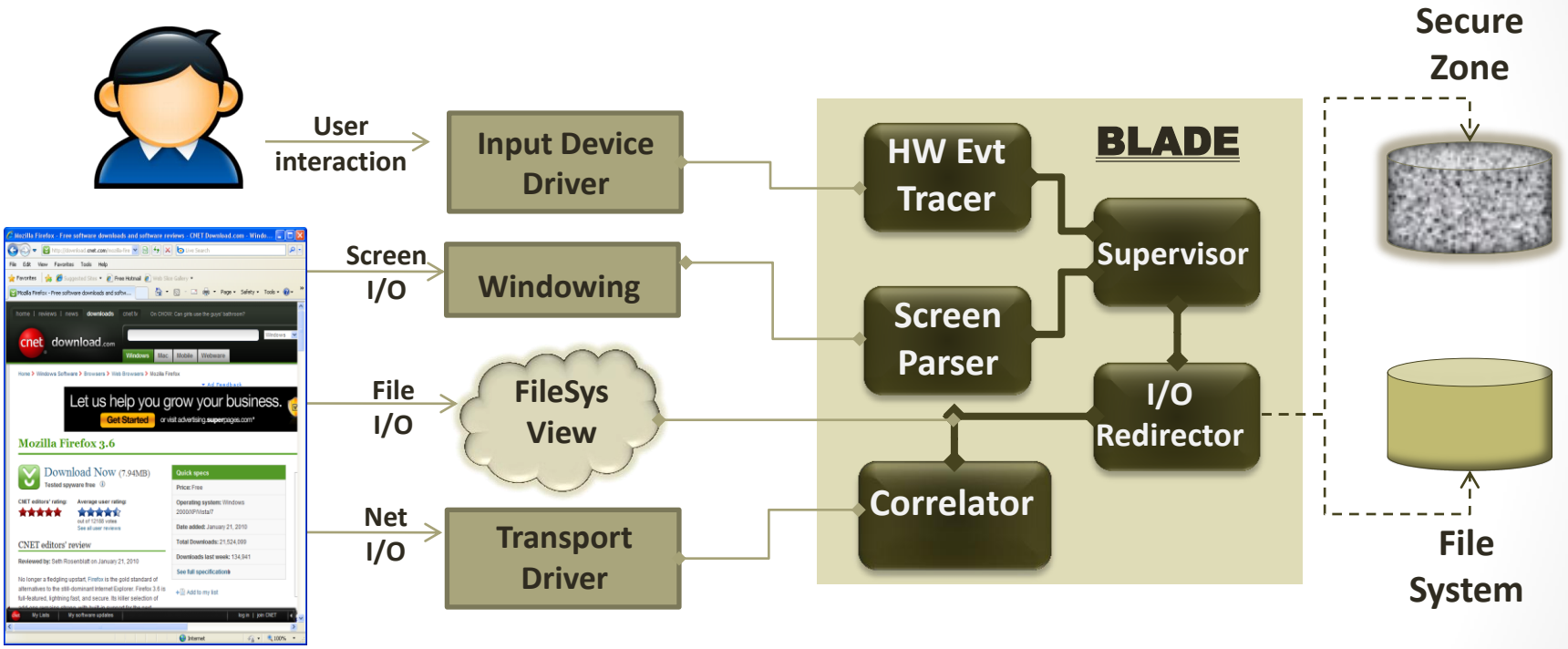
- Browsers may be fully compromised;
- OS is trusted;
- H/W is trusted.

Design choices

- BLADE is designed as a kernel driver;
- User intents are inferred from H/W and window events ;
- Consented download is correlated and verified;
- Unconsented download are contained in “SecureZone”.

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

BLADE Architecture



BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

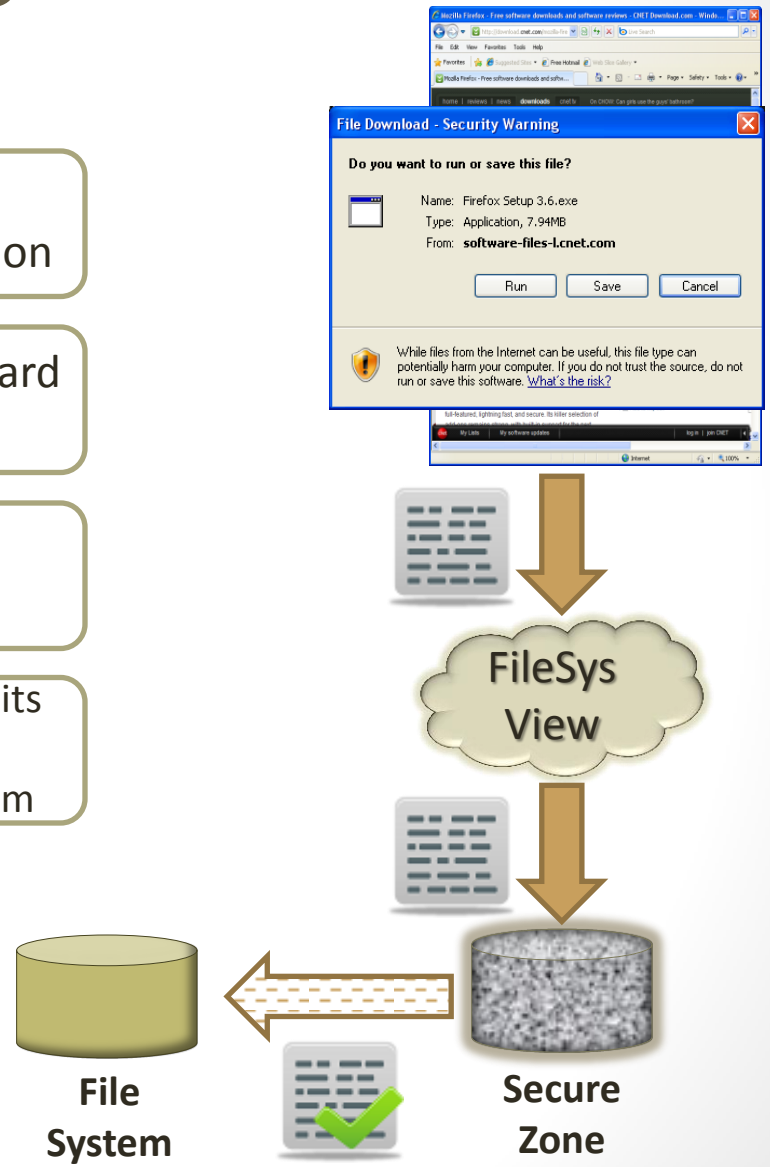
How it works – regular download

Screen Parser
- Locate consent button(s)
- Parse correlation information

H/W Evt. Tracer
- Monitor mouse and keyboard input

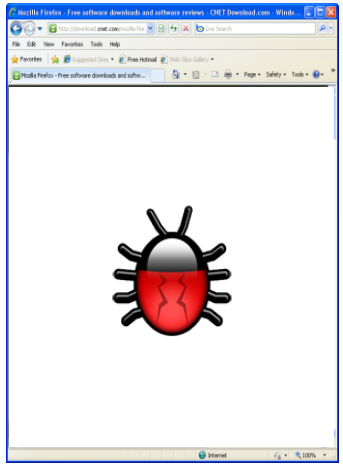
I/O Redirector
- Redirect disk writes from browsers

Correlator
- Discover candidate and verify its origin
- Map it to the regular file system



BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

How it works – drive-by download

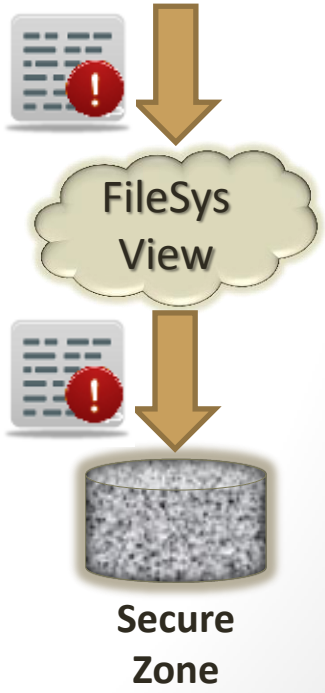


I/O Redirector

- Redirect disk writes from browsers

I/O Redirector

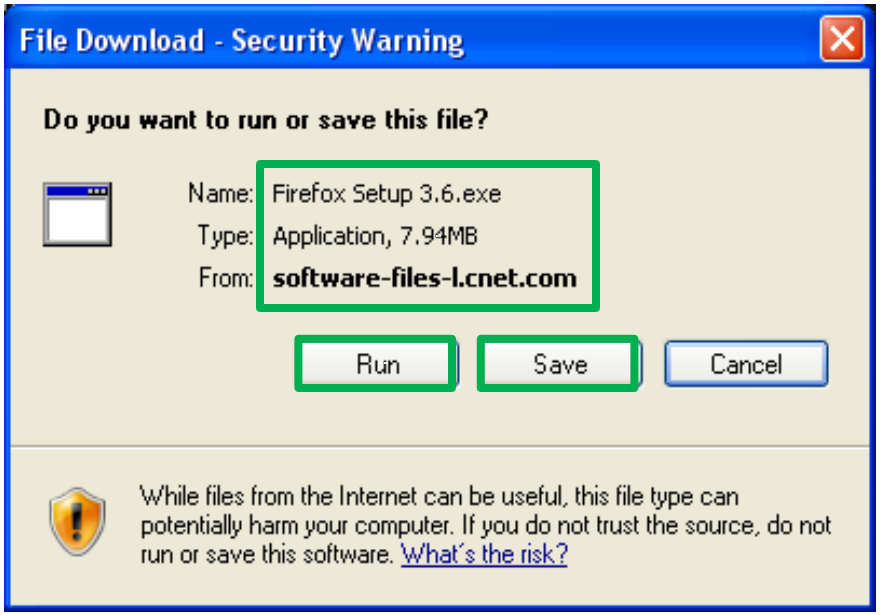
- Alert when execution is attempted



BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Implementations

- Screen Reader
  - Monitors certain windowing events
  - Parses internal composition of consent dialogues



BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Implementations

- H/W Event Tracer
  - Resides above device drivers
  - Listens to IRPs

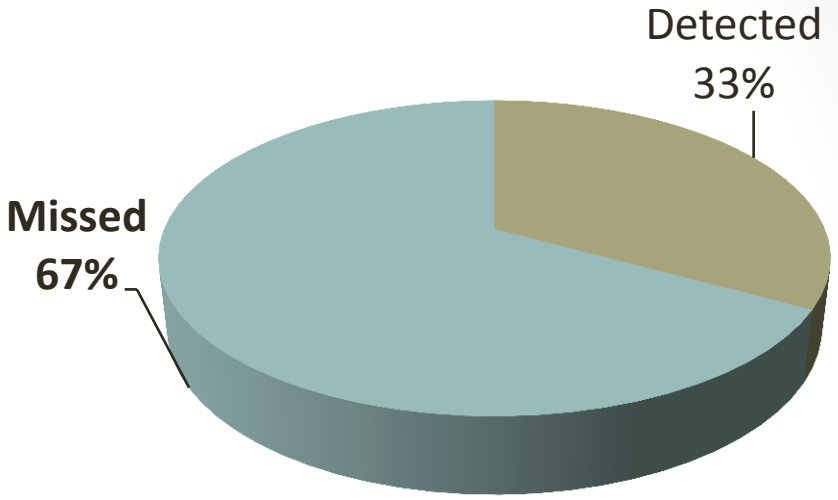
Implementations

- I/O Redirector
  - Built as a file system mini-filter
  - Redirects file accesses
  - Provides a merged view
- Correlator
  - Uses transport driver interface
  - Records streams coming from download sources
  - Content-base correlation and verification

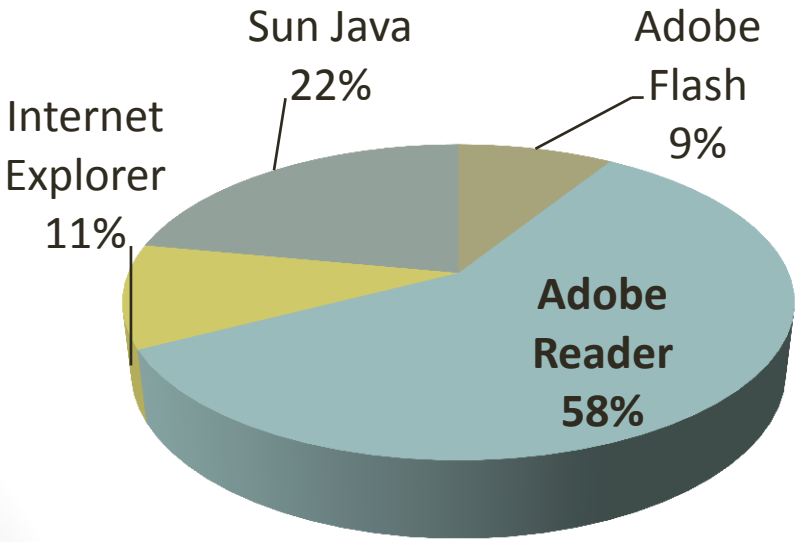
Empirical Evaluation

- An automated test bed
- Harvest new real-world malicious URLs daily
- VMs with various software configurations

Empirical Evaluation



VirusTotal Detection Rate



Most Targeted Applications

Attack Coverage Evaluation

- Using 19 specifically hand-crafted exploits
- Covering all common exploiting techniques
- Targeting at diverse vulnerabilities (11 zero-days)
- BLADE prevented all 19 infection attempts

ID	Exploit CVE-ID	Browser	Exploit Payload	Detected By Blade	Vuln. Notes
1	2006-3677	Firefox 1.5	Remote_shell_bind	YES	window.navigator
2	2005-1476	Firefox 1.5	Download_exec	YES	InstallTrigger.install()
3	2007-0038	Firefox 2.0	Download_exec	YES	LoadAniIcon()
			Dll_injection	YES	
4	2009-2477	Firefox 3.5	Download_exec	YES	TraceMonkey 0-day

Security analysis

- Potential ways to evade/attack BLADE

Spoofing attacks	• Fake GUI • Fake user response
Download hijacking	• Replace download file • Piggybacking
Coercing attacks	• Execute in Secure Zone • Evade I/O redirection

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Benign Website Evaluation

- Normal file downloads

- Normal site-browsing

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, L. Lu et al.

Performance Evaluation

- Per-component test
- End-to-end test
- Worst case overhead – **3%**
- Negligible on average

Browser	Time (sec) w/o BLADE	Time (sec) w/ BLADE	Delay
Firefox 3.5	3.531	3.563	**0.91%**
IE 7.0	4.328	4.401	**1.69%**
IE 8.0	4.028	4.733	**1.18%**

File Size (MB)	Time (sec) w/o BLADE	Time (sec) w/ BLADE	Delay
0.98	2.134	2.201	**3.14%**
9.23	33.201	33.879	**2.04%**
94.66	313.443	316.003	**0.81%**

Limitations

- Social engineering attacks
- In-memory execution of shellcode
- Only effective against binary executables

Q&A

www.blade-defender.org