Corporate Exposure Analysis (CEA)

How corporate security breaks in the real world

27 February 2012

nsense

Agenda

- Sarid Harper
- Summary
- CEA Origination
- The problem
- CEA vs. Security Assessments
- Real life
- Is this stuff real?

Sarid Harper

- Started off as a programmer
- Started spotting the bad mistakes “good” programmers were making
- Moved into security
- Worked with security for 10+ years (nsense, secunia, csis, back to nsense :)
- Help create attack scenarios, which reflect reality

Summary

The purpose of this talk is to present a different way of assessing corporate security, which reflects reality much better.

CEA Origination

- Also called penetration testing
- Been around for ages
- Having worked with customers for over 10 years, I felt that the term “pentest” was misused and often misunderstood.

The problem

- Every organisation is (currently) being run by humans and thus psychology (emotions, expectations, etc.)
- Everything and anything that is done in an organisation is based on the decision of a human
- If (when) an attacker is able to leverage the decision making process of at least one human, then the doors of opportunity will fly open (check my Sublime Communication slides)

- *Can you see how important people are for your organisation?*
- *Can you imagine the problems that could be introduced if a bad guy was able to take advantage of your people?*

CEA vs. Security Assessments

- Organisation-wide / limited focus
- Real-life scenarios / pre-defined scenarios
- Real weaknesses / case-specific weaknesses

- Both are necessary

Security Assessment

- Focus is on technology (e.g. applications, operating systems, sub-systems)
- Due to tight budgets, assessment focus is often forced away from the real problems
- Poor ROI regarding security awareness (isn't security awareness what it's all about?)

- **Customer:** *"We know that X is a problem for us, so we don't need to focus on that"*

- **Me:** *"WTF, and you're ok with that?"*

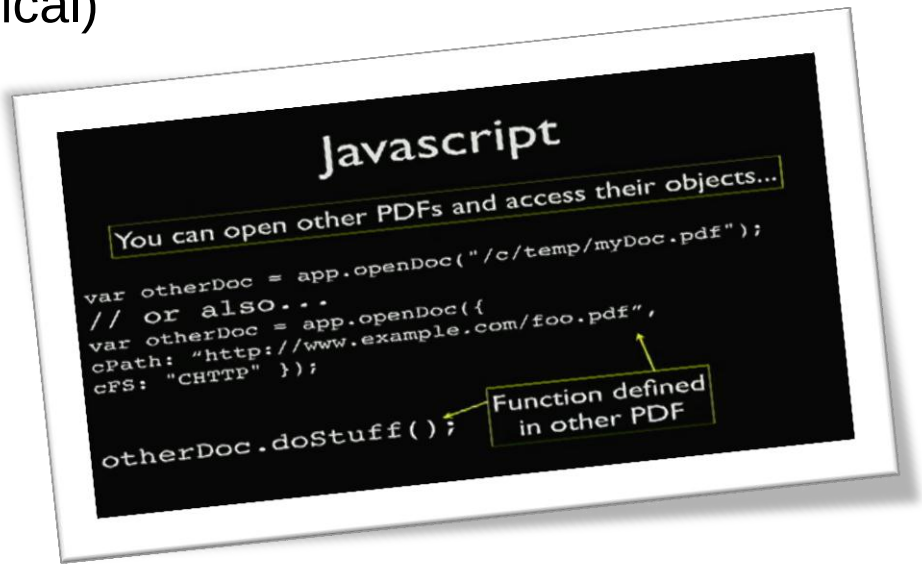
Corporate Exposure Analysis (CEA)

- Focus is on the organisation in its entirety (e.g. people, physical presence, technology)
- Vectors focus on the real risks, the people

Real Life

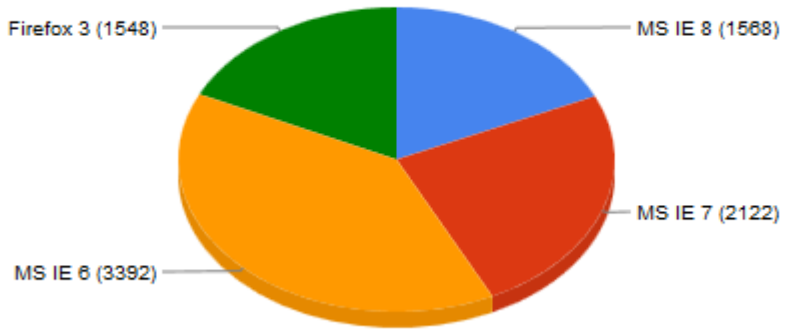
How the bad guys really get in

- Social Engineering (check my slides entitled Sublime Communication)
- Physical access (e.g. UK Medical)
- Spear-phishing
- Phishing (e.g. credentials)
- Drive-bys
- Devices (e.g. mobile)

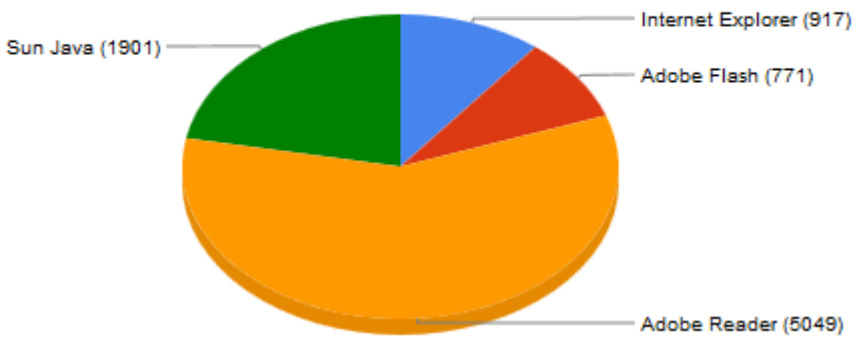


- *You may be wondering how this is possible..*

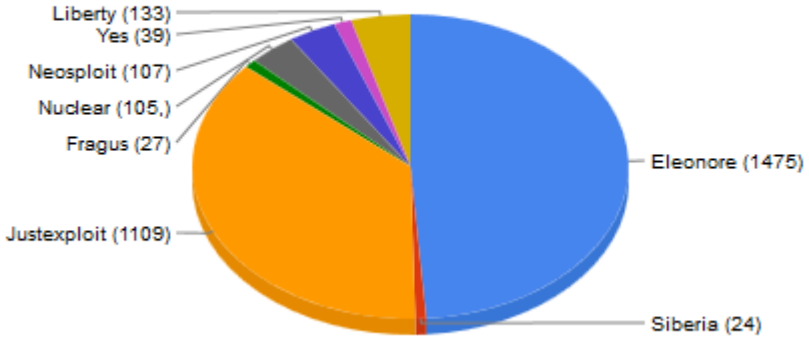
Browser Infection Rate Per Drive-by Exploit



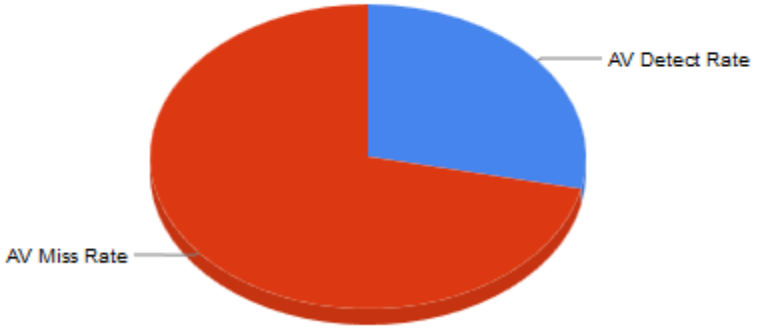
Applications Targeted by Drive-by Exploits



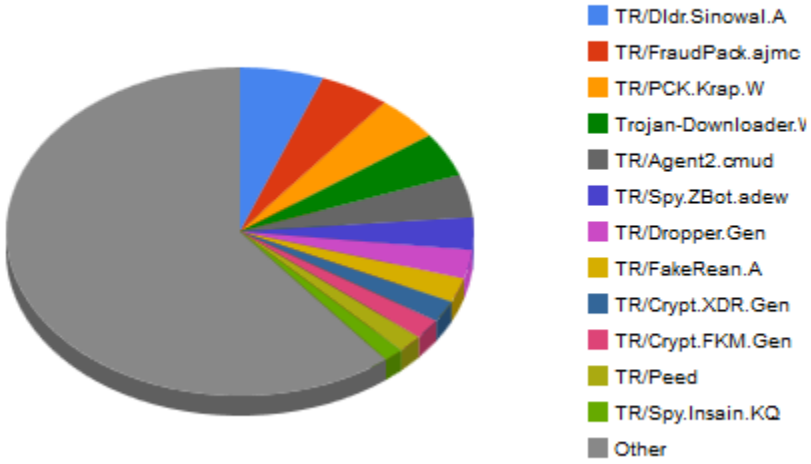
Exploit Kits and Attack Pack Usage



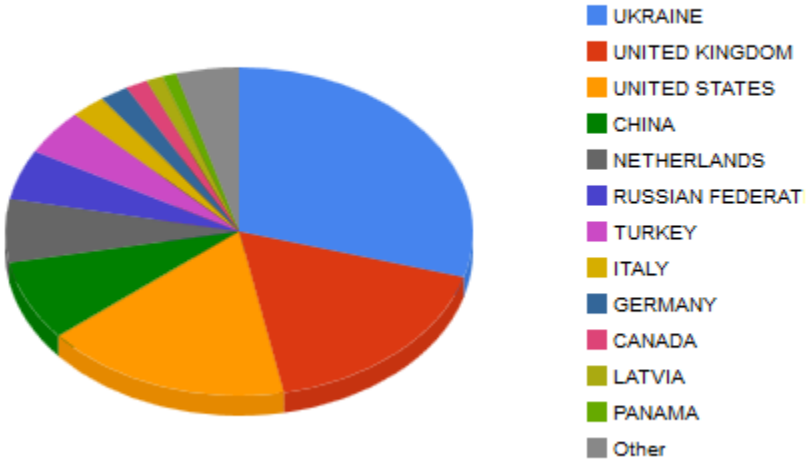
VirusTotal Detect/Miss Rates of Drive-by Exploit Binaries



TOP 12 Malware Families Downloaded from Drive-by Exploits



TOP 12 Countries Serving Active Drive-by Exploits



Real Life

How attacks are performed in real life (1/2)

- Know the target / goal / objective
- May or may not know where it is (A)
- May or may not know which people are associated with target (B) *(e.g. The Mainframe programmer on Linkedin)*
- Information Gathering (IG) / analysis (A, B)
- Decide which vectors will be the most successful based on IG (e.g. use of social networks & technologies)

Real Life

How attacks are performed in real life (2/2)

- Compromise targets (e.g. spear-phishing) *(e.g. Polish admin)*
- Positioning analysis (where are we in relation to where we need to be)
- Target acquisition (e.g. screen dumps, emails, files)
- Access maintenance / removal

Know the target / goal / objective

- Intellectual property
- To introduce the ability to securely leak information
- To raise hell (e.g. briberies)
- Specific data
- Emails
- Application access

- *E.g. SCADA (ability to manipulate stuff)*

May or may not know where it is

- Geographical locations
- File servers
- Network segments

- *E.g. network*

Information Gathering

- Pertains to the targets (e.g. building, people, systems)
- What information regarding our target can we find?
- Can this information be exploited?
- Social sites (e.g. Facebook, Linkedin)

Vectors

- Looking for ways in
- Knowing their weaknesses (e.g. software)
- Spear-phishing
- Phishing sites / drive-bys
- Storage media

Compromise Targets

- Phishing emails (Sublime Communication)
- Physical material (e.g. CDROM, USB, free gifts)
- Payloads have been deployed, wait and monitor (e.g. spear-phishing, phishing)
- Social Engineering activities

Positioning analysis

- This is all about figuring out where you are in relation to where you need to be
- Do we need to hop onto another network?

Target acquisition

- Getting / do what you came there to get / do

Access Maintenance / Removal

- Has the target been reached or does remote access need to be established to enable target acquisition at a later time? Do we need to wait?

Is this stuff real?

- 48% of enterprises surveyed admitted to having being victims of Social Engineering
- 25% within the past 2 years
- Survey participants estimated damages to be between $25K $100K
- Methods
  - Phishing mails → 47%
  - Social networking → 39%
  - Mobile devices → 12%

Remediation

- Security awareness
- Update third party software packages
- Local user privileges
- Network segmenting
- Etc.

Thank you!