The Exploit Intelligence Project

Dan Guido

dguido@isecpartners.com

07/25/2011

iSEC PARTNERS

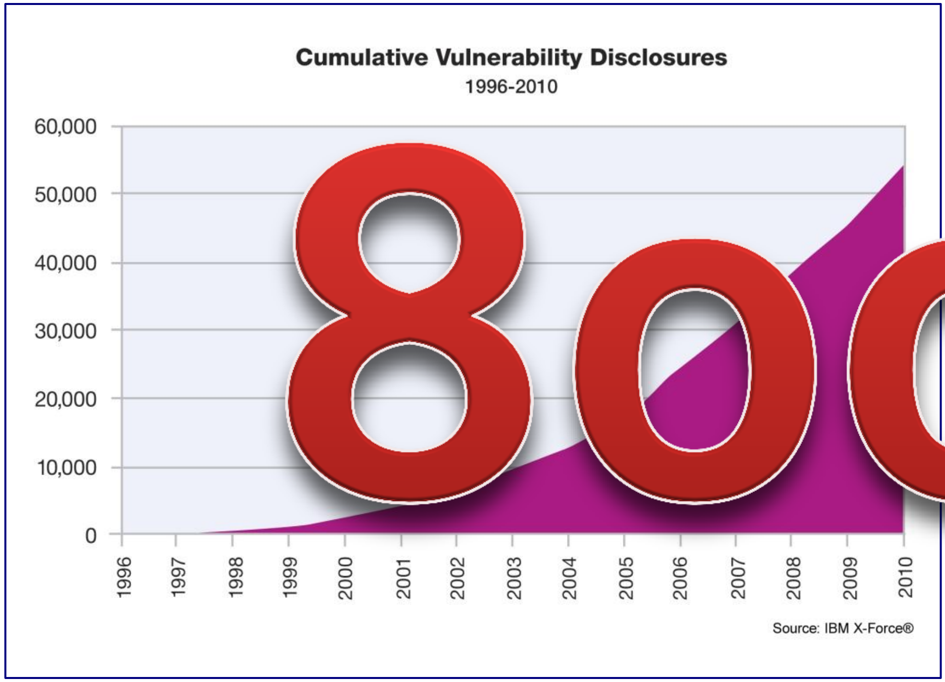
Intro and Agenda

- Talk series discussing intelligence-driven security
  - Provide actual data on attacker characteristics
  - Provide analysis tradecraft to analyze it
    - Intrusion kill chains
    - Attacker characterization
    - Adversarial attack graphs

- Informed defense is more effective and less costly
  - Less hypothetical, more verifiable
  - Defenses supported by observation
  - “Technology doesn’t beat determination”

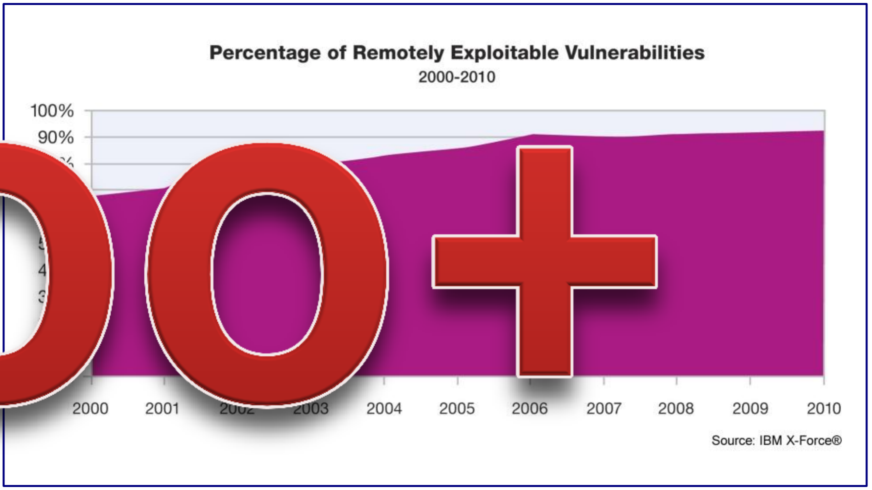
Let’s Talk About Vulnerabilities

800+



Cumulative Vulnerability Disclosures
1996-2010

Source: IBM X-Force®



Percentage of Remotely Exploitable Vulnerabilities
2000-2010

Source: IBM X-Force®

*IBM X-Force 2010 Trend and Risk Report

How many vulnerabilities did you have to pay attention to avoid SpyEye, Zeus, Gozi, Clampi, etc?

13

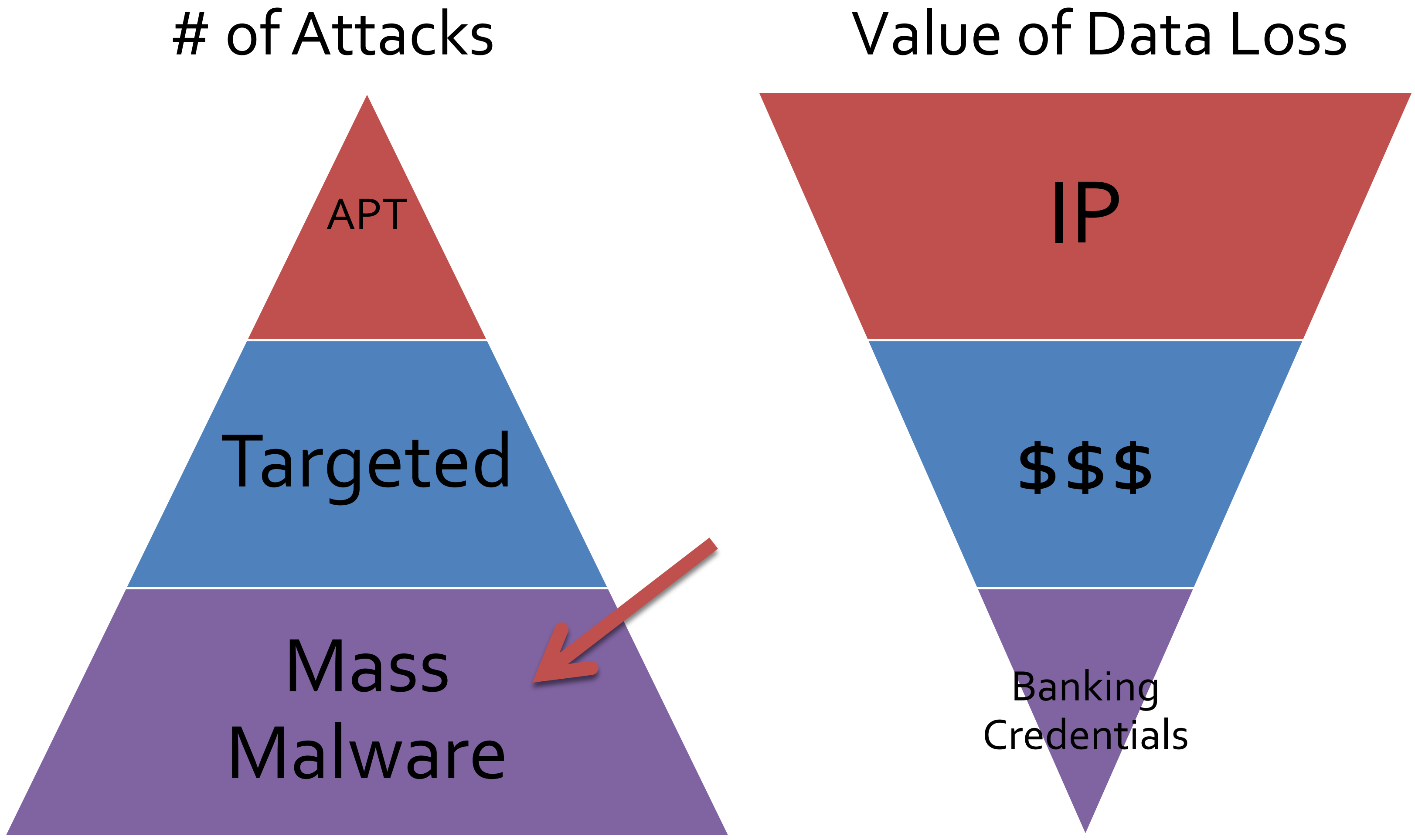
2010

14

2009

What are we doing wrong?

Maslow's Internet Threat Hierarchy



iSEC PARTNERS

Mass Malware

How does it work?

Gain Exposure

Welcome to TimesPeople
Get Started

TimesPeople recommended: Ahem! Are You Talking to Me? (Or Texting?)

The New York Times

Sunday, April 17, 2011 Last Update: 2:11 PM ET

The Times introduces Digital Subscriptions. Learn More »

Switch to Global Edition ›

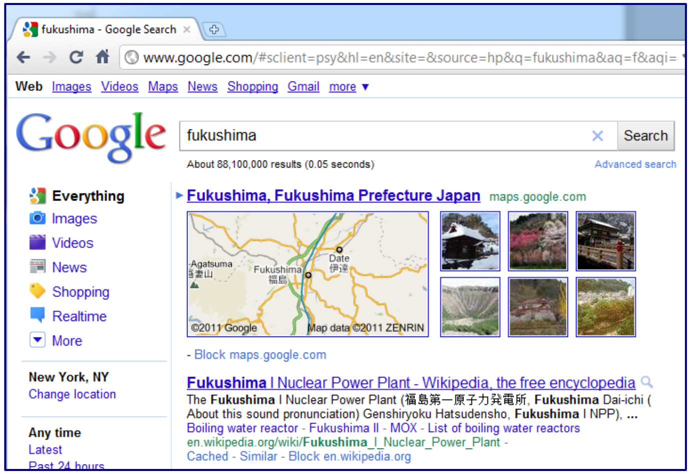
JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

Regulation of Offshore Rigs Is a Work in Progress

By JOHN M. BRODER and

OPINION
OP-ART
A Westm
Prince William a
Kate

Malicious Ads



www.google.com/#sclient=psy&hl=en&site=&source=hp&q=fukushima&aq=f&aqi=

fukushima

About 88,100,000 results (0.05 seconds)

Fukushima, Fukushima Prefecture Japan maps.google.com

- Block maps.google.com

Fukushima I Nuclear Power Plant - Wikipedia, the free encyclopedia

The **Fukushima** I Nuclear Power Plant (福島第一原子力発電所, **Fukushima** Dai-ichi (About this sound pronunciation) Genshiryoku Hatsudensho, **Fukushima** I NPP), ...
Boiling water reactor - Fukushima II - MOX - List of boiling water reactors
en.wikipedia.org/wiki/**Fukushima**_I_Nuclear_Power_Plant -
Cached - Similar - Block en.wikipedia.org

New York, NY
Change location

Any time
Latest
Past 24 hours

SEO

https://www.facebook.com/

Dan Guido
Edit My Profile

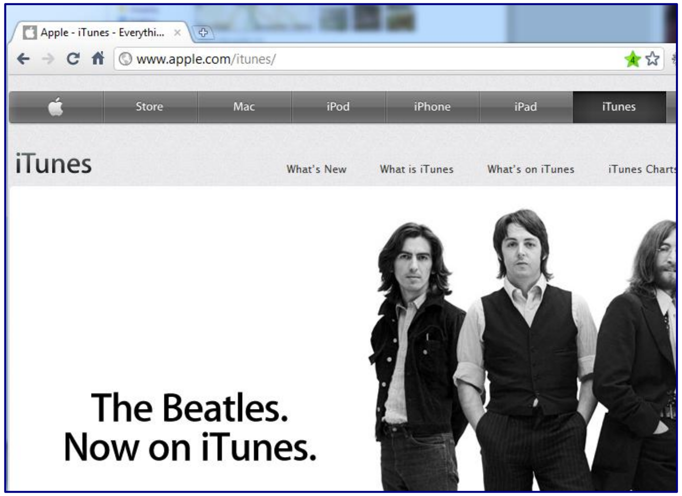
News Feed

What's on your mind?

Post Hidden
This post will no longer appear in your News Feed. Undo

Dino Dai Zovi
It is really really crappy outside right now, but I'm considering venturing out into the wilderness to get some half and half to make some coffee. Not at all addicted, nope.
17 hours ago · Like · Comment
3 people like this.
View all 4 comments

Compromised Friends

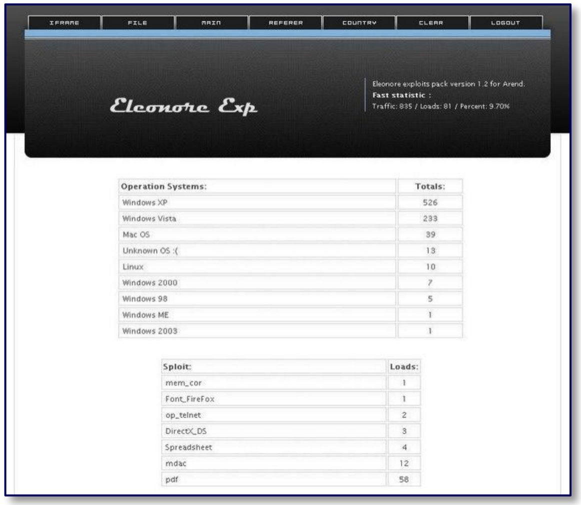


The Beatles.
Now on iTunes.

SQL Injection

iSEC PARTNERS

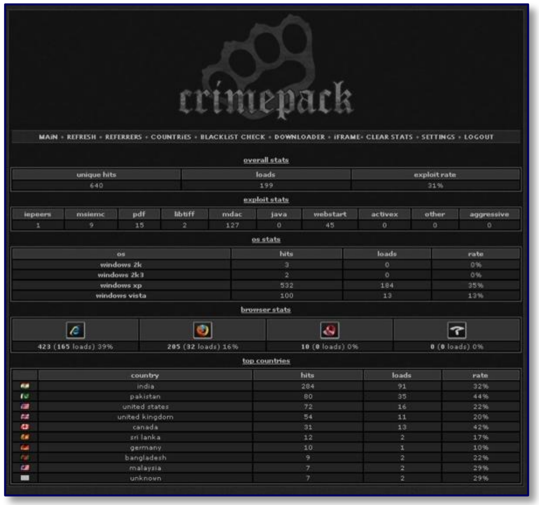
Weaponize Capabilities



Eleonore exploits pack version 1.2 for Arend.
Fast statistic :
Traffic: 835 / Loads: 81 / Percent: 9.70%

Operation Systems:	Totals:
Windows XP	526
Windows Vista	233
Mac OS	39
Unknown OS :(	13
Linux	10
Windows 2000	7
Windows 98	5
Windows ME	1
Windows 2003	1

Sploit:	Loads:
mem_cor	1
Font_FireFox	1
op_telnet	2
DirectX_DS	3
Spreadsheet	4
mdac	12
pdf	58


crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTINGS • LOGOUT

overall stats

unique hits	loads	exploit rate
640	199	31%

exploit stats

iepeers	msiemc	pdf	libtiff	mdac	java	webstart	activex	other	aggressive
1	9	15	2	127	0	45	0	0	0

os stats

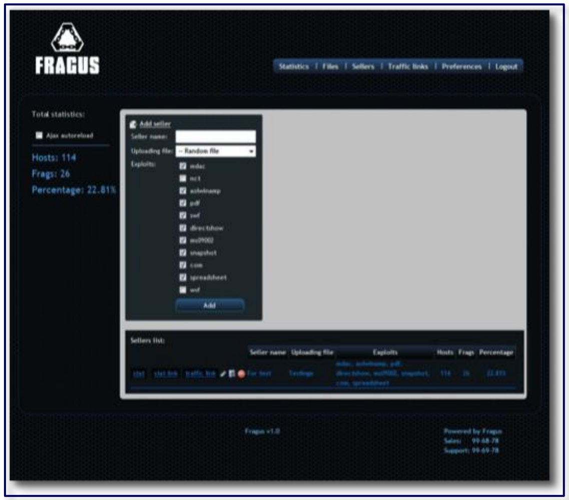
os	hits	loads	rate
windows 2k	3	0	0%
windows 2k3	2	0	0%
windows xp	532	184	35%
windows vista	100	13	13%

browser stats

423 (165 loads) 39%	205 (32 loads) 16%	10 (0 loads) 0%	0 (0 loads) 0%

top countries

country	hits	loads	rate
india	284	91	32%
pakistan	80	35	44%
united states	72	16	22%
united kingdom	54	11	20%
canada	31	13	42%
sri lanka	12	2	17%
germany	10	1	10%
bangladesh	9	2	22%
malaysia	7	2	29%
unknown	7	2	29%


FRAGUS
Statistics | Files | Sellers | Traffic links | Preferences | Logout
Add seller
Add

Total statistics:
☐ Ajax autoreload
Hosts: 114
Frags: 26
Percentage: 22.81%

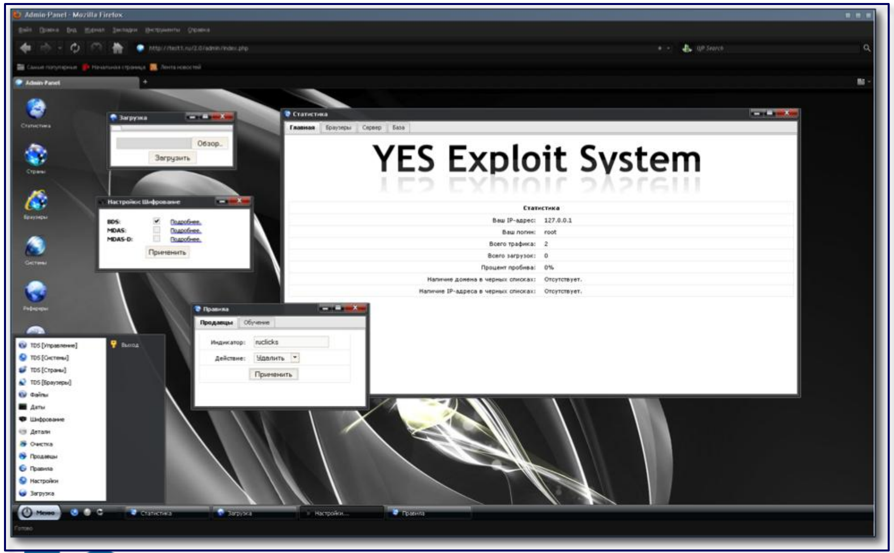
Seller name:
Uploading file: -- Random file
Exploits:
☑ mdac
☐ mct
☑ aolwinamp
☑ pdf
☑ swf
☑ directshow
☑ ms09002
☑ snapshot
☑ com
☑ spreadsheet
☐ wvf

Sellers list:

	Seller name	Uploading file	Exploits	Hosts	Frags	Percentage
stat stat link traffic link	For test	Testing	mdac, aolwinamp, pdf, directshow, ms09002, snapshot, com, spreadsheet	114	26	22.81%

Fragus v1.0

Powered by Fragus
Sales: 99-68-78
Support: 99-69-78

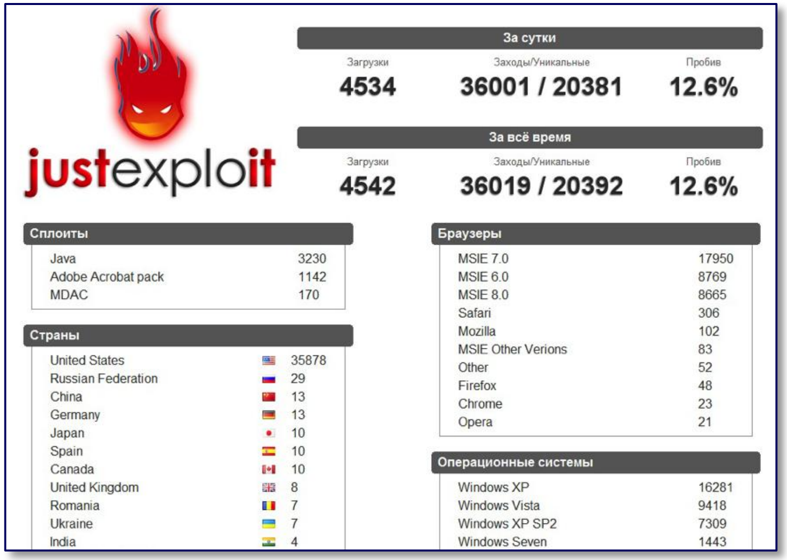


BDS: ☑ Подробнее.
MDAS: ☐ Подробнее.
MDAS-D: ☐ Подробнее.

Индикатор: ruclicks
Действие: Удалить

Статистика

Ваш IP-адрес: 127.0.0.1
Ваш логин: root
Всего трафика: 2
Всего загрузок: 0
Процент пробива: 0%
Наличие домена в черных списках: Отсутствует.
Наличие IP-адреса в черных списках: Отсутствует.



За сутки

Загрузки	Заходы/Уникальные	Пробив
4534	36001 / 20381	12.6%

За всё время

Загрузки	Заходы/Уникальные	Пробив
4542	36019 / 20392	12.6%

Сплоиты

Java	3230
Adobe Acrobat pack	1142
MDAC	170

Страны

United States	35878
Russian Federation	29
China	13
Germany	13
Japan	10
Spain	10
Canada	10
United Kingdom	8
Romania	7
Ukraine	7
India	4

Браузеры

MSIE 7.0	17950
MSIE 6.0	8769
MSIE 8.0	8665
Safari	306
Mozilla	102
MSIE Other Verions	83
Other	52
Firefox	48
Chrome	23
Opera	21

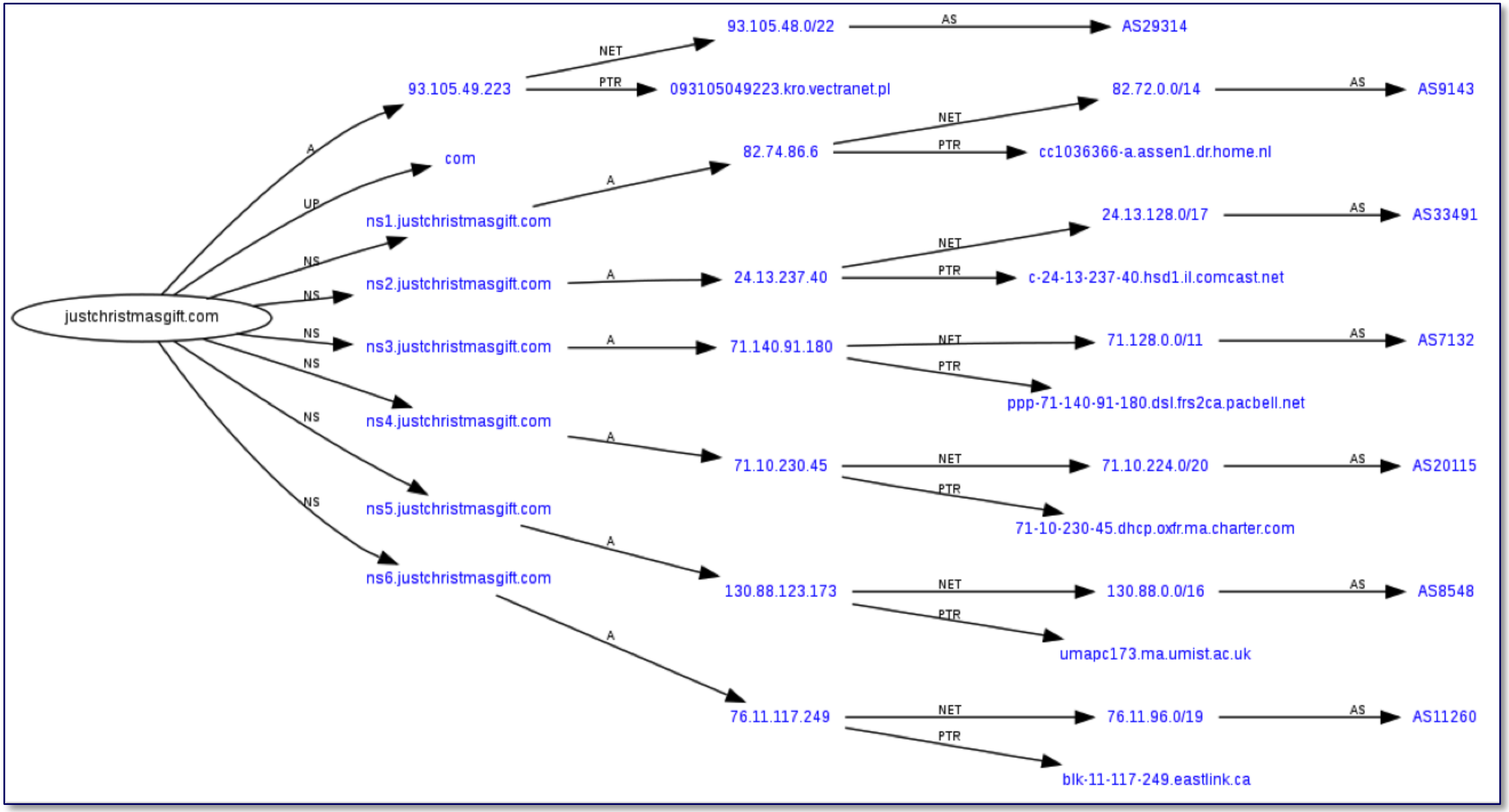
Операционные системы

Windows XP	16281
Windows Vista	9418
Windows XP SP2	7309
Windows Seven	1443

iSEC PARTNERS

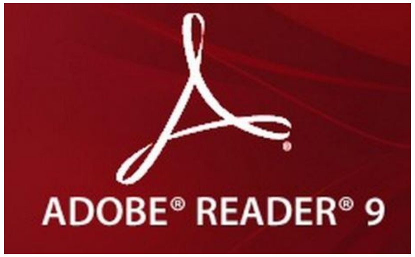
5-20 exploits, $200-$2000 dollars

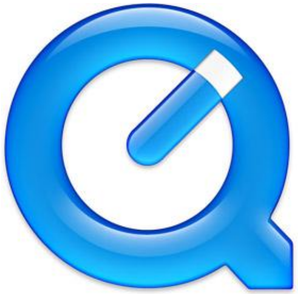
Establish Delivery Network



Exploit Targets

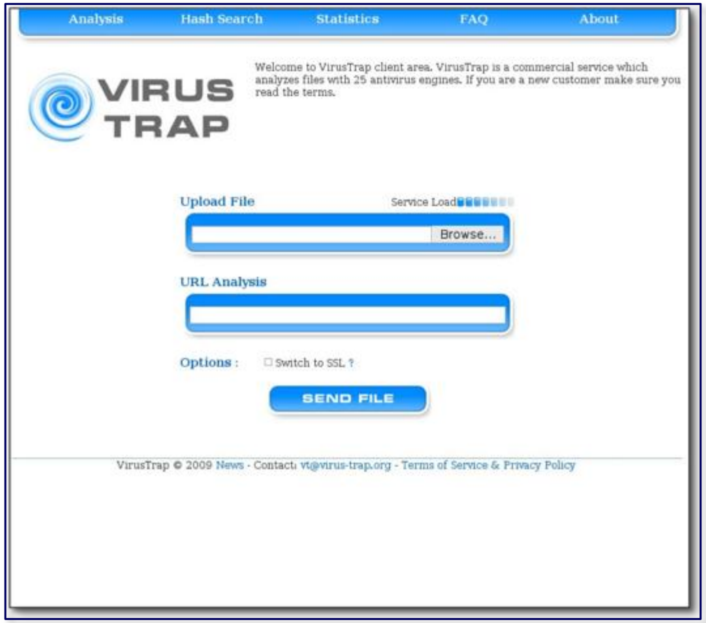
Windows®
Internet
Explorer® 7





Java
Sun Microsystems

Install Malware



Welcome to VirusTrap client area. VirusTrap is a commercial service which analyzes files with 25 antivirus engines. If you are a new customer make sure you read the terms.

Upload File

Service Load

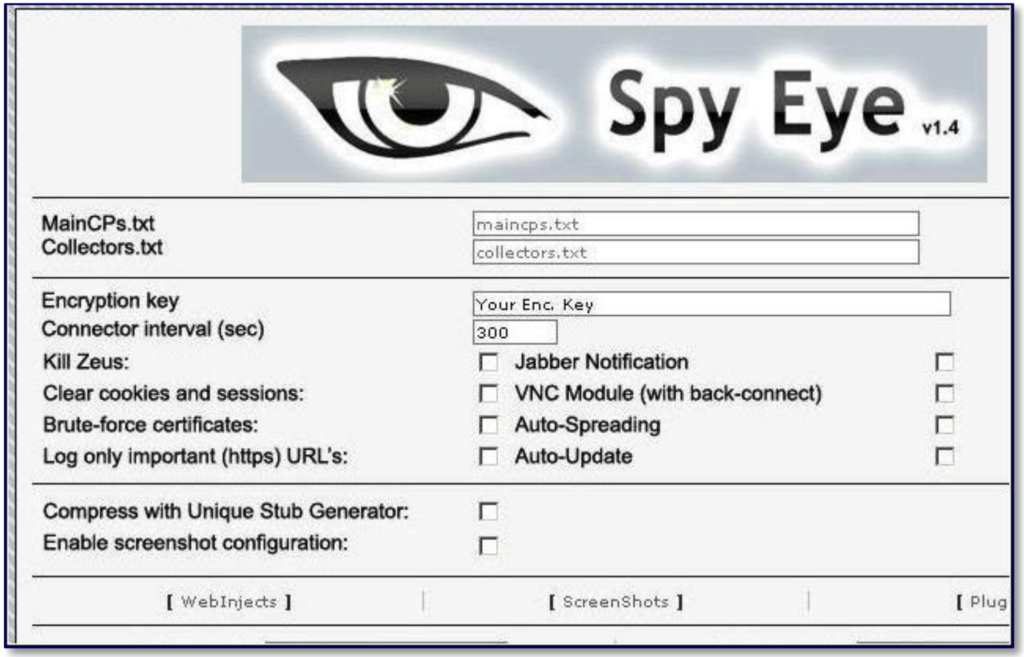
Browse...

URL Analysis

Options : □ Switch to SSL ?

SEND FILE

VirusTrap © 2009 News - Contact: vt@virus-trap.org - Terms of Service & Privacy Policy



MainCPs.txt: maincps.txt
Collectors.txt: collectors.txt

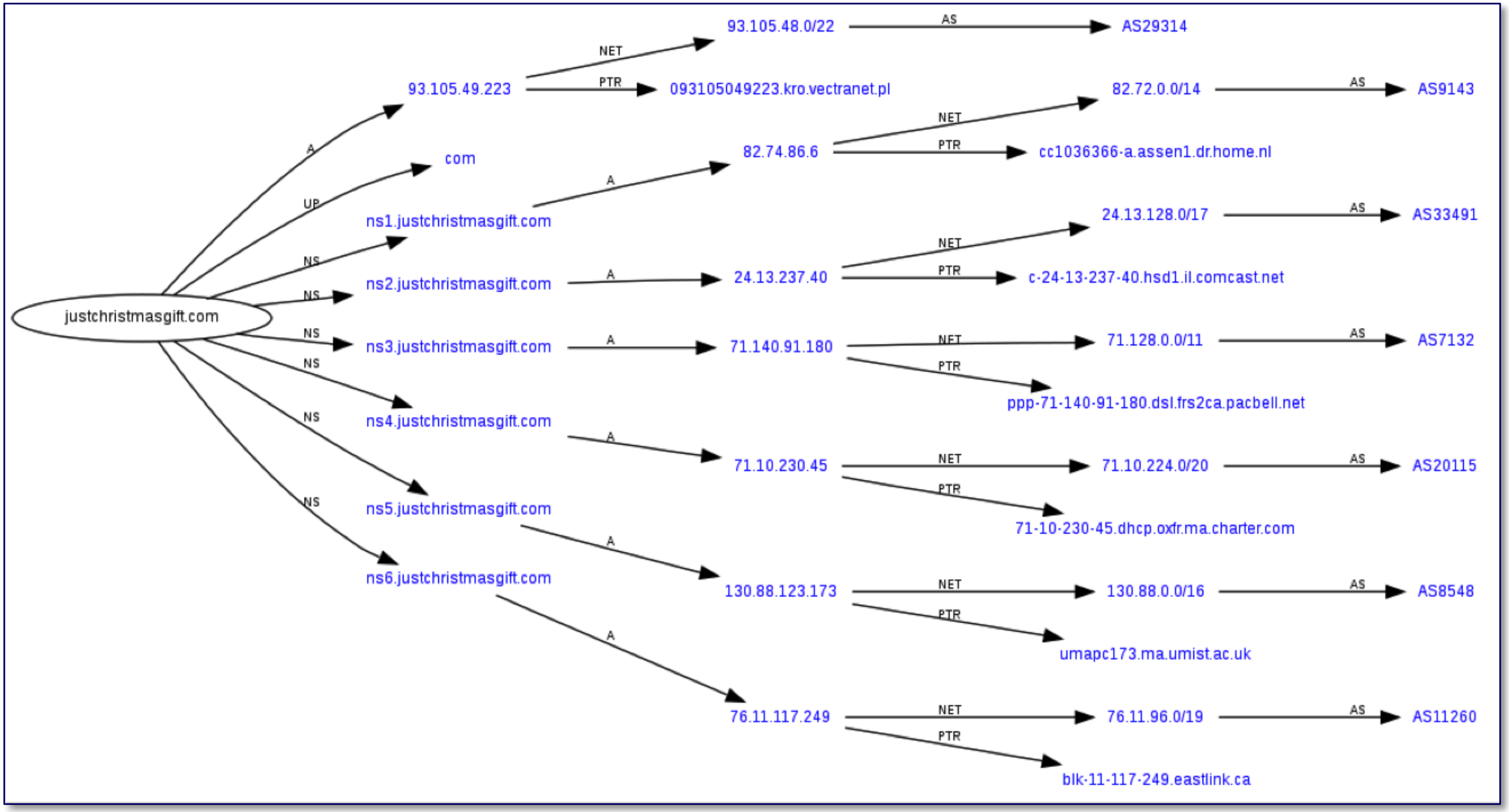
Encryption key: Your Enc. Key
Connector interval (sec): 300

Kill Zeus: □
Clear cookies and sessions: □
Brute-force certificates: □
Log only important (https) URL's: □

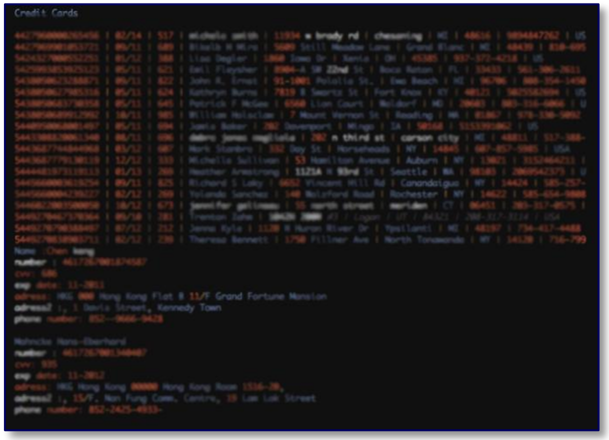
Jabber Notification □
VNC Module (with back-connect) □
Auto-Spreading □
Auto-Update □

Compress with Unique Stub Generator: □
Enable screenshot configuration: □

Establish Command and Control

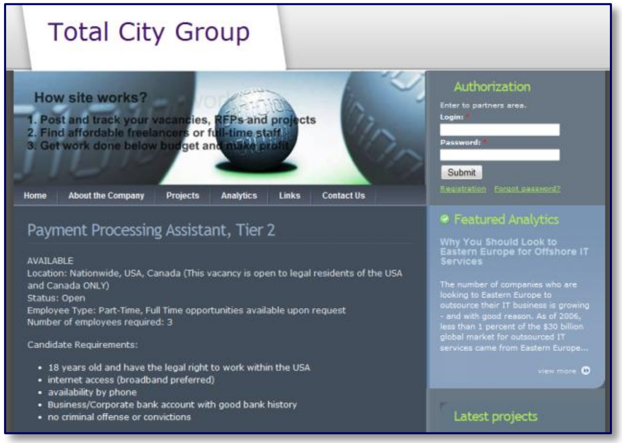


Perform Actions on Objectives



Credit Cards

[illegible]



Total City Group

How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

Authorization

Enter to partners area.

Login: *

Password: *

Submit

Registration Forgot password?

Payment Processing Assistant, Tier 2

AVAILABLE
Location: Nationwide, USA, Canada (This vacancy is open to legal residents of the USA and Canada ONLY)
Status: Open
Employee Type: Part-Time, Full Time opportunities available upon request
Number of employees required: 3

Candidate Requirements:

- 18 years old and have the legal right to work within the USA
- internet access (broadband preferred)
- availability by phone
- Business/Corporate bank account with good bank history
- no criminal offense or convictions

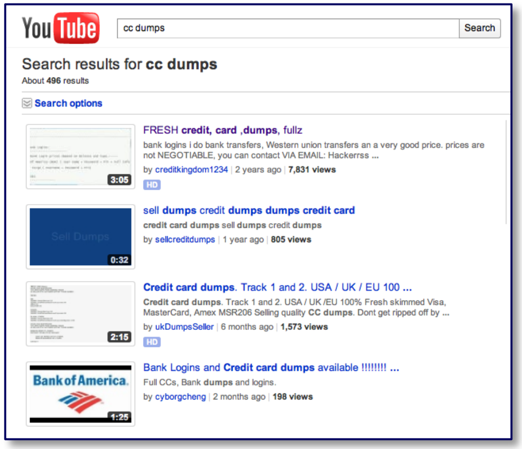
Featured Analytics

Why You Should Look to Eastern Europe for Offshore IT Services

The number of companies who are looking to Eastern Europe to outsource their IT business is growing - and with good reason. As of 2006, less than 1 percent of the $30 billion global market for outsourced IT services came from Eastern Europe...

view more

Latest projects



cc dumps Search

Search results for **cc dumps**

About **496** results

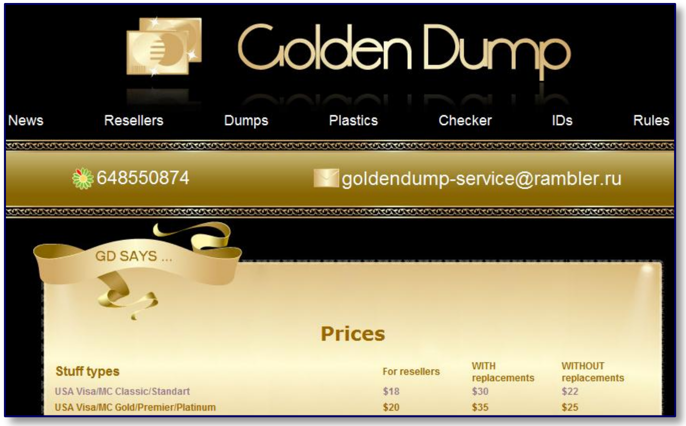
Search options

FRESH **credit, card ,dumps,** fullz
bank logins i do bank transfers, Western union transfers an a very good price. prices are not NEGOTIABLE, you can contact VIA EMAIL: Hackerrss ...
by creditkingdom1234 | 2 years ago | **7,831 views**
HD
3:05

sell **dumps** credit **dumps dumps credit card**
credit card dumps sell **dumps** credit **dumps**
by sellcreditdumps | 1 year ago | **805 views**
0:32

Credit card dumps. Track 1 and 2. USA / UK / EU 100 ...
Credit card dumps. Track 1 and 2. USA / UK /EU 100% Fresh skimmed Visa, MasterCard, Amex MSR206 Selling quality **CC dumps**. Dont get ripped off by ...
by ukDumpsSeller | 6 months ago | **1,573 views**
HD
2:15

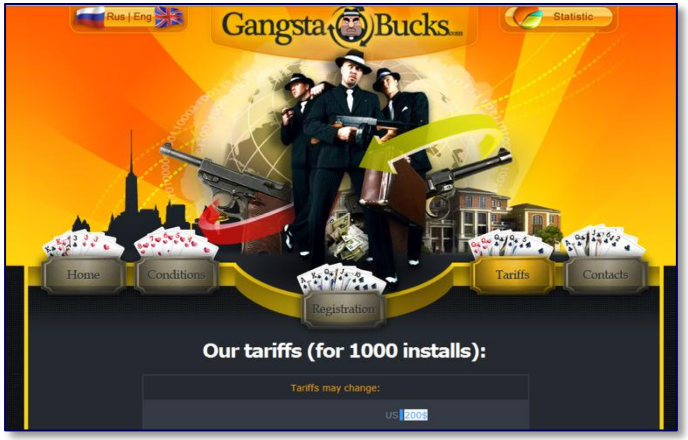
Bank Logins and **Credit card dumps** available !!!!!!!! ...
Full CCs, Bank **dumps** and logins.
by cyborgcheng | 2 months ago | **198 views**
1:25



648550874 goldendump-service@rambler.ru

Prices

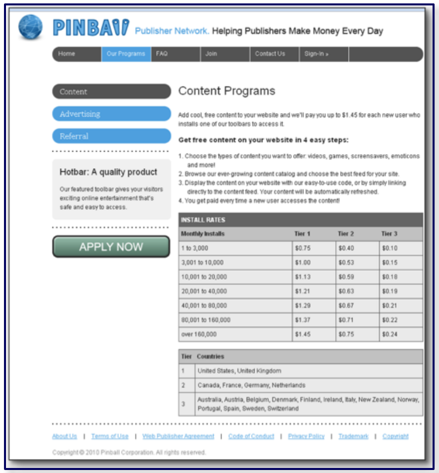
Stuff types	For resellers	WITH replacements	WITHOUT replacements
USA Visa/MC Classic/Standart	$18	$30	$22
USA Visa/MC Gold/Premier/Platinum	$20	$35	$25



Our tariffs (for 1000 installs):

Tariffs may change:

US 200$



PINBALL Publisher Network. Helping Publishers Make Money Every Day

Hotbar: A quality product

Our featured toolbar gives your visitors exciting online entertainment that's safe and easy to access.

Content Programs

Add cool, free content to your website and we'll pay you up to $1.45 for each new user who installs one of our toolbars to access it.

Get free content on your website in 4 easy steps:

1. Choose the types of content you want to offer: videos, games, screensavers, emoticons and more!
2. Browse our ever-growing content catalog and choose the best feed for your site.
3. Display the content on your website with our easy-to-use code, or by simply linking directly to the content feed. Your content will be automatically refreshed.
4. You get paid every time a new user accesses the content!

INSTALL RATES

Monthly Installs	Tier 1	Tier 2	Tier 3
1 to 3,000	$0.75	$0.40	$0.10
3,001 to 10,000	$1.00	$0.53	$0.15
10,001 to 20,000	$1.13	$0.59	$0.18
20,001 to 40,000	$1.21	$0.63	$0.19
40,001 to 80,000	$1.29	$0.67	$0.21
80,001 to 160,000	$1.37	$0.71	$0.22
over 160,000	$1.45	$0.75	$0.24

Tier	Countries
1	United States, United Kingdom
2	Canada, France, Germany, Netherlands
3	Australia, Austria, Belgium, Denmark, Finland, Ireland, Italy, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland

About Us | Terms of Use | Web Publisher Agreement | Code of Conduct | Privacy Policy | Trademark | Copyright

Copyright © 2010 Pinball Corporation. All rights reserved.

Leads to Cyber Pompeii

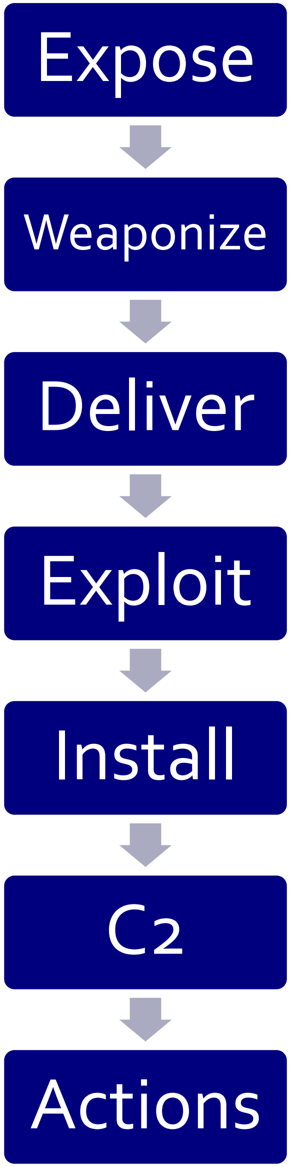
The Intrusion Kill Chain

- Systematic process that an intrusion must follow
    - Deficiency in one step will disrupt the process

- Evolves response beyond point of compromise
    - Prevents myopic focus on vulnerabilities or malware
    - Identifies attacker reuse of tools and infrastructure

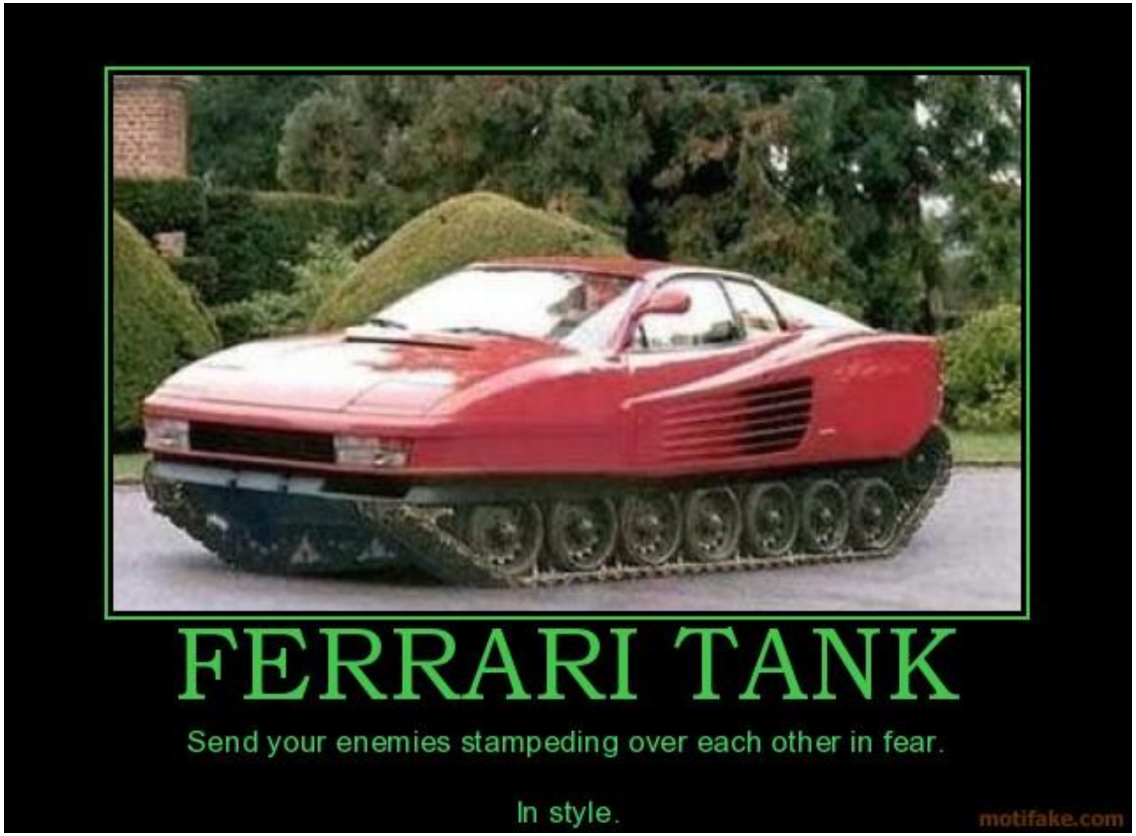
- Guides our analysis and implementation of defenses
    - Align defenses to specific processes an attacker takes
    - Force attackers to make difficult strategic adjustments

Spy vs Spy

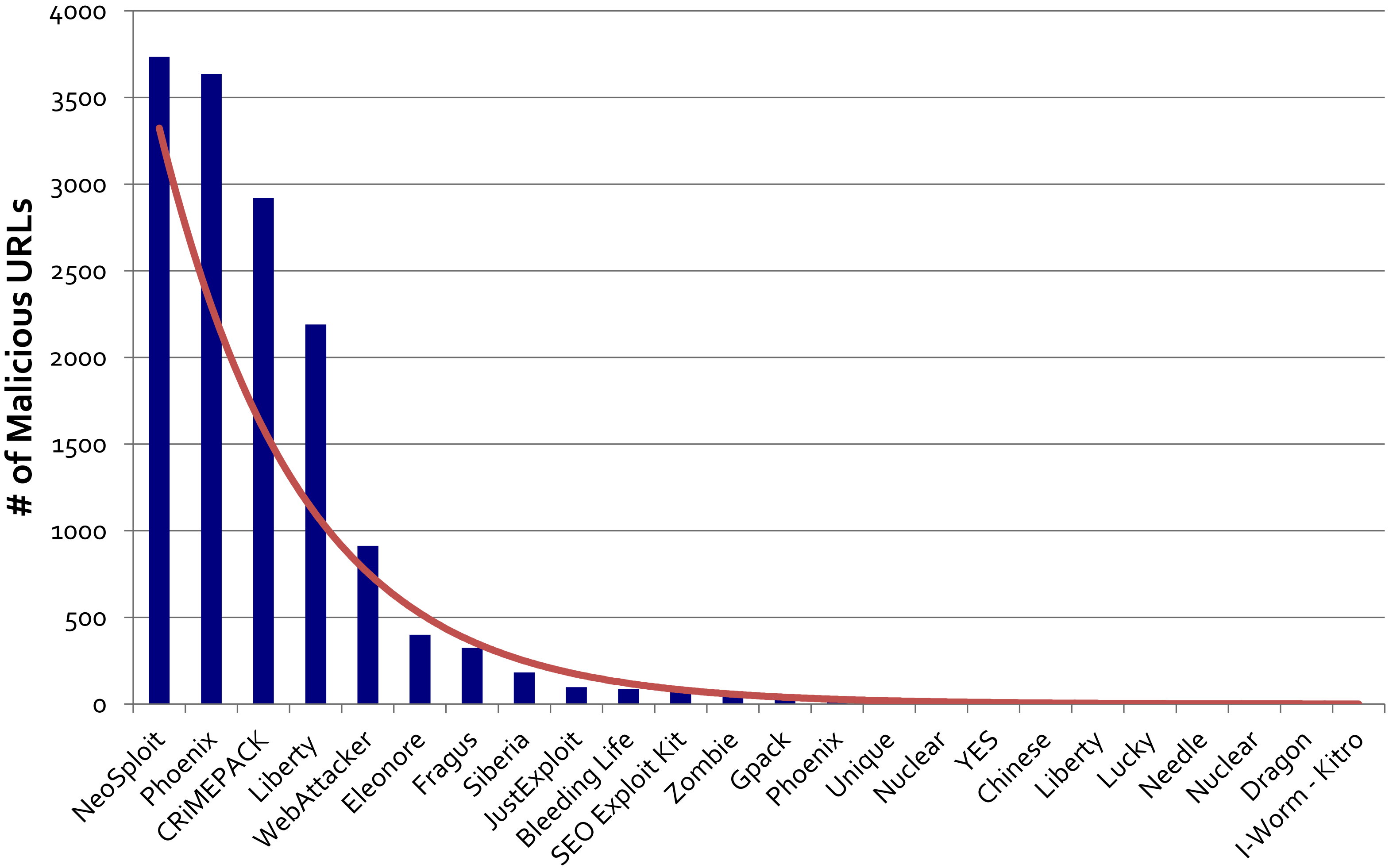


Millions of Infected Sites	Expose	Blacklists, Categorization
Thousands of Vulnerabilities	Weaponize	IDS, Patches, Secure Code
Thousands of IPs	Deliver	Blacklists
Tens of Applications	Exploit	???
Millions of Malware Samples	Install	AV
Thousands of IPs	C2	Blacklists, IDS, DLP
???	Actions	???

Going on the Offensive



Exploit Kit Popularity (Q1 2011)



*ThreatGRID Data

Collected Data Sources

- Blackhole
- Bleeding Life
- CrimePack
  - 3.1.3, 3.0, 2.2.8, 2.2.1
- Eleonore
  - 1.6, 1.4.4, 1.4.1, 1.3.2
- Fragus
- JustExploit
- Liberty
  - 2.1.0, 1.0.7
- LuckySploit
- Phoenix
  - 2.5, 2.4, 2.3, 2.2, 2.1, 2.0
- SEO Sploit pack
- Siberia
- Unique Pack
- WebAttacker
- YES
- Zombie

Mapping of Kits to Exploits + Metadata

Phoenix Exploit Kit

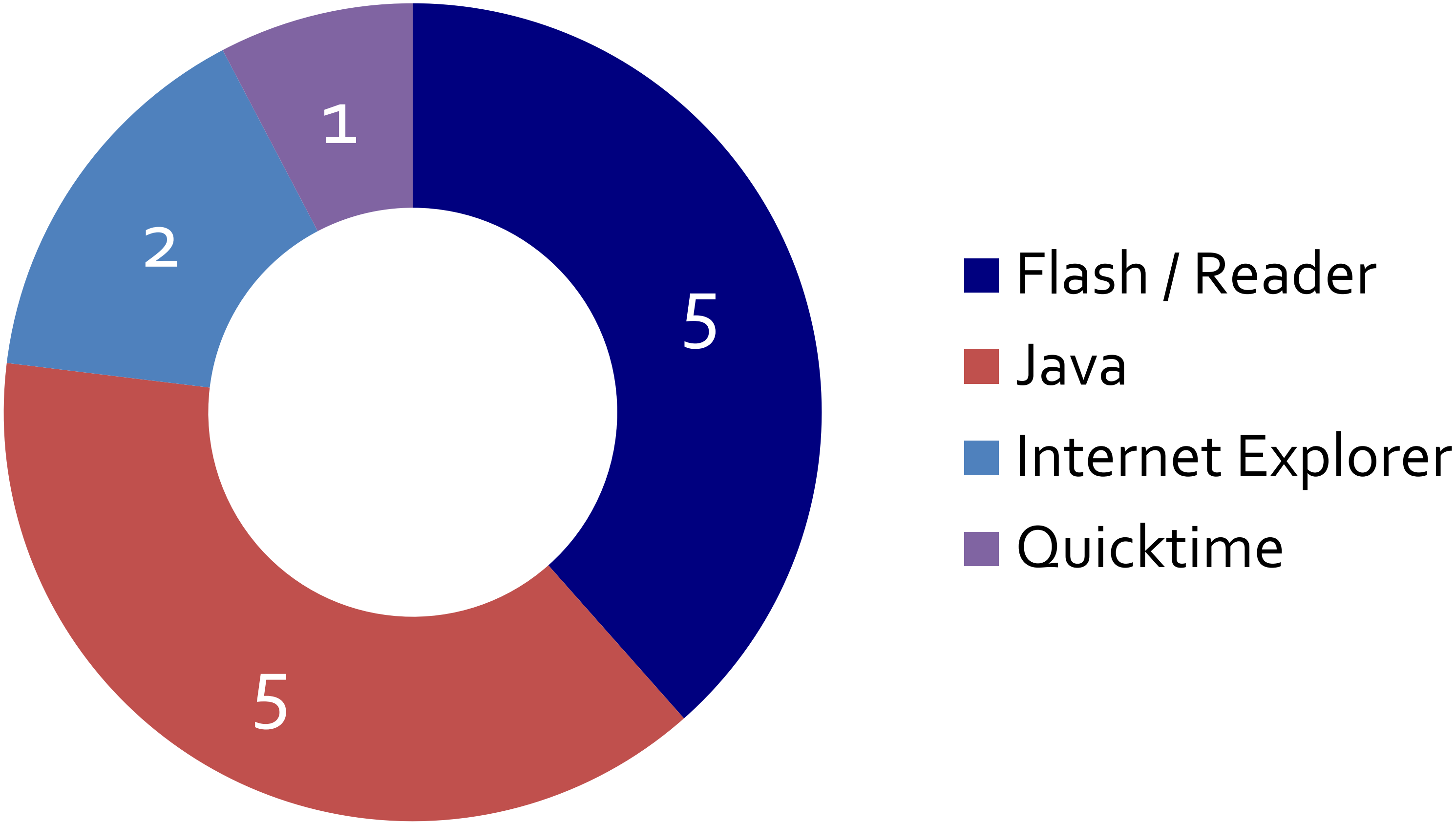
- CVE-2009-0836
- CVE-2009-0927
- CVE-2009-1869
- CVE-2010-0188
- CVE-2010-0840
- CVE-2010-0842
- CVE-2010-1297
- CVE-2010-1818
- CVE-2010-1885
- CVE-2010-2883

Affected Vendor: Apple
Affected Product: Quicktime
Type: Memory Corruption
Bypasses: DEP, ASLR

Discovered: 08/30/2010
By: Ruben Santamarta
MSF: 08/30/2010
MSF Rank: Great

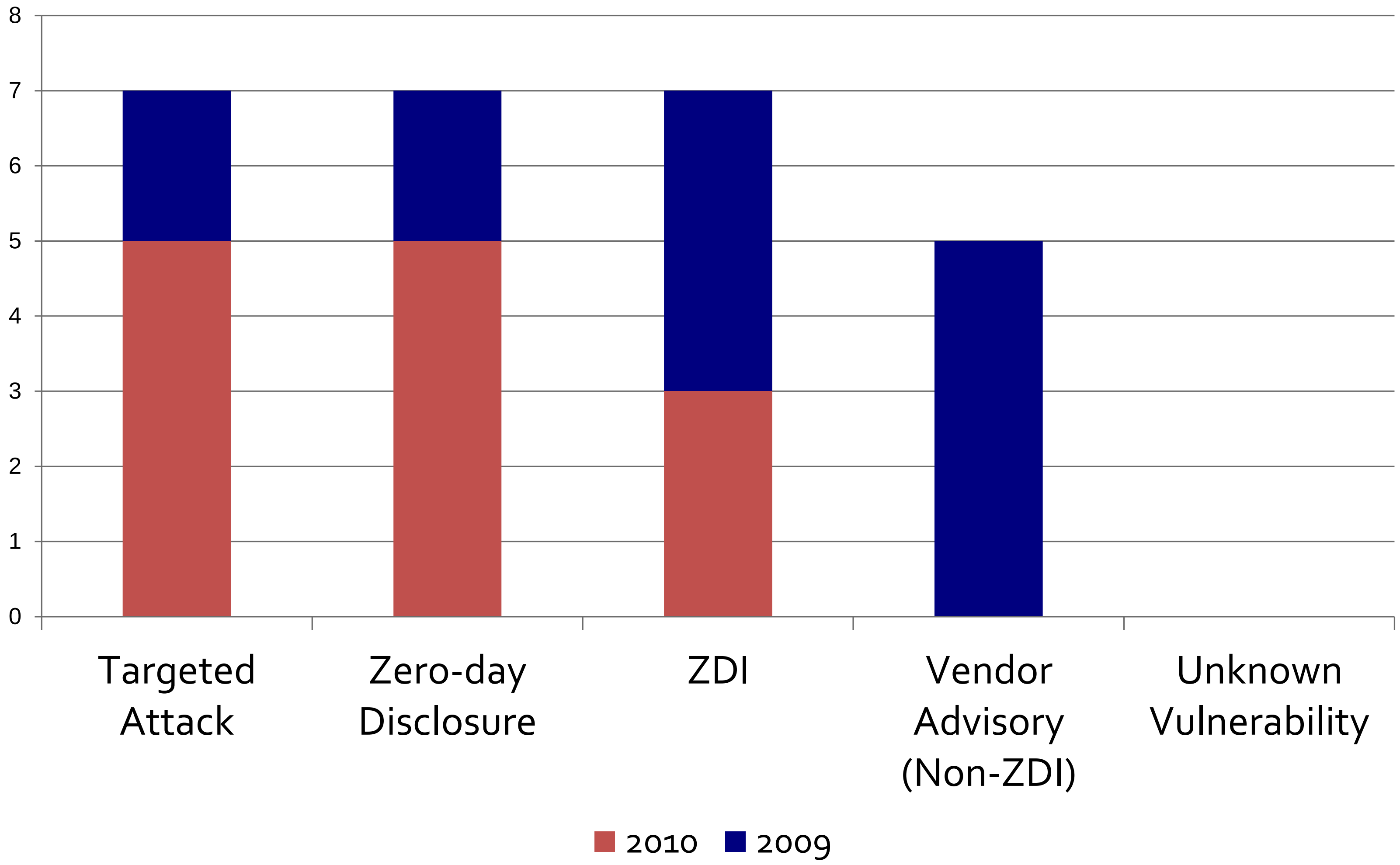
ExploitDB-14843
OSVDB-67705
Zero Day Initiative? No
Discovery Location? Whitehat

Targets Attacked (2010)



Exploitation is focused on dominant platforms (check statowl.com)

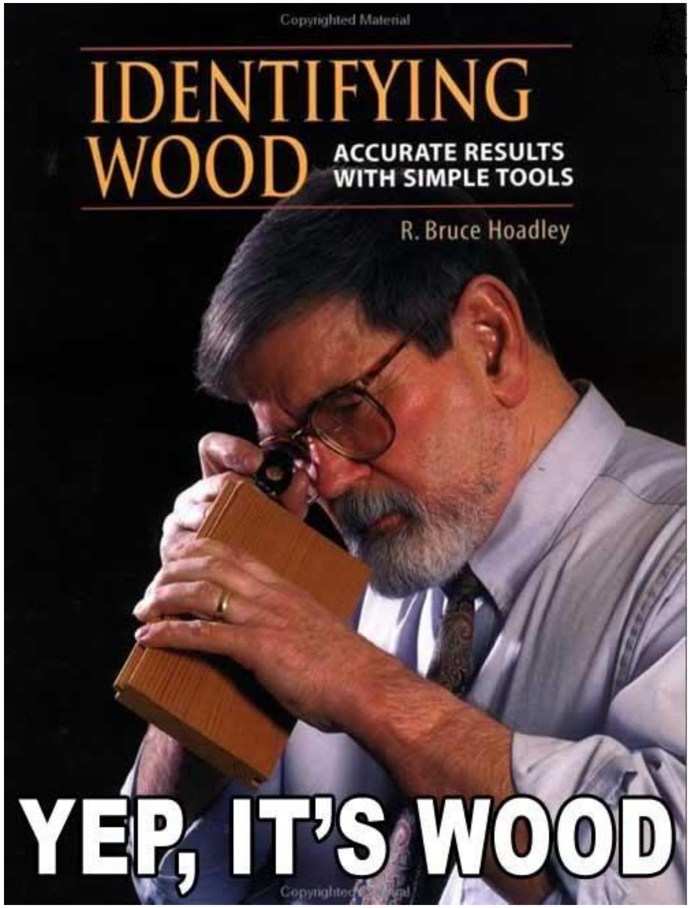
Vulnerability Origin (2009-2010)



iSEC PARTNERS

Where were massively exploited vulnerabilities first disclosed?

Effective Analysis



Evaluate Your Defenses

- Intelligence gives us data to evaluate our defenses and verify they work as intended

- Jan 1, 2009 – what can we put in place to mitigate all exploits for the next two years?
  - Restrictions: *no patching allowed*
  - There are ALWAYS more bugs

- Corporate Desktop circa 2009
  - Internet Explorer 7, Firefox 3.0
  - Adobe Reader 9, Java, Quicktime, Flash, Office 2007
  - Windows XP SP3

Effective Defenses (2009-2010)

Memory Corruption (19)	
Defeated by DEP	14
Defeated by ASLR	17
Defeated by EMET	19

Logic Flaws (8)	
No Java in Internet Zone	4
No EXEs in PDFs	1
No Firefox or FoxIt Reader	2

The Myth of Sophistication

"I don't presume that a bug discovered by a researcher can't be exploited by malware writers. Some are very capable."

DEP Bypasses (2009-2010)

Reader	CoolType SING	APT
~~Reader~~	~~libTIFF~~	~~APT~~
~~Flash~~	~~newfunction~~	~~APT~~
~~Java~~	~~getSoundBank~~	~~kf~~
Quicktime	_Marshaled_pUnk	reversemode

Even the “advanced” exploits come with heavy limitations

Logic Flaws

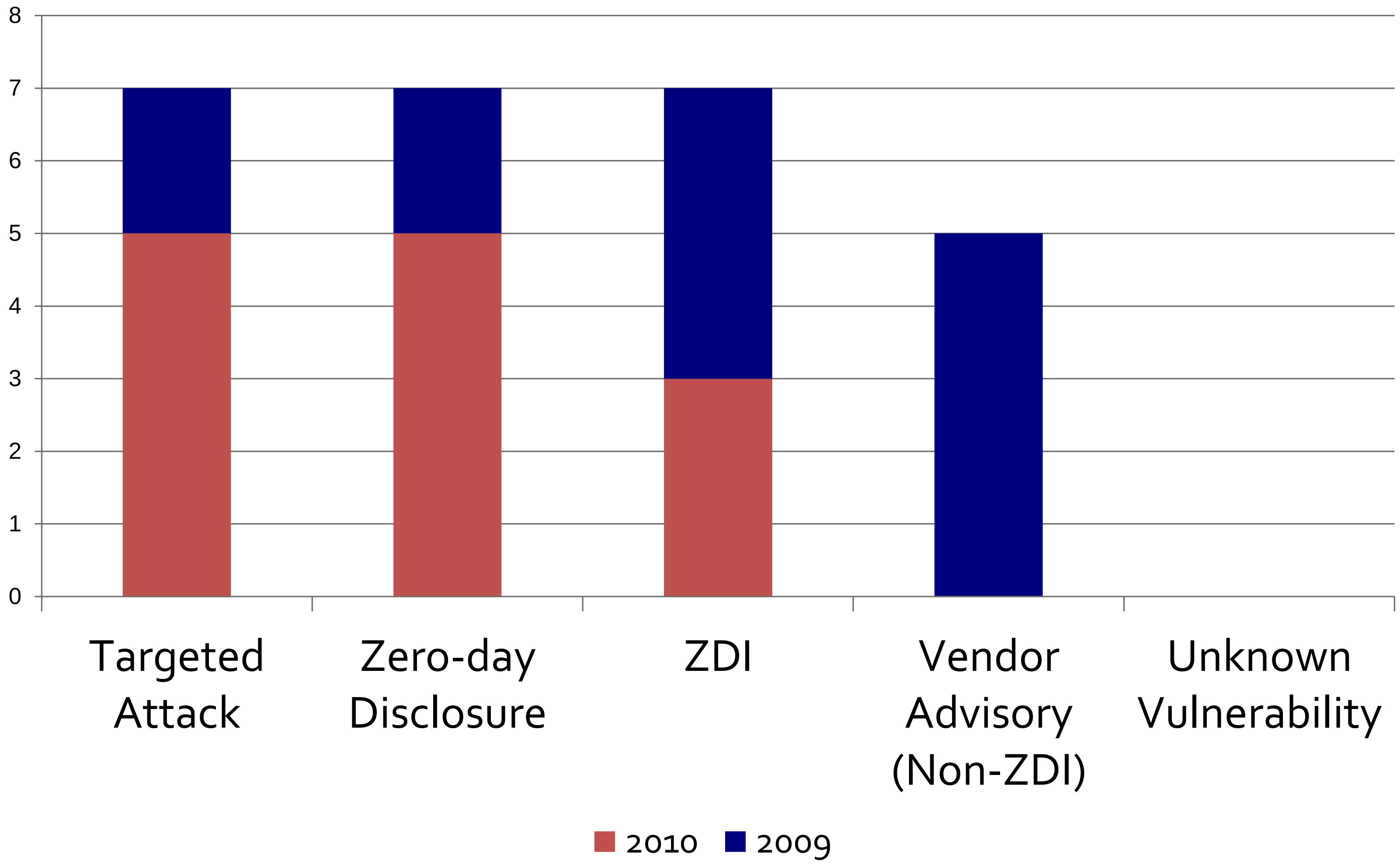
Java	Calendar Deserialization	Sami
Java	Trusted Method Chaining	Sami
Java	WebStart	Tavis
Java	URI Argument Injection	Tavis
IE	Help Center XSS	Tavis
FoxIt	Auth Bypass	Didier
Reader	PDF Social Engineering	Colin
Firefox	SessionStore	moz_bug_r_a4

The Myth of Sophistication

DEP Bypasses (5)	
Developed by APT	3
Developed by Whitehats	2
Developed by Malware Authors	0

Logic Flaws (8)	
Discovered by APT	0
Discovered by Whitehats	8 (!)
Discovered by Malware Authors	0

Public Exploit Code Preferred



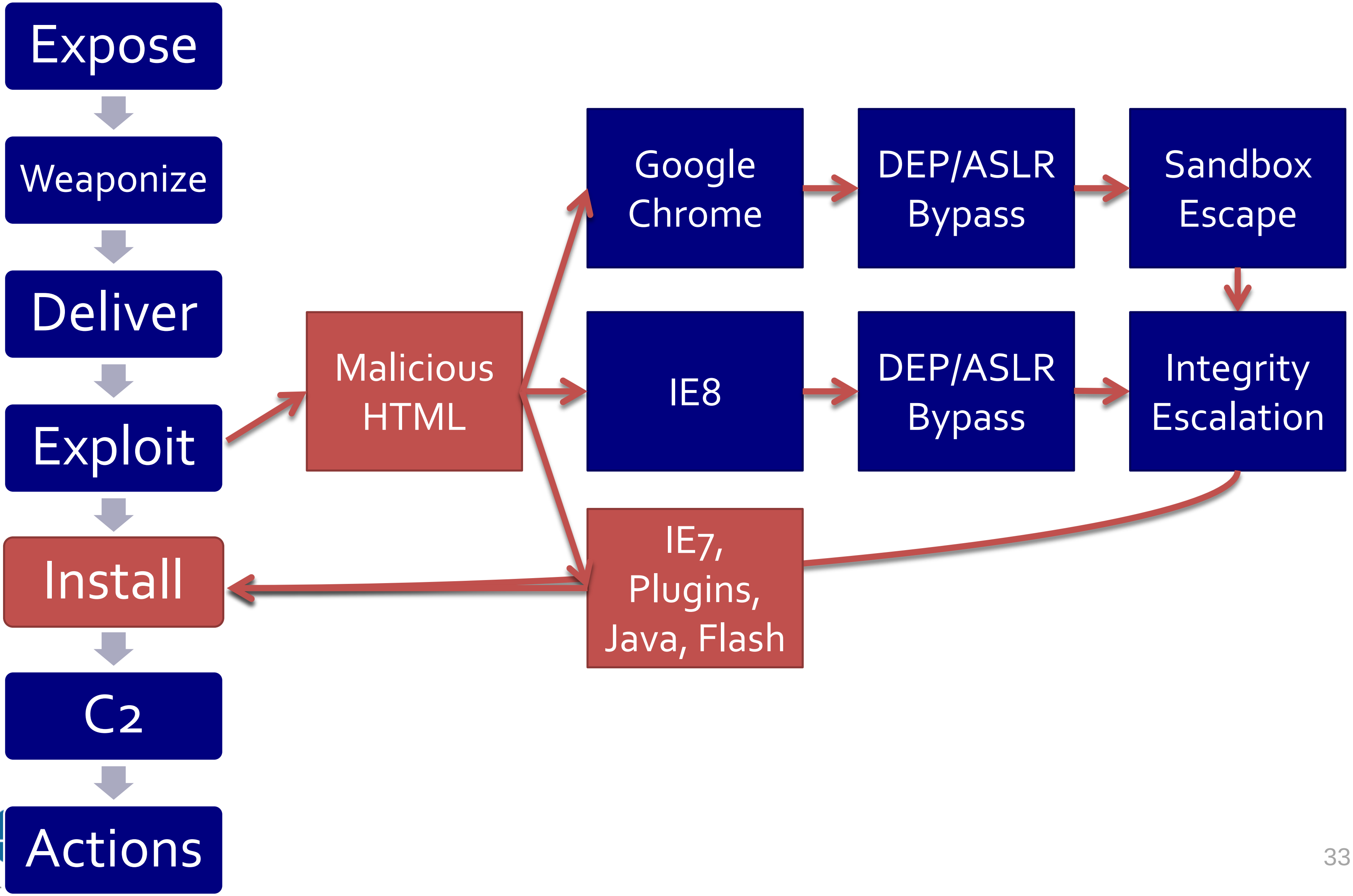
Gradient of Information Detail →

The Defender’s Dilemma?

Defending successfully is making no mistakes.

Don’t make mistakes and you won’t get hacked, guaranteed.

Basic Browser Attack Graph



Expose

Weaponize

Deliver

Exploit

Install

C2

Actions

Malicious HTML

Google Chrome

DEP/ASLR Bypass

Sandbox Escape

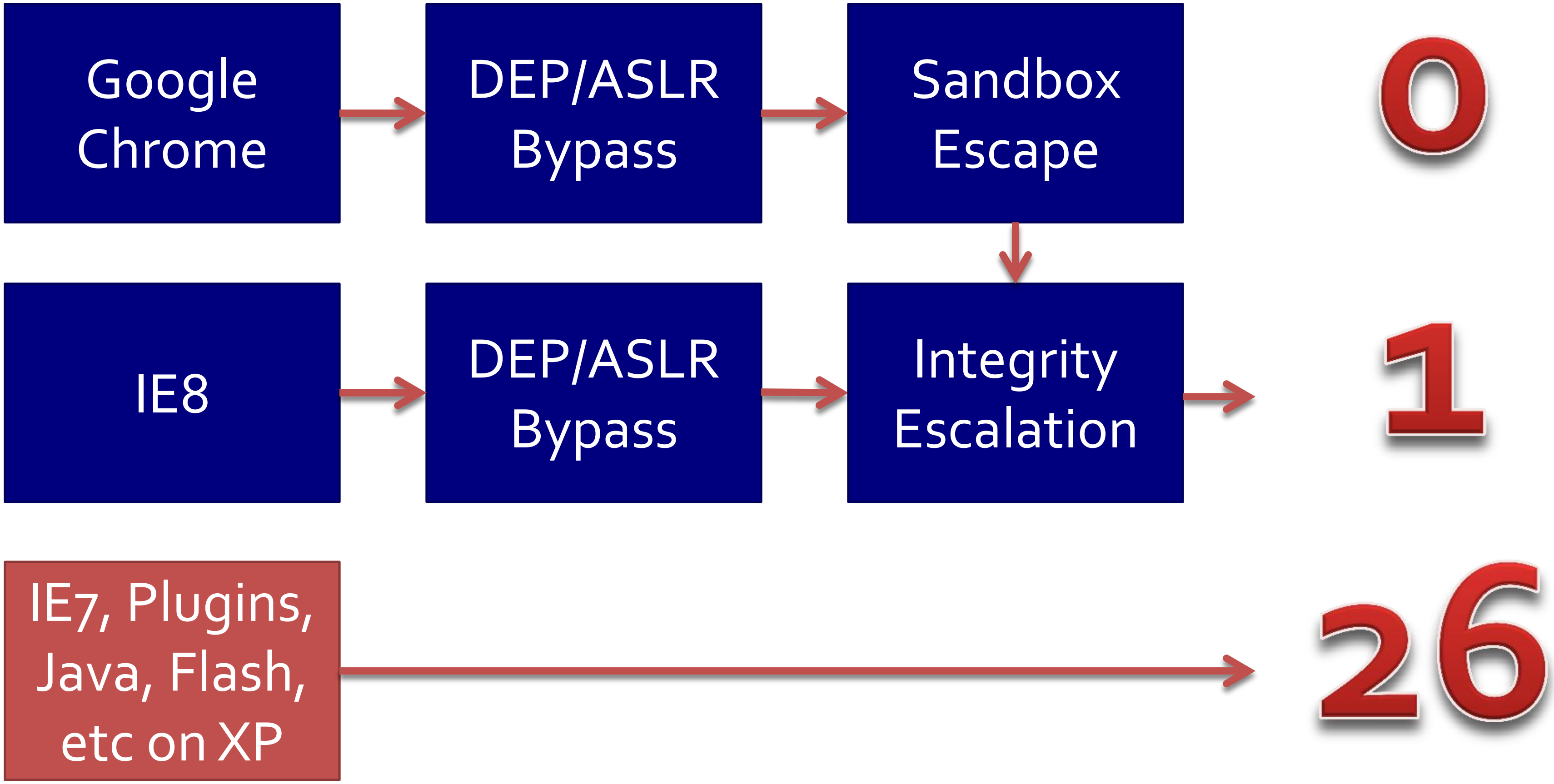
IE8

DEP/ASLR Bypass

Integrity Escalation

IE7, Plugins, Java, Flash

Attack Graph Traversals (2009-2010)



Google Chrome → DEP/ASLR Bypass → Sandbox Escape → Integrity Escalation

IE8 → DEP/ASLR Bypass → Integrity Escalation → 1

IE7, Plugins, Java, Flash, etc on XP → 26

Intelligence-Driven Conclusions

- Start making vaccines and fighting your adversaries
  - Find their resource constraints and attack them!
  - Benchmark your defenses against attack data
  - Create and maintain an attacker’s dilemma

- Mass Malware Authors Case Study
  - Can’t write exploits and rely on public disclosures
  - Can’t evade simple defensive techniques
  - Choose predictably easy targets

Related Work

- UCSD, Oakland 2011 – Holistic Analysis of Spam
  - "Click Trajectories: End-to-End Analysis of the Spam Value Chain"
- Mike Cloppert, ICIW 2011 – Holistic Analysis of APT
  - "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"
- Dino Dai Zovi, SOURCE Boston 2011 – Attack Graphs
  - "Attacker Math 101"
- Microsoft, SRD Blog – Exploit Mitigations
  - "Mitigating Software Vulnerabilities" Whitepaper