Botnets at Application+ Layer

Lt Cdr Raj Shastrakar

SECURITYBYTE 2011
CONFERENCE & WORKSHOPS

whoami

Lt Cdr Raj Shastrakar

Deputy Director , CERT – Navy

.rajshas [at] gmail

.twit @rajshas

Talk ??

Threats and Trends

Defensive systems

New (latest) attack vector

Example – PoC

Mutants

Mitigation

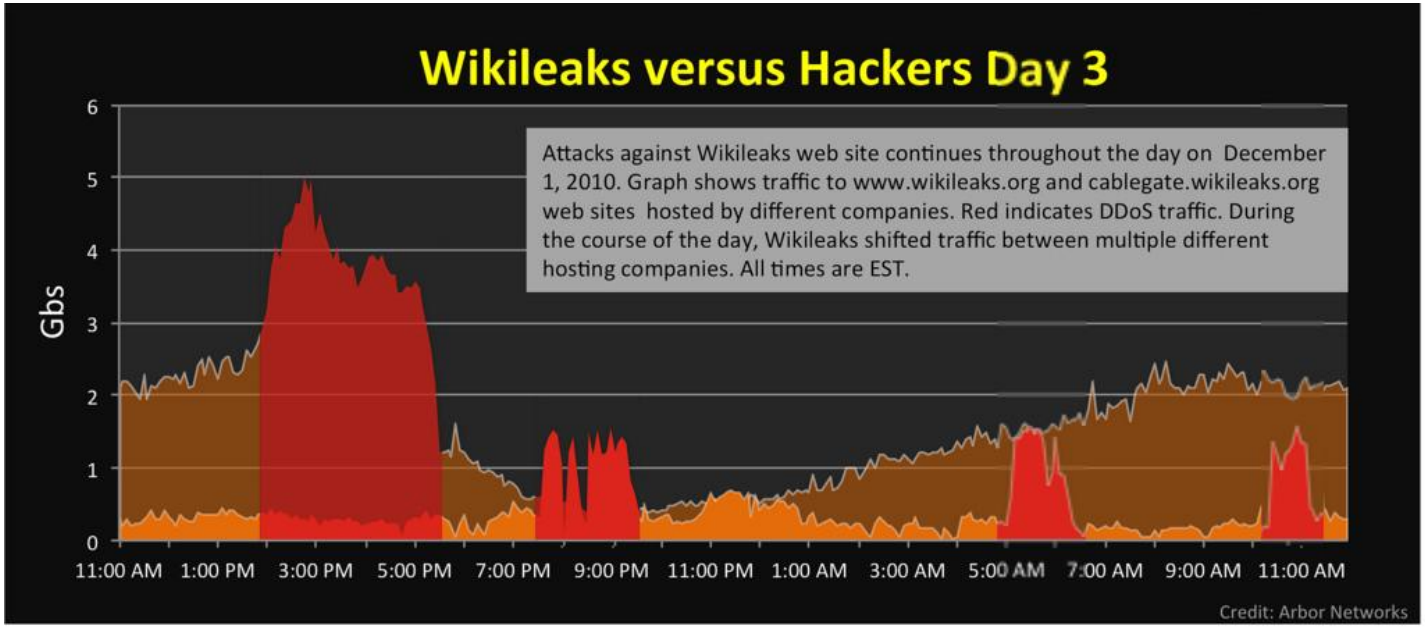
Threats

Money (USD $10 Billion)

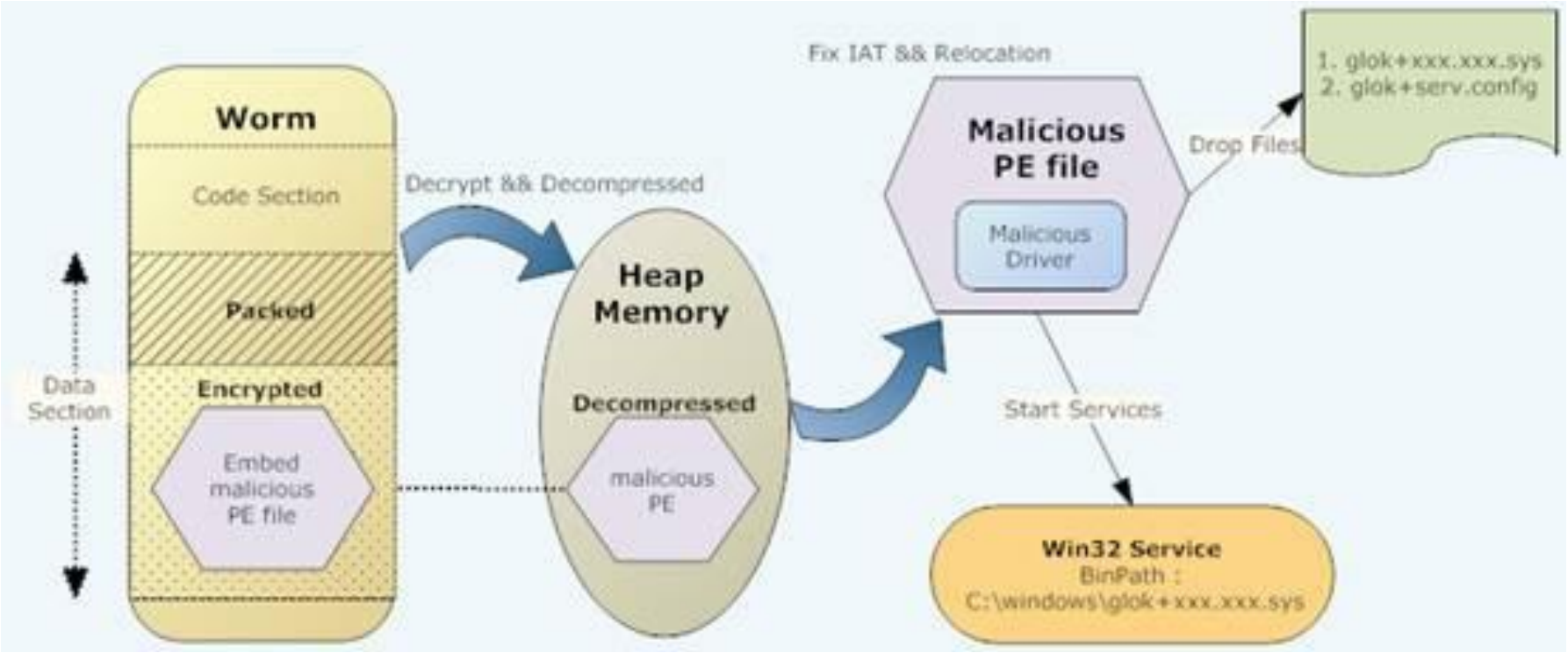
Power (Estonia)

Information (you)

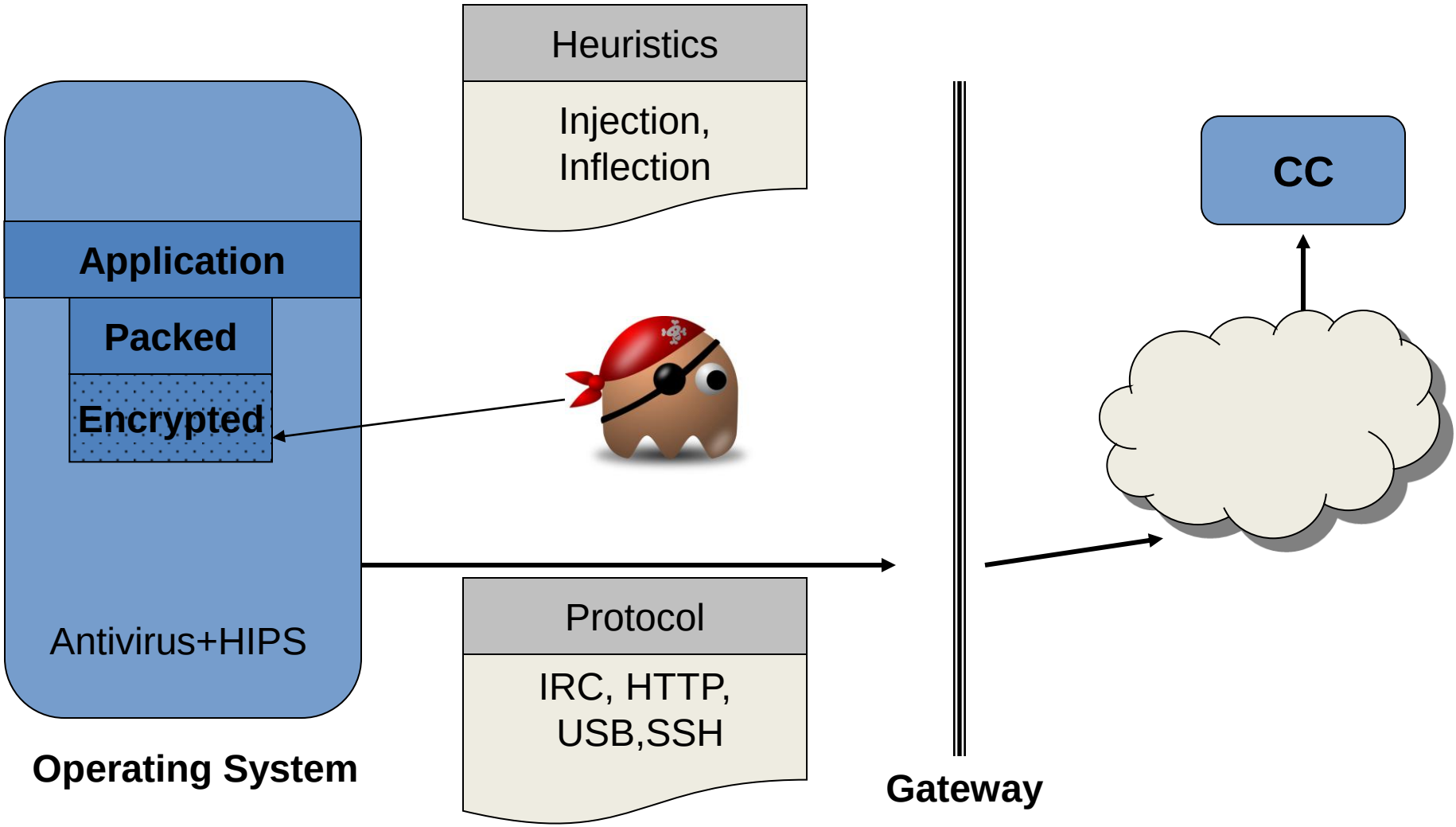
Trends


Wikileaks versus Hackers Day 3
Attacks against Wikileaks web site continues throughout the day on December 1, 2010. Graph shows traffic to www.wikileaks.org and cablegate.wikileaks.org web sites hosted by different companies. Red indicates DDoS traffic. During the course of the day, Wikileaks shifted traffic between multiple different hosting companies. All times are EST.
Gbs
6
5
4
3
2
1
0
11:00 AM
1:00 PM
3:00 PM
5:00 PM
7:00 PM
9:00 PM
11:00 PM
1:00 AM
3:00 AM
5:00 AM
7:00 AM
9:00 AM
11:00 AM
Credit: Arbor Networks

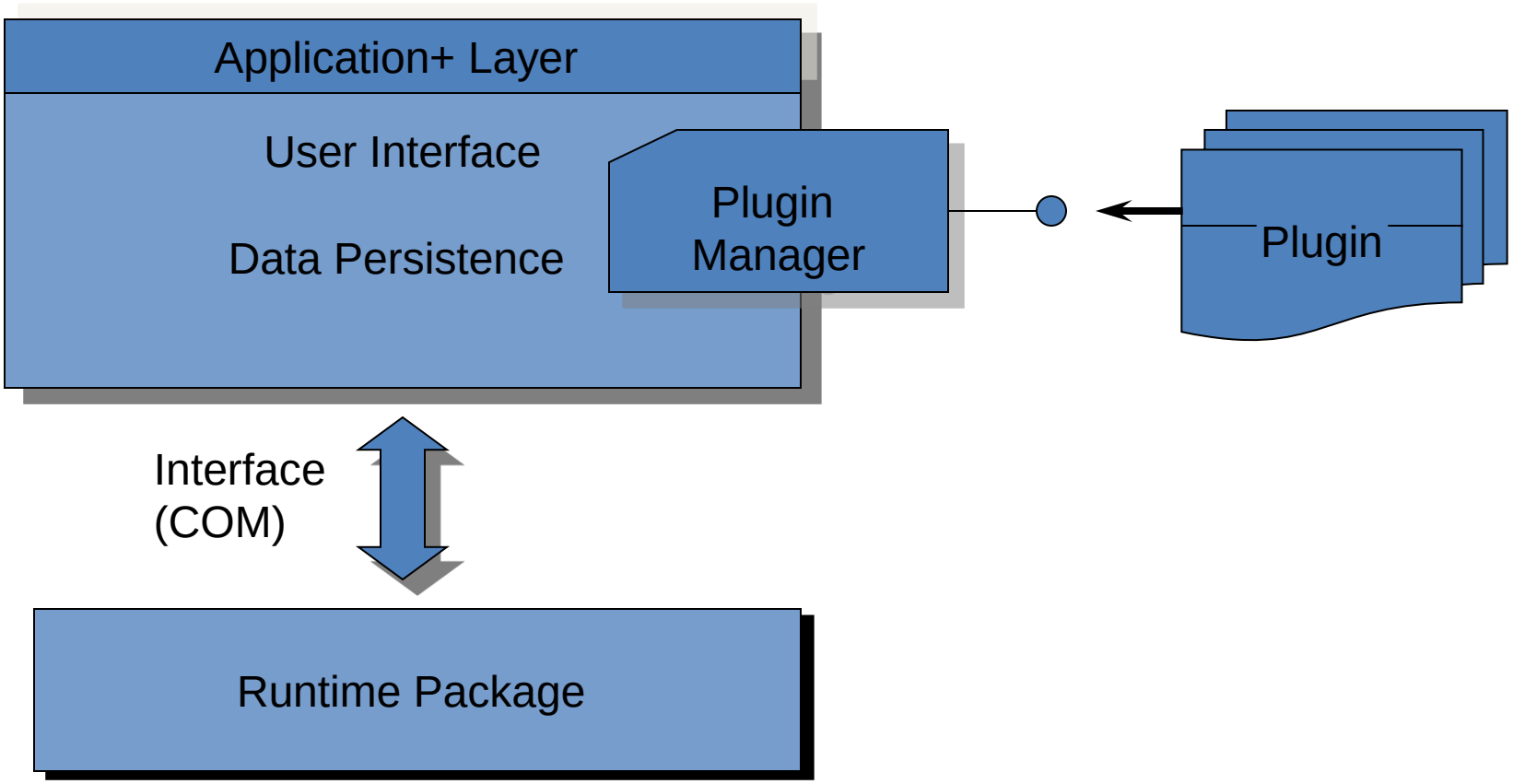
Traditional Worm



Bot + Template



Attack Vector….



Bot+ Power ☺

No installation required
Legitimate program
Legitimate traffic
Platform independent
No (triggering) heuristics

Bot+ Limitations ☹

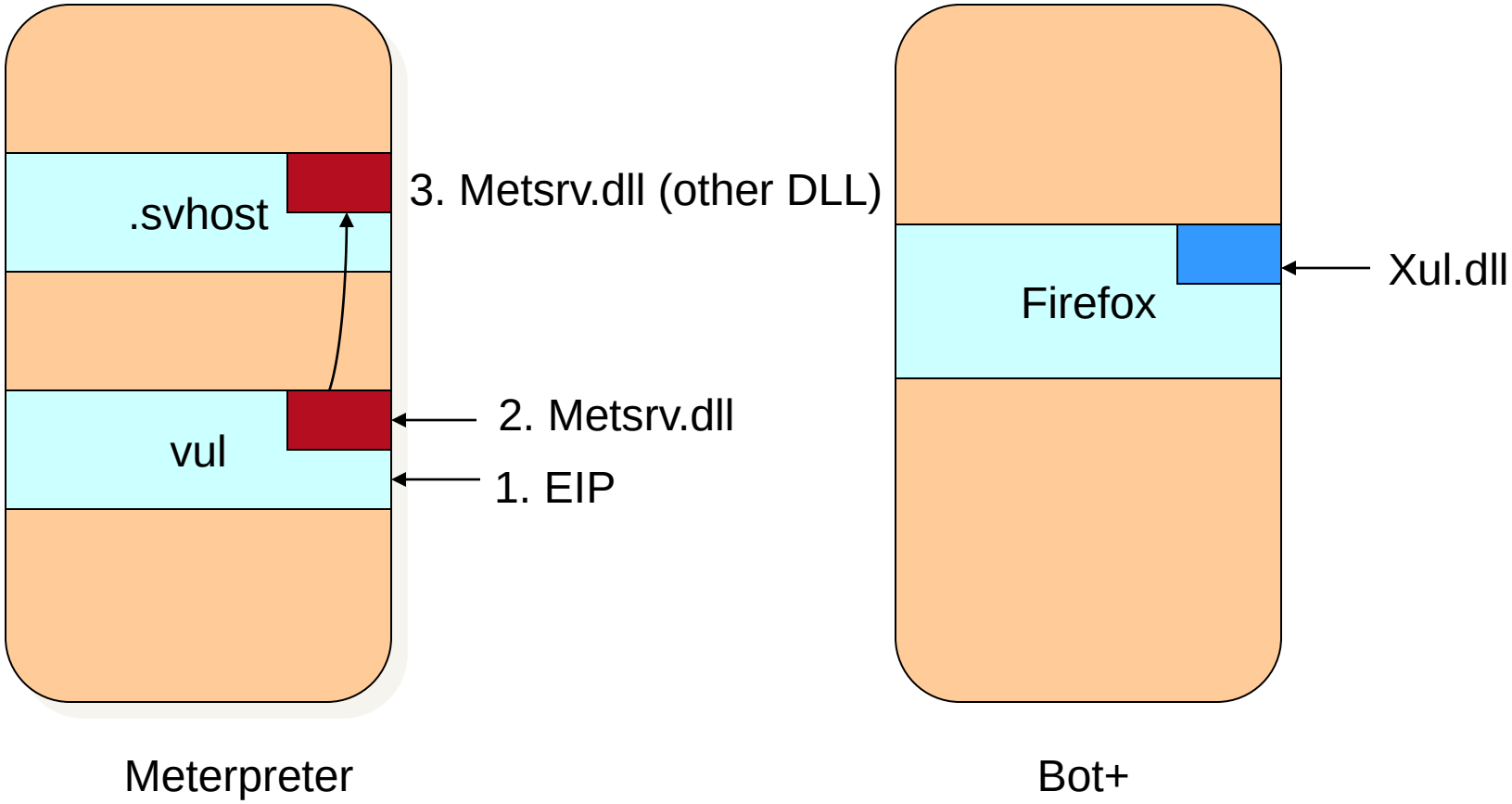
Bot Power = API Power

Jailed environment

Migration not possible

Distribution

Meterpreter v/s our Bot+

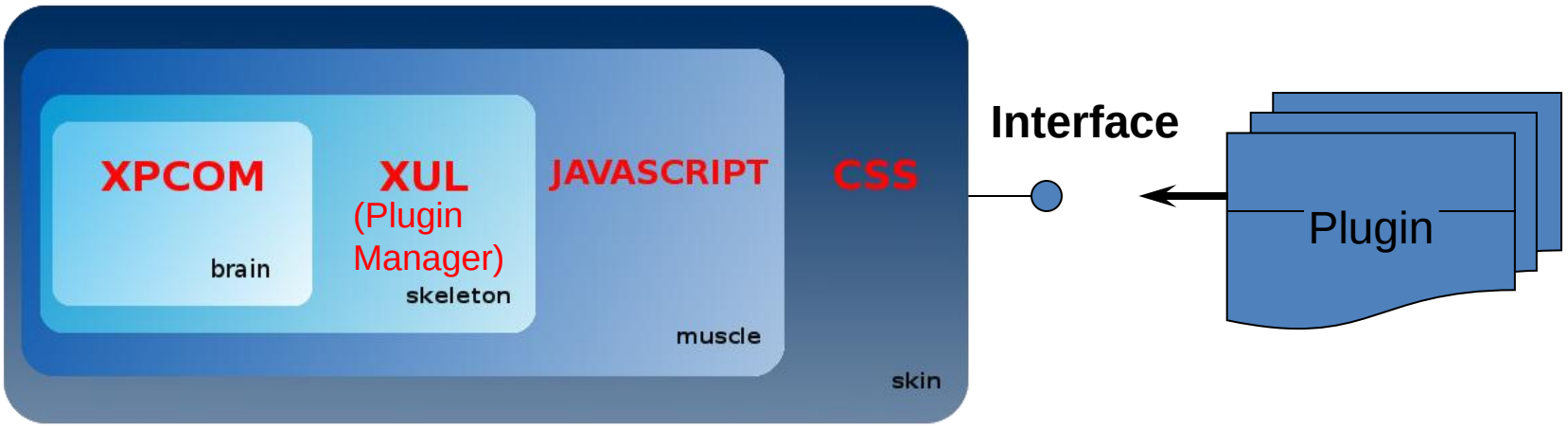


Breeding Grounds

	Platform	Technology	Products
Mozilla	XUL	XML	All
Skype	Skype4 COM	DLL	
Adobe	Adobe SDK	DLL	Reader

and many many more ....

Firefox App+ Layer



Gecko Engine

OS

Necko (Networking)

Parser & JS

Graphics Adapter

API Calls

- System (clipboard, notifications, file)
- Browser (private browsing, tab-browser)
- UI (Widget, context-menu, panel)
- Requests (xhr)
- Web Content (pagemods)

XUL (XML UI Language)

HTML file with XML syntax

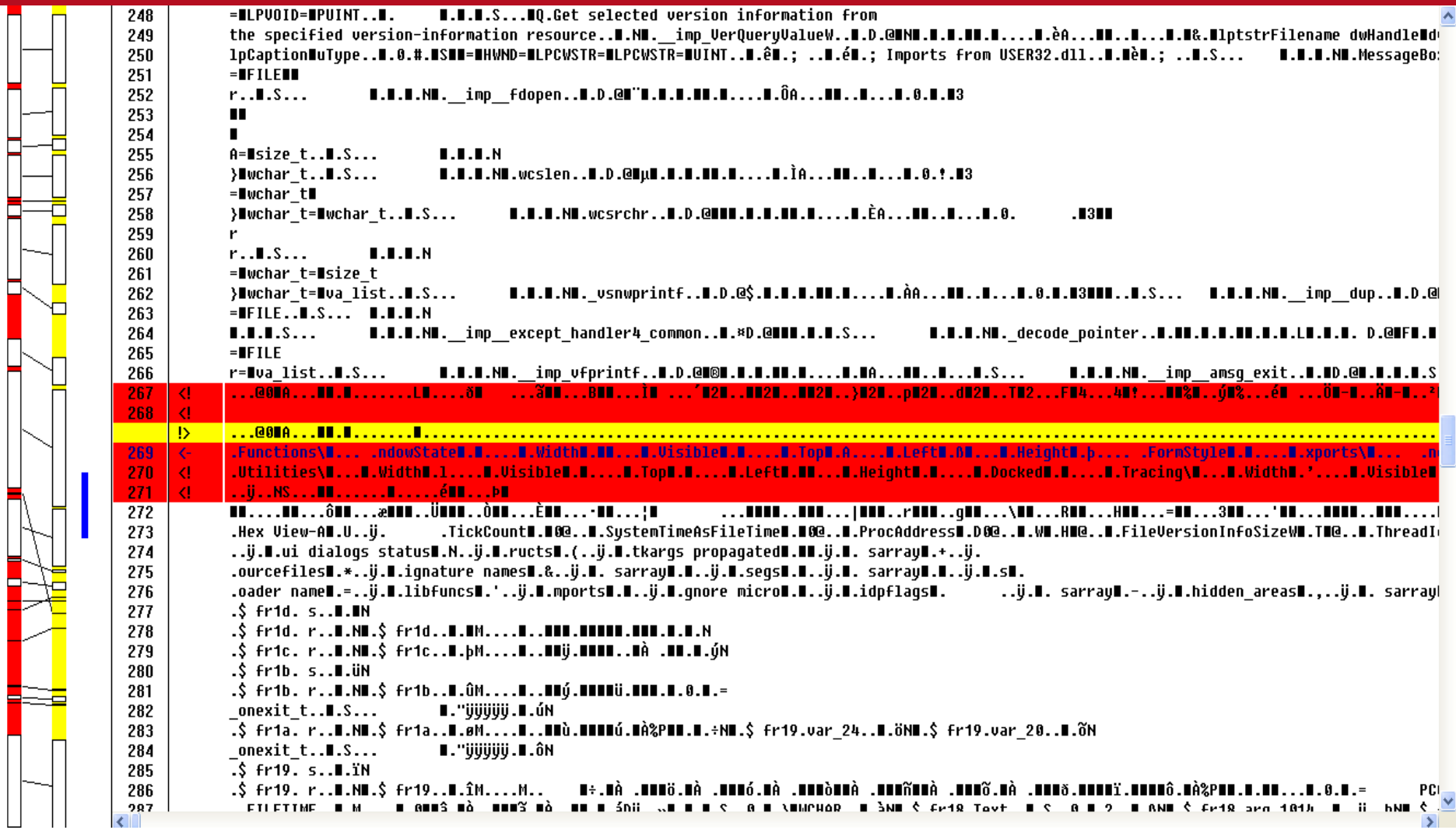
Rendered by XUL Engine

Access to Gecko

And of course access to OS.

```
<?xml version="1.0"?>
<?xml-stylesheet href="chrome://global/skin/xul.css" type="
text/css"?>
<!DOCTYPE window>
<window id="main-window" xmlns:html="http://www.w3.
org/1999/xhtml"       xmlns="http://www.mozilla.
org/keymaster....xul">
  <menubar>
    <menu label="File">
    <menupopup>
      <menuitem label="Hello World!" onclick="alert('Hello
world!\n');"/>
    </menupopup>
    </menu>
  </menubar>
```

Memory Diff



Adobe Reader

Plugins are DLLs (Binary),
Adobe SDK
Installation on the fly
Powerfull API
Digitial Signature required (not default)

Bot+ Mutants

Zeus Banking Trojan

Canvas plugin for thunderbird

Firefox – Mozilla Sniffer addons

Stop me if u can…

Developers – API restriction
- No on the fly inclusion
- Pragmatic proactive defenses
- Channelize community codes

AVs

Admins

Demo

Q&A

Ref