

QUARESSO

The Web Browser As A New Perimeter

***pe·rim·e·ter* Noun /pə'rimɪtər/**

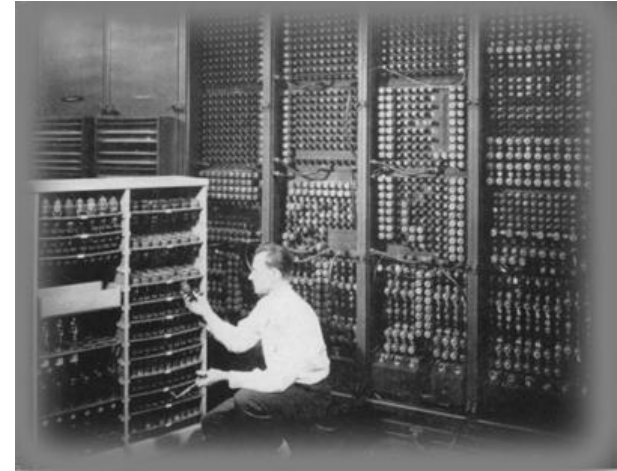
The continuous line forming the boundary of a closed geometric figure.





Perimeter c.2000

- ▶ Good old days: Well defined boundary
 - Simpler external connectivity needs
 - Internet access not critical to business
 - Less data leaving physical boundaries
 - By network, storage media, mobile devices
 - More benign malicious software environment
- ▶ Operational response:
 - Main focus was on gateway(s) between intra and inter Net
 - Encrypt (VPN) data in transit on public networks
 - Malware was mainly availability / downtime issue
- ▶ Physical network boundary was information protection boundary

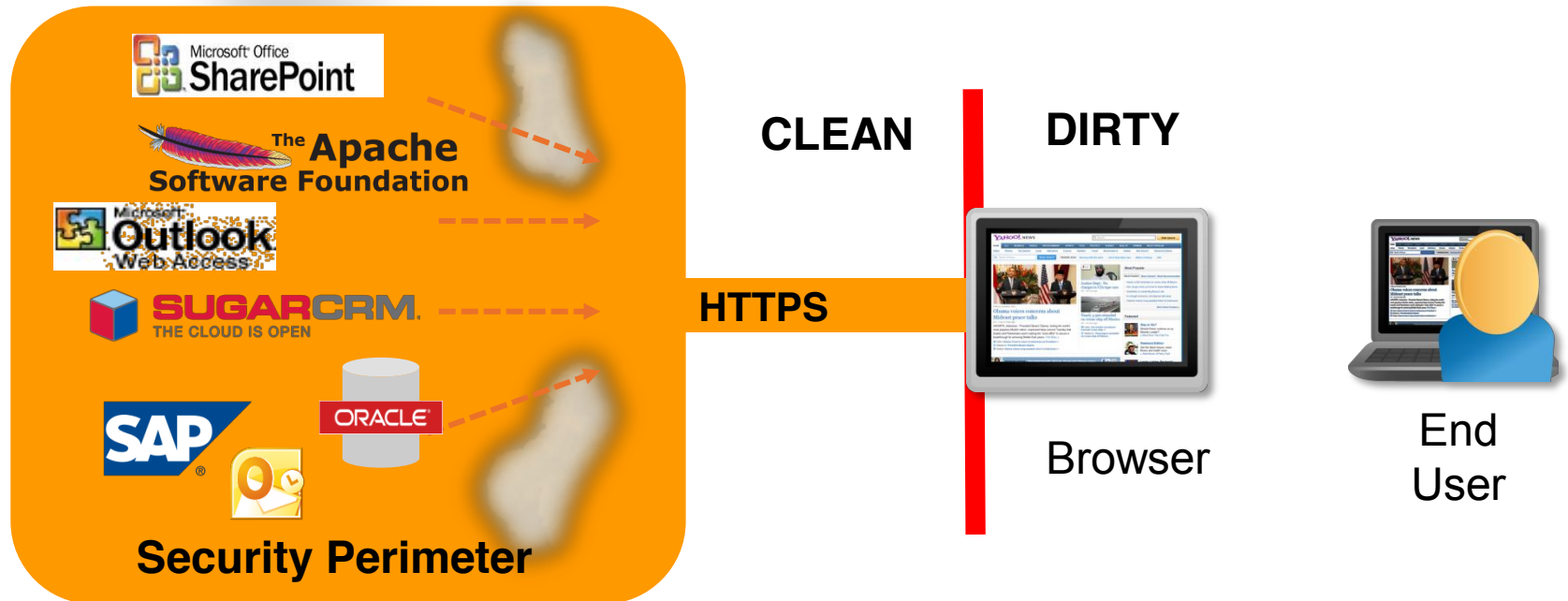


Where the perimeter is today



- ▶ Hard to discern today's boundary
 - External connectivity is business critical
 - Many participants: employees, partners customers
 - Critical data and / or transactions travel outside of perimeter
 - Network mobility, consumerization of IT increase gateway bypass
- ▶ Operational response:
 - Wide use of end-to-end crypto, tunneling through gateways
 - Many orgs begin treating internal networks as “dirty”
- ▶ Physical and information security boundaries no longer align
Enterprise SaaS adoption will accelerate this trend

Web Browsers As A New Perimeter?



- ▶ InfoSec ultimately about protecting data and transactions
- ▶ New boundary: where ciphertext becomes cleartext

Data Loss is Having Devastating Impact



E-News
June 13, 2011

Many employees would sell corporate information, finds study

Research from SailPoint found many employees in one country would be willing to steal corporate data and sell it for profit

By Joan Goodchild, CSO
July 26, 2011 02:31 PM ET

RSA breach
'Extremely so

By Dan Goodin
Posted in Enterpr
Get a free report ar

Attackers breach
compromise the
access sensitive

FT.com
FINANCIAL TIMES

Although potentially devastating, these breaches are preventable, Litan says. "These types of attacks can be stopped with a layered fraud-prevention approach that starts with secure browsing and includes multiple layers of user and account monitoring, and appropriate interventions."

Avivah Litan, Gartner Group "IMF Attack: 1 of Dozens of Breaches?"

IMF Attack: 1 of Dozens of Breaches?

Analyst Says 'It's Time to Roll Out the Defenses'

by Tracy Kitten



Avivah Litan

ional Monetary
t Avivah Litan
I have not been

/ shows 75%
a in 2010

t research from the
% of UK businesses
ph

CE COMMENT BLOGS CULTURE TRAVEL LIFESTYLE
panies Technology Reviews Video Games Start-Up 100 Tech

Front page
World
Companies
Energy
Industrials
Transport
Retail & Consumer
Health

FT Home > Companies > Financials > Banks

Citi admits customer data at risk after breach

By Suzanne Kapner in New York

Published: June 9 2011 00:44 | Last updated: June 9 2011 00:44

Citigroup has acknowledged that a computer breach may have given hackers access to the data of hundreds of thousands of bank card customers.

PlayStation Network user data theft

Sony has said it will be emailing around 70 million users of its PlayStation Network after confirming that customer data was stolen during an attack on its servers last week.



Share: [Facebook] [Twitter] [Print]

Recommend 574

Tweet 60

Sony
Technology >
Shane Richmond >
Video Games >
Technology News >
Christopher Williams >

IN TECHNOLOGY

QUARESSO

End point risks to web applications



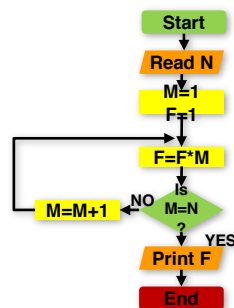
User actions:

- Weak browser settings
- Social engineering
- Malicious user actions
- Careless user actions



Malware:

- Keyloggers
- Framgrabbers
- Data miners
- MITB
- MITM
- Phishers / Pharmers
- ...



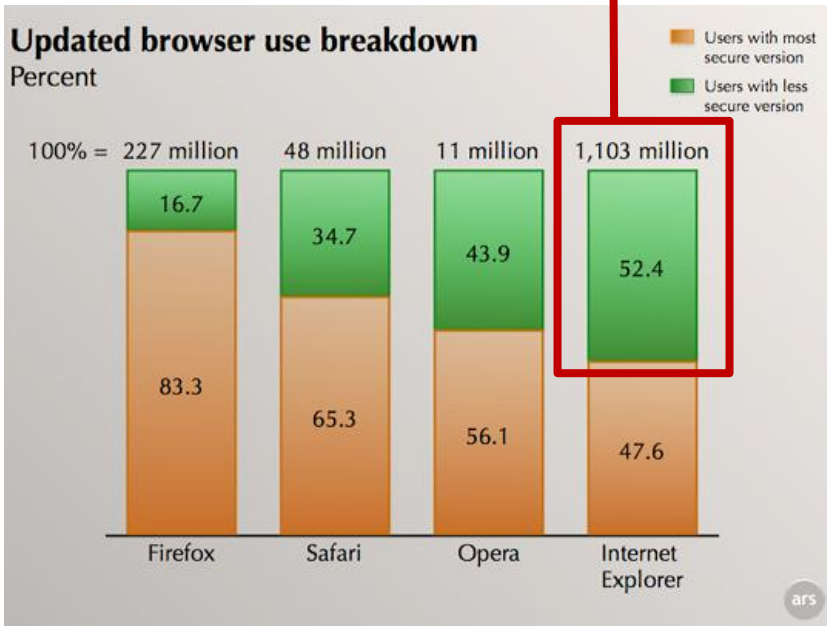
Browser application behavior:

- Caching content
- Disk cookies, history
- Browser plug-ins

Why Worry About Browsers?

Fact: End users are bad sys admins

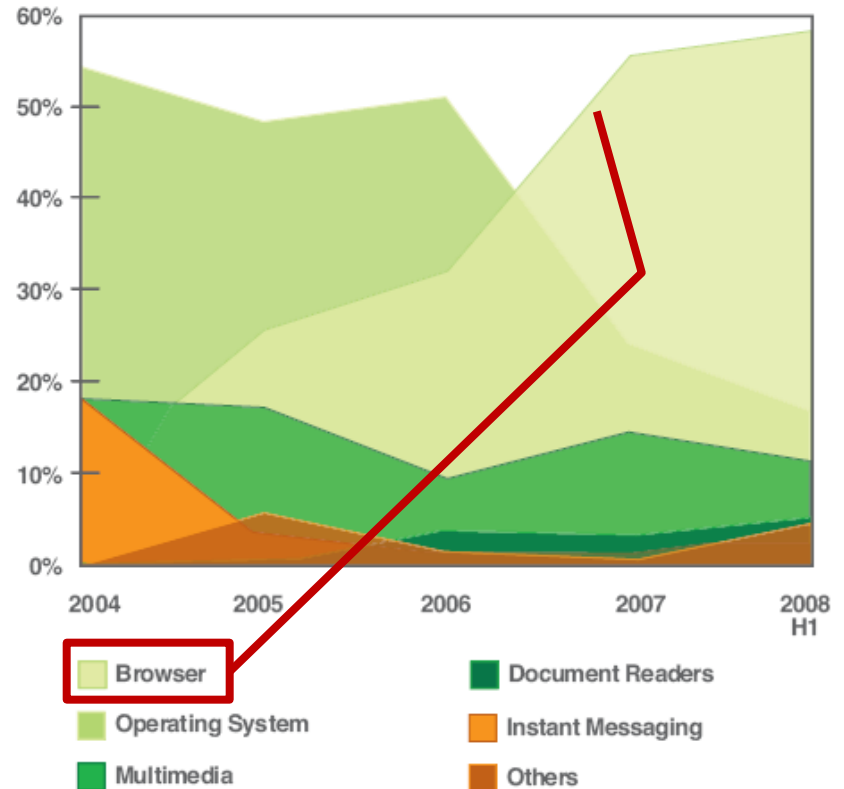
550M IE users alone!



Source: *Understanding the Web Browser Threat*
Google, IBM and Swiss Federal Institute of Technology

Fact: Malware's primary target

Client-Side Public Exploits
by Category



Source: IBM ISS X-Force® 2009 Mid-Year Trend Statistics



Today's malware

▶ Zeus (Ztob, PRG, et al)

- Crimeware toolkit enables scoped attacks
- Multi-function Trojan
- Bot with centralized C & C
- Affected 100M+ PCs
- Data stealing, page rewriting, remote control, data searching, etc.

▶ Attack sequence:

- Bad guy builds package with unique fingerprint
- End user inadvertently loads
 - Many paths: SEO poisoning, plug in vulnerability, etc.
- Trojan established connection to C&C system
 - For functional updates, dropsites
- Lifts login credentials, forms submissions, other data
 - Can be generalized or scoped to specific URLs
- Info sent via log or real time alarms to botmaster
- Detection times from AV 20+ days

abuse.ch ZeuS Tracker

[Home](#) | [FAQ](#) | [ZeuS Blocklist](#) | [ZeuS Tracker](#) | [Removals](#) | [ZTDNS new!](#) | [Statistic](#) | [RSS Feeds](#) | [Contact](#) | [Links](#)

Welcome to the ZeuS Tracker

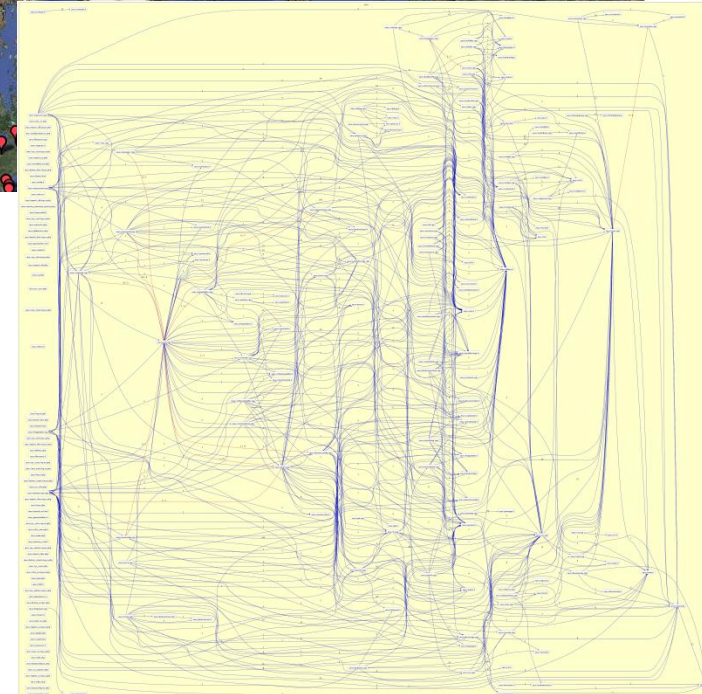
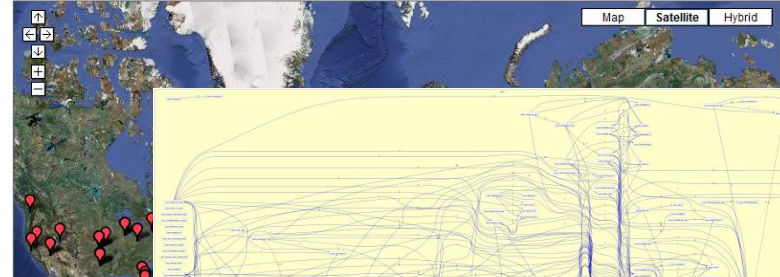
The *ZeuS Tracker* tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the [FAQ](#) or send me a email ([contact](#)).

Here are some quick statistics about the ZeuS crimeware:

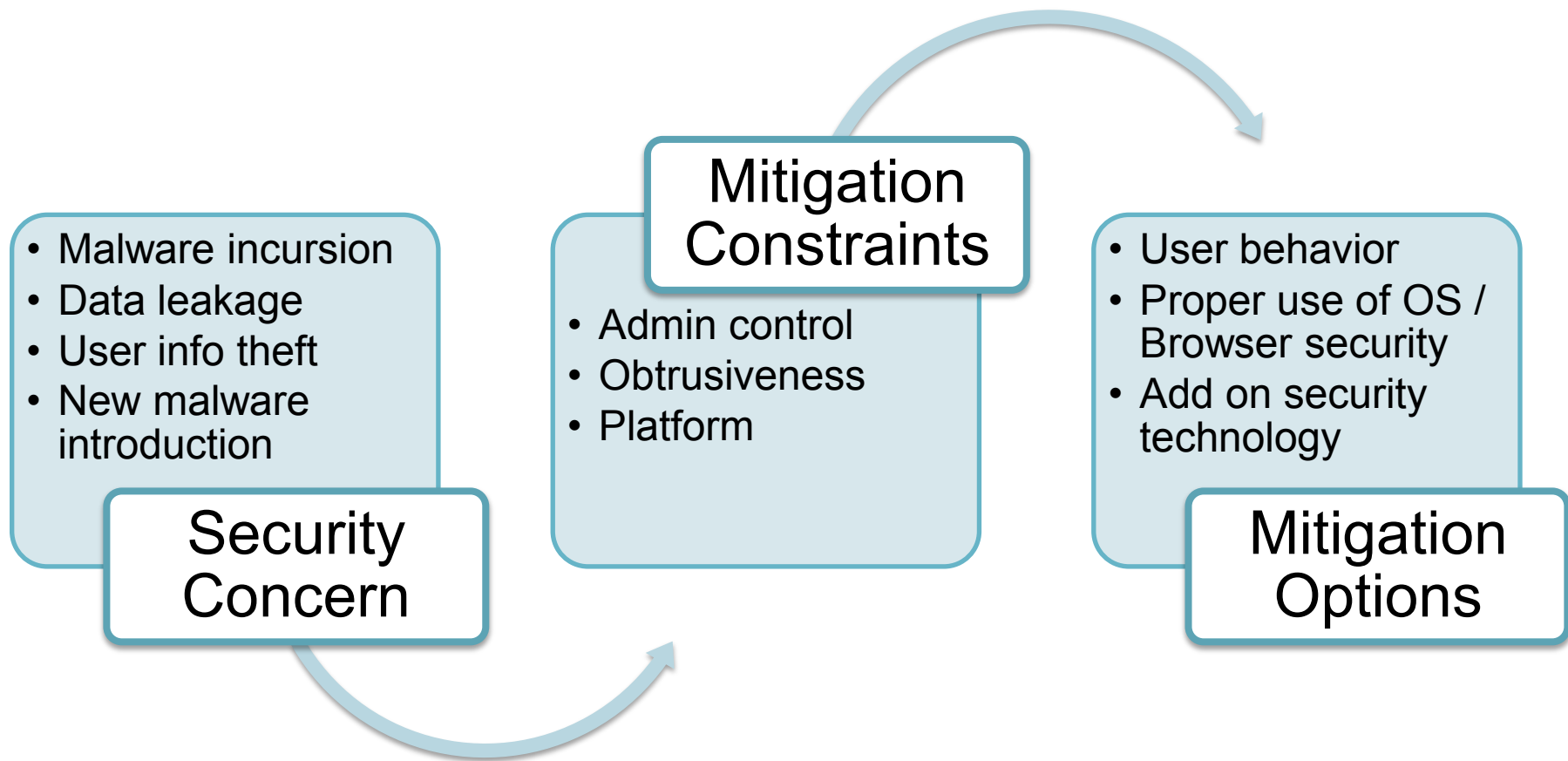
- ZeuS C&C servers tracked: **692**
- ZeuS C&C servers online: **217**
- ZeuS C&C servers with files online: **40**
- ZeuS FakeURLs tracked: **13**
- ZeuS FakeURLs online: **4**
- Average ZeuS binary Antivirus detection rate: **38.87%**

You can find more interesting statistics about the ZeuS crimeware on the [ZeuS Tracker statistic page](#).
The map below shows a dot for each ZeuS Command&Control server (ip or domain).

Note: If you are using IE 6/7 you will get a security warning due to the fact that the Google maps API currently does not support SSL (https).

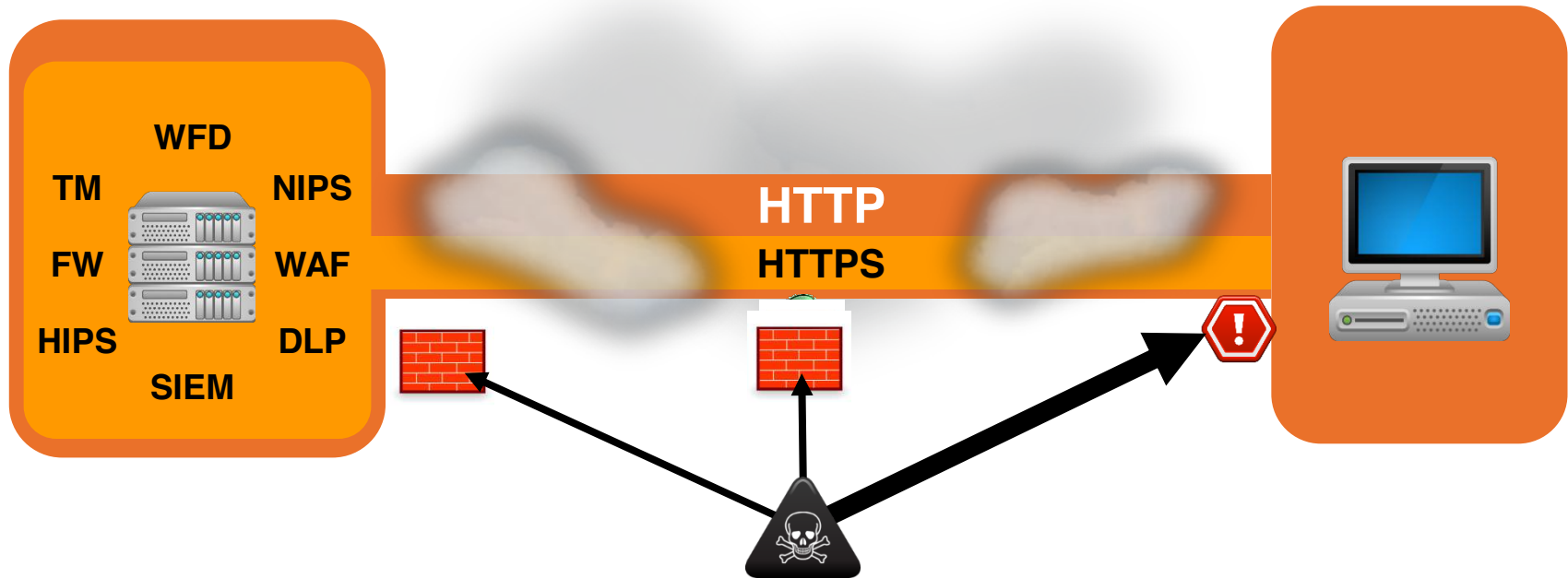


Improving Security At The Browser Perimeter





Big Challenge For High Assurance Web App Owners



What you know

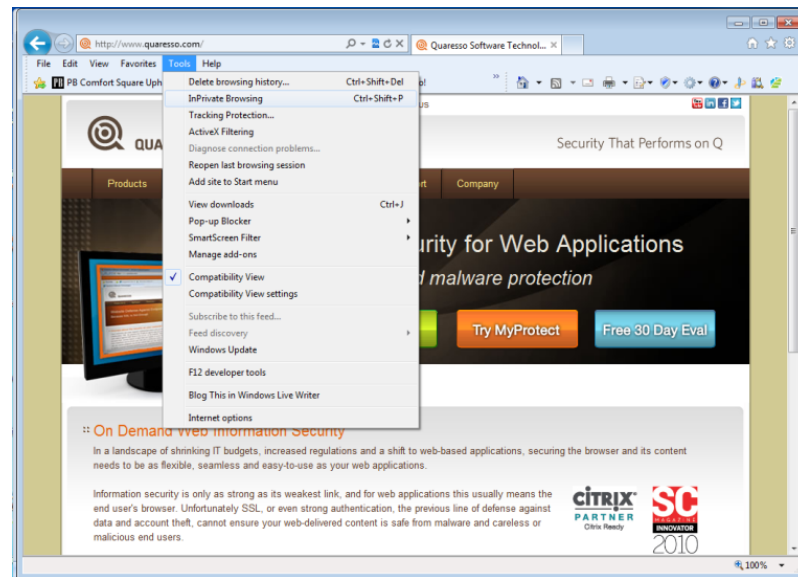
- ▶ User credentials
- ▶ User agent info
- ▶ Data is encrypted to client
- ▶ HTTP requests from client

What you don't know

- ▶ Browser settings / configuration
- ▶ Security state of the end point?
- ▶ Am I really talking to client / MITM?
- ▶ Post consumption data handling

Mitigating Browser Security Risks

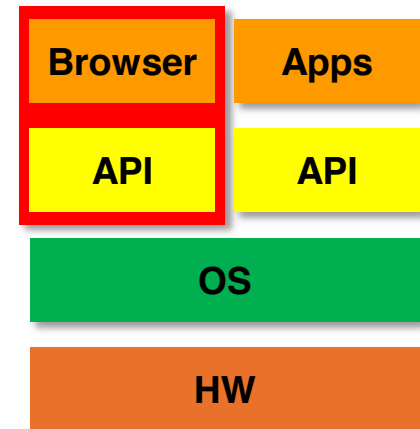
- ▶ Must touch client in some way
- ▶ Utilize browser security features!
 - Private browsing
 - Anti-phishing, malware site blacklisting
 - Download screening
 - Tracking cookie controls
 - Protected Mode - low integrity (Chrome, IE)
- ▶ Layer additional security if requirements dictate
 - Host IPS style products offer better defense against 0 hour
 - Additional technologies recently utilized:
 - Browser Isolation
 - System Isolation





Browser Isolation

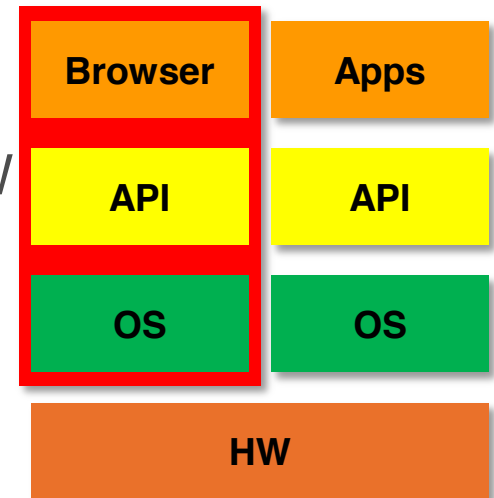
- ▶ Approach: sandbox browser from other applications
 - Using jails, rule based execution, pseudo-VM techniques
 - Some focus on PC protection, others on session protection
- ▶ Implementations: ALL require endpoint SW or HW
 - Plug-in security agents
 - Purpose built browser
 - Web site-pushed agent
- ▶ Pros:
 - Have proven effective against sophisticated malware
 - Solutions for both incursions to and infections from browser
- ▶ Cons:
 - Tough to defeat rooted OSes
 - Often require admin rights or installation rights
 - User involvement may be heavy: configuration, msg pop-ups





System Isolation

- ▶ Places browser in separate OS instance from host
 - Eliminate risks from host OS malware
 - Minimize infection risks from browser
- ▶ Implementations: require client SW and/or HW
 - VM (VDI)
 - System on a Stick
 - “Semi” Virtual Desktops: New Win shell
- ▶ Pros:
 - Provides strong defenses against rootkit-ed machines
 - Pristine OS provides known security state
- ▶ Cons:
 - Heavy user involvement typically required
 - VM host may have malware (key logger) installed





Final Thoughts

- ▶ Browsers are a principle battle ground for security today
- ▶ Browser risks impact both consumers and web app owners
- ▶ For consumers: you are your system's InfoSec Admin
 - On “unknown” systems: exercise extreme caution!
- ▶ For enterprises:
 - Endpoints operating internally: leverage gateway security tools
 - Endpoints operating externally: proxy traffic; endpoint security
- ▶ For high value web applications:
 - HTTPS is almost irrelevant
 - If you cannot control the browser, you have significant threats!



Questions?

About Quaresso

- ▶ Leading provider of on-demand web information protection
 - Securely control information and content at the endpoint.
 - Extend security controls temporarily to web sessions
 - Provide data loss & malware protection wherever users are
 - Significant deployment, support and usability cost savings
- ▶ Headquartered in Austin, TX, USA
 - Privately held, investor-backed company
 - Spun technology out from Blue Coat Systems in April 2008
 - Patented, unique browser information security technology

■ ■ ■ RSA CONFERENCE
INNOVATION SANDBOX



Gartner Cool Vendors in User and Data Security, 2011

QUARESSO

Thank you

