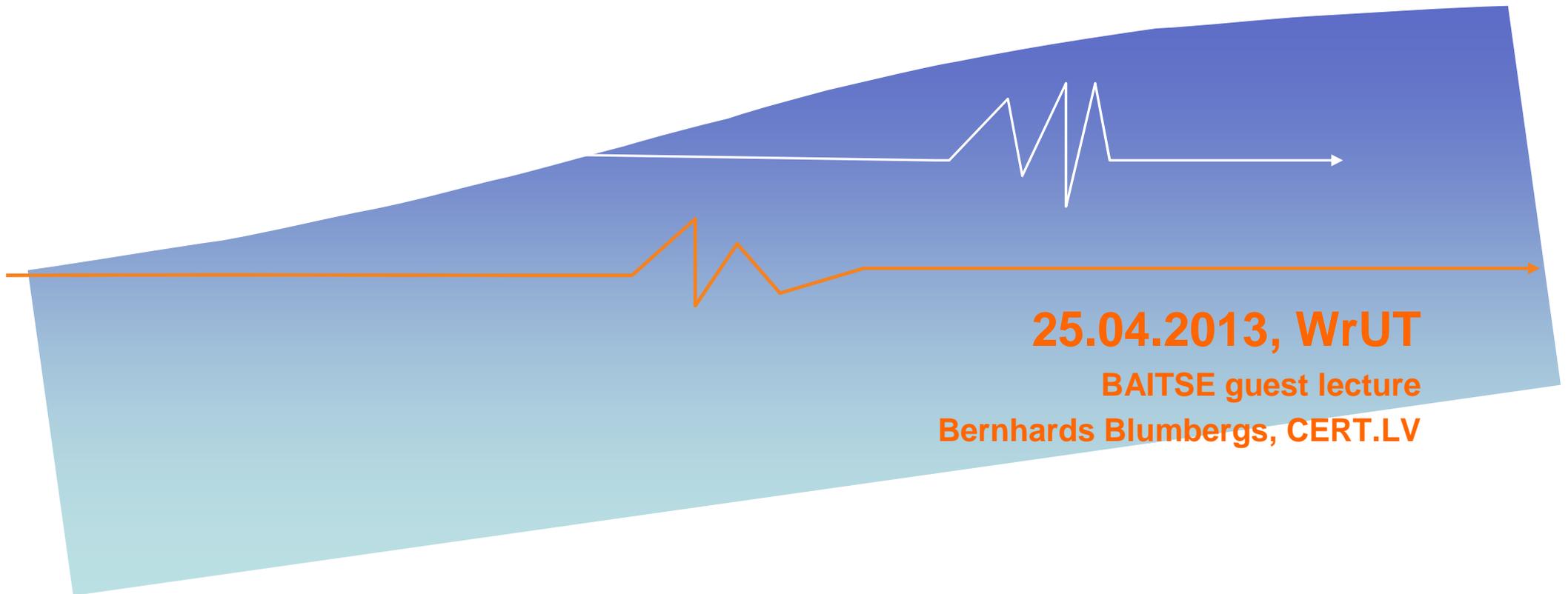




Introduction to network penetration testing



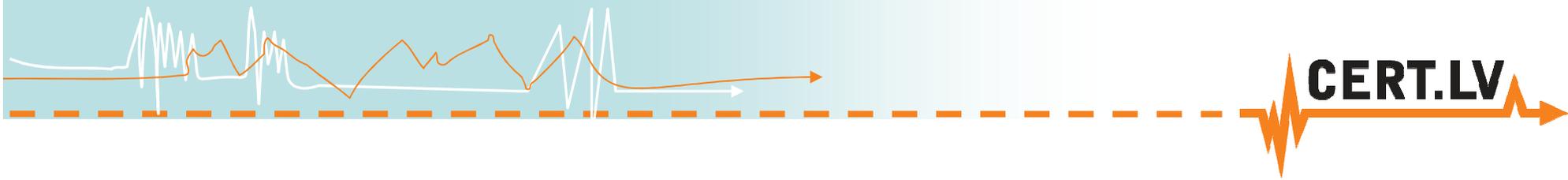
25.04.2013, WrUT

BAITSE guest lecture

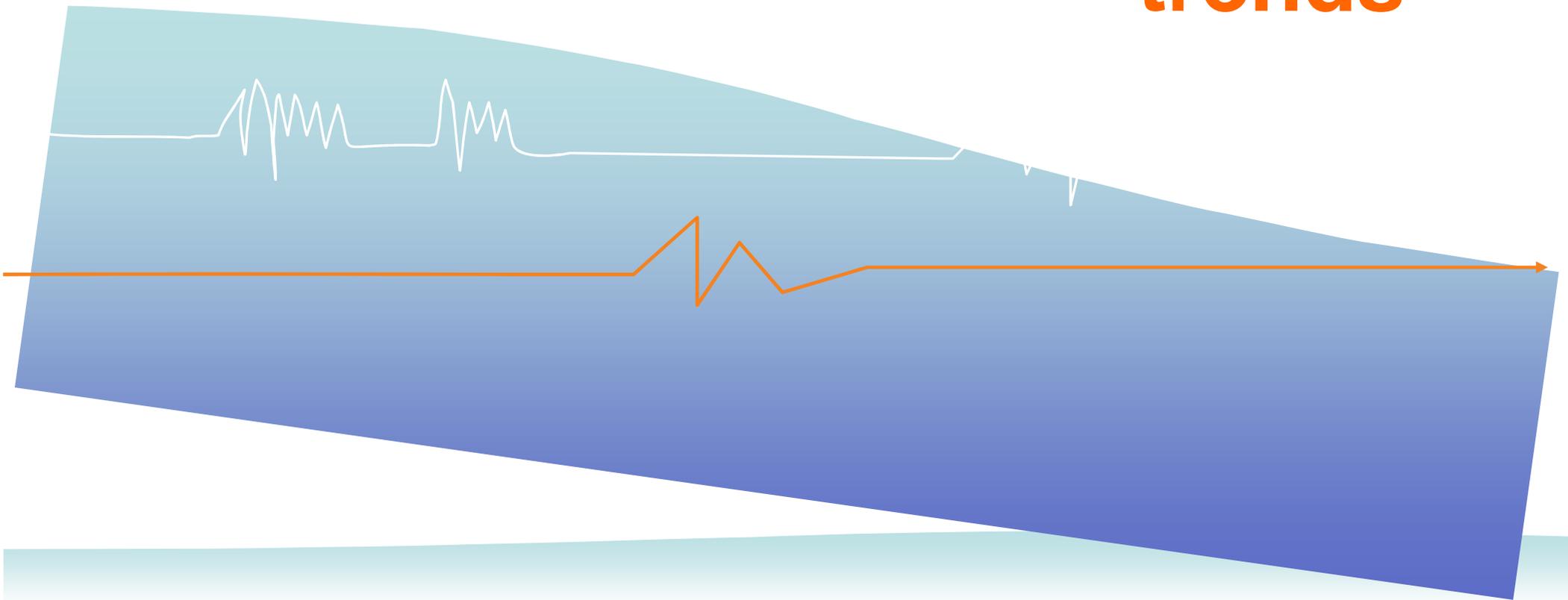
Bernhards Blumbergs, CERT.LV

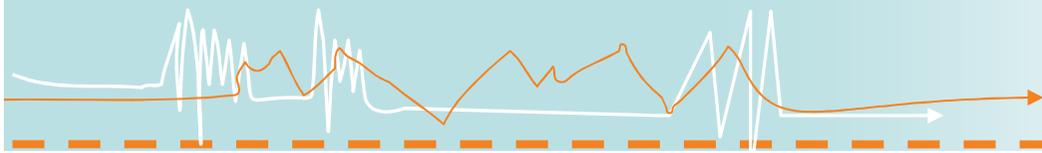
Outline

- Current IT security trends
 - IT Security principles
 - The need for IT security testing
 - Terminology explained
 - Applicable standards and models
 - Reporting results
- 



Current IT security trends

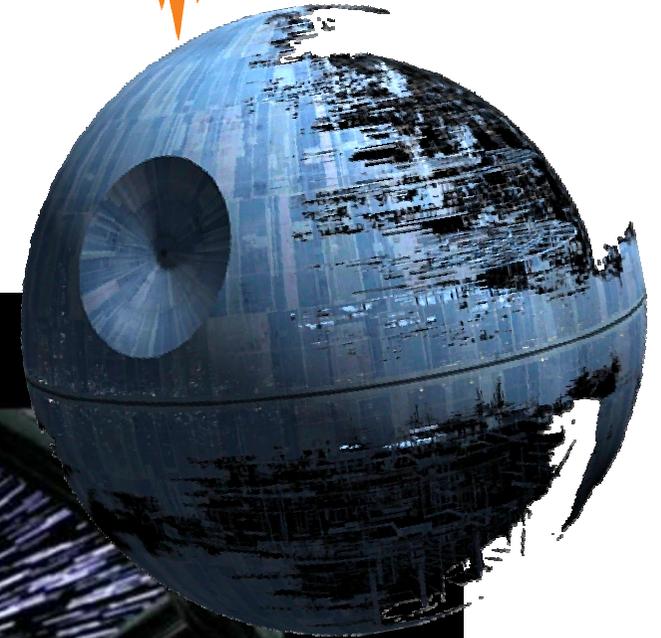




CERT.LV

Not long time ago...

- In a galaxy nearby....



The story so far...

- Cyber warfare

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD"))())
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.TABLE_EXT"))())
    if not __LIB_FLAME_PROPS_LOADED__ then
      LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MARRON"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECONDS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG_KEY = "SUCCESSFUL_INTERNET_TIMES_CONFIG_KEY"
      flame_props.INTERNET_CHECK_KEY = "CONNECT"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH"
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get(flame_props.FLAME_ID_CONFIG_KEY)
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
      end
    end
  end
end
```



The story so far...

- Revenge attacks

Three tweets from TheSTOPhaus Movement (@stophaus) dated 25 Mar:

- Tweet 1: @bernieleung @cloudfare @spamhaus although we (cb3rob) still support the ddos effort, in the long run, there need to be other steps.
- Tweet 2: @bernieleung @cloudfare @spamhaus killing the zen.spamhaus.org zone by giving false positives will be the way to go to end spamhaus.
- Tweet 3: @bernieleung @cloudfare @spamhaus spamhaus: our bgp injection seems to work, we'll find a larger business partner (@chinanet? ;) to run it.

SPAMHAUS

Navigation menu: Home, SBL, XBL, PBL, DBL, DROP, ROKSO

Subscribe to RSS News Feed

SPAMHAUS NEWS

Answers about recent DDoS

Spamhaus Hit With 'Largest Publicly Announced DDoS Attack' Ever, Affecting Internet Users Worldwide

SATTER  
3/27/2013 7:47 pm EDT

RISK ASSESSMENT / SECURITY & HACKTIVISM

When spammers go to war: Behind the Spamhaus DDoS

The story behind the 300Gb/s attack on an anti-spam organization.

The story so far...

- Botnets

Zeus :: Statistics

Information:

Profile: ██████████
 GMT date: 11.03.2009
 GMT time: 14:15:27

Statistics:

→ Summary

Botnet:

Online bots
 Remote commands

Logs:

Search

Information:

Total logs
 Time of first
 Total bots
 Total active bots

Botnet: Any >>

Installs (137)	Reset
GB	32
--	23
RU	19
US	19

Security

THE SMARTPHONE ZOMBIES COME

Recognize and fend off mobile botnets

09.04.2013 | by Oliver at Shek



Beware! DNS Changer's IP Blocks are re-allocated and advertised!

On August 11, 2012 By bgreene

From Senki.org By bgreene On August 10, 2012 · As of Friday morning (August 10, 2012), the IP address blocks us by the Rove Digital criminal operations have been re-allocated by RIPE-NCC and advertised to the Internet:

<http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRCO01&query=1&arg=85.255.112.0%2F20> Read Full Article →

twitter



upd4t3

Follow

aHR0cDovL2JpdC5seS8xN2Ezd...

about 2 hours ago from web

aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYmI0Lm...

about 2 hours ago from web

aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN...

about 4 hours ago from web

aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYmI0Lm...

about 4 hours ago from web

aHR0cDovL2JpdC5seS9HaHVvdSBodHRwOi8vYmI0Lm...

about 5 hours ago from web



The story so far...

- Espionage

15 January 2013, 16:16

Operation Red October - large-scale cyber-espionage uncovered

Security experts at [Kaspersky Lab](#) have apparently [uncovered](#) a massive case of cyber-espionage. An [analysis](#) published on Monday states that computer networks in diplomatic missions, government and trade organisations, energy companies, and research, aerospace and military institutions have been infiltrated for an estimated five years. A sophisticated infrastructure appears to have enabled the unknown hackers to make off with terabytes of highly confidential geopolitical information and other data.

Kaspersky reports that it first found indications of the existence of the espionage infrastructure,

The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor



GReAT

Kaspersky Lab Expert

Posted February 27, 14:00 GMT

Tags: Adobe PDF, Obfuscation, Data Encryption, Targeted Attacks, Adobe, Vulnerabilities and exploits

(or, how many cool words can you fit into one title)



The structure of the command and control servers serves to conceal the actual point of origin

Source: [Kaspersky Lab](#)

Microsoft releases law enforcement figures

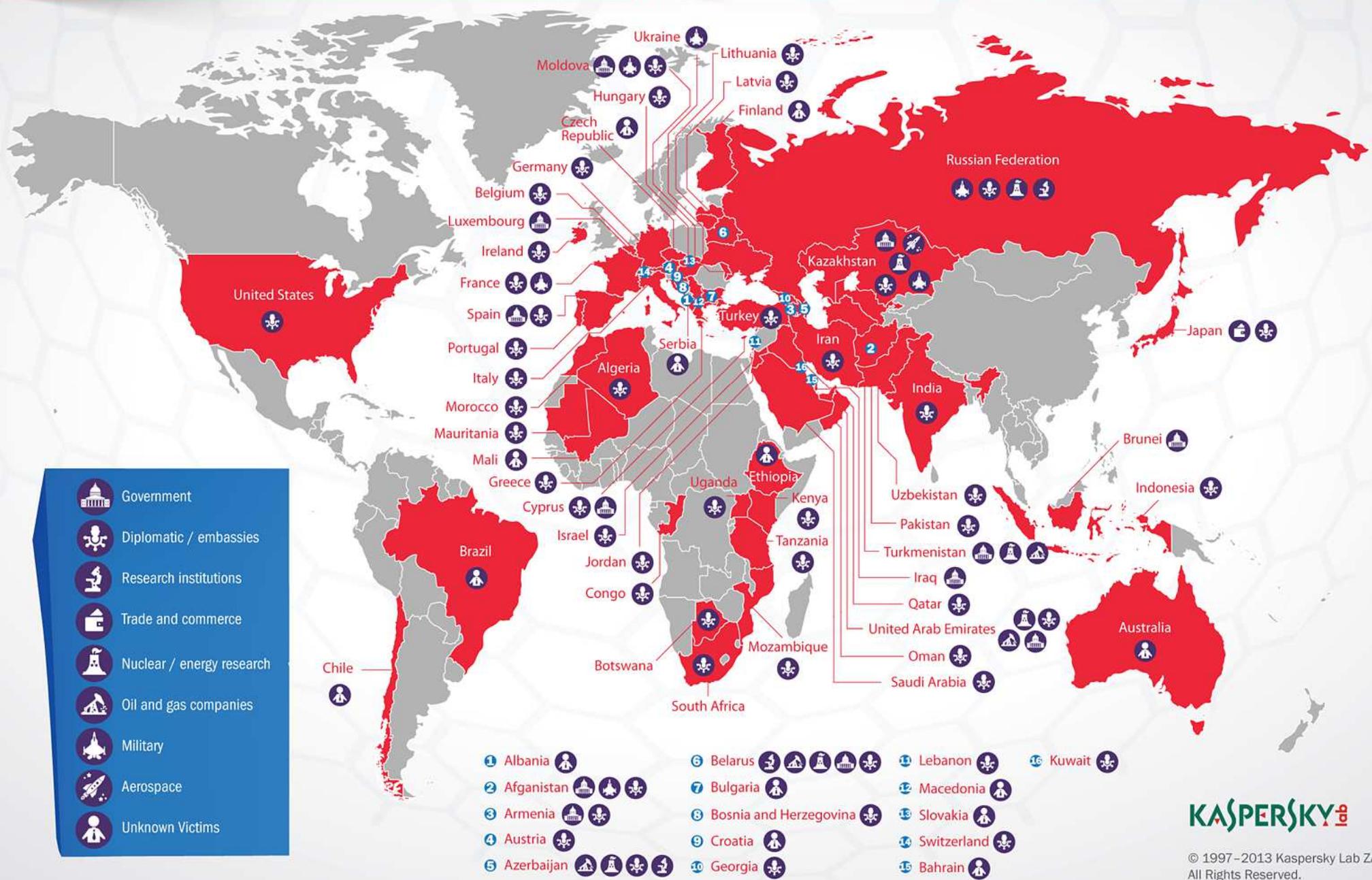
enforcement Skype, user content disclosure figures

Summary: Weeks after US privacy groups called on Microsoft to disclose law enforcement requests to Skype, amid controversy over China surveillance and snooping, the software giant did. While China appears low in the table, the devil is in the details.



Operation "Red October"

Victims of advanced cyber-espionage network



The story so far...

- Ransomware

I.P.A.
Międzynarodowego Stowarzyszenia Policji
UWAGA!
Ten komputer został zablokowany przez: system automatycznej kontroli informacyjnej Dlaczego?

Twój adres IP: [redacted]
Imię Host: [redacted]
Twoja lokalizacja jest ustalona

To mogło nastąpić wskutek jednej z następujących przyczyn:

1. Ten komputer był używany w celu odtwarzania zakazanych stron internetowych
2. Ten komputer był używany w celu odtwarzania stron internetowych, zawierających elementy pornografii dziecięcej
3. Ten komputer był używany w celu przekazania informacji zakazanej
4. Ten komputer był używany w celu przechowywania/odtwarzania treści nielegalnych

Możesz nabyć w jednym z PaysafeCard tys. PLN w Internecie, przez portfel, w kiosku dodatek bar

PaySafeCard można kupić w sklepach, które poniżej.

RELAY **inmedio Cafe**

Ransom Trojans spreading beyond Russian heartland
Security companies starting to see more infections
By John E Dunn | Techworld | Published: 19:20, 09 March 2012

Ransom malware has moved out of its traditional Russian market and is starting to become a measurable problem in countries such as the US and Germany, figures from Trend Micro have confirmed.

As reported by Trend's Smart Protection Network cloud, the US headed the list with just over 2,000 infections, ahead of Germany on 1,203, and Hungary on 561. Other countries reporting in the hundreds include France, Russia, Australia, Italy and Taiwan.

Wpisz kod 300 PLN PaysafeCard:

The story so far...

- WEBapp vulnerabilities

5,000+ sites hacked in 2 days by Indonesian Top Hacker Hmei7

Reported by Sabari Selvan on Wednesday, January 02, 2013 |



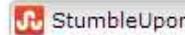
145



3



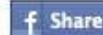
223



0



0



414



N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	iskorpibx	78015	392768	470783	267387	203396
2.	1923Turki	37353	169080	206433	78151	128282
3.	Hmei7	37204	91131	128335	63295	65040
4.	GHaST61	22411	265212	287623	168544	119079
5.	Fatal Error	21518	42603	64121	57820	6301
6.	kaMbiEz	14871	16435	31306	10010	21296
7.	SASD HaCk3D	13032	32342	45374	12985	32389
8.	ZoRRoKIN	11298	9679	20977	7860	13117
9.	misafir	10047	28823	38870	6689	32181
10.	Ashiyane Digital Security Team	9573	33591	43164	14783	28381

Indonesian Top Hacker named "Hmei7", known for Mass Defacements, has claimed to have defaced more than 5000 websites in two days (31 Dec 2012 and 1 Jan 2013).

So far, he hacked a lot of high profile websites including IBM, Microsoft, SIEMENS, AVG, Foxconn. He also defaced thousands of Government websites belonging to different countries.

Mirror saved on: 2013-02-12 02:55:40

Notified by: Hmei7

System: Win 2008

This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-02-12 02:55:40

Domain: <http://bienestar.unimaqdalena.edu.co/x.txt>

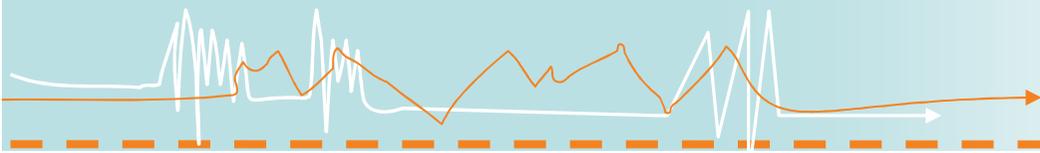
Web server: IIS/7.5

IP address: 190.254.21.212

[Notifier stats](#)

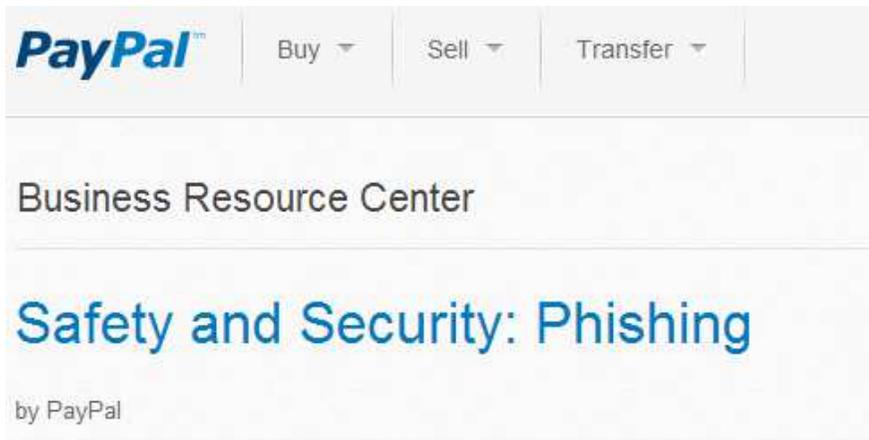
Just upload a file named "x.txt" or

hacked by Hmei7



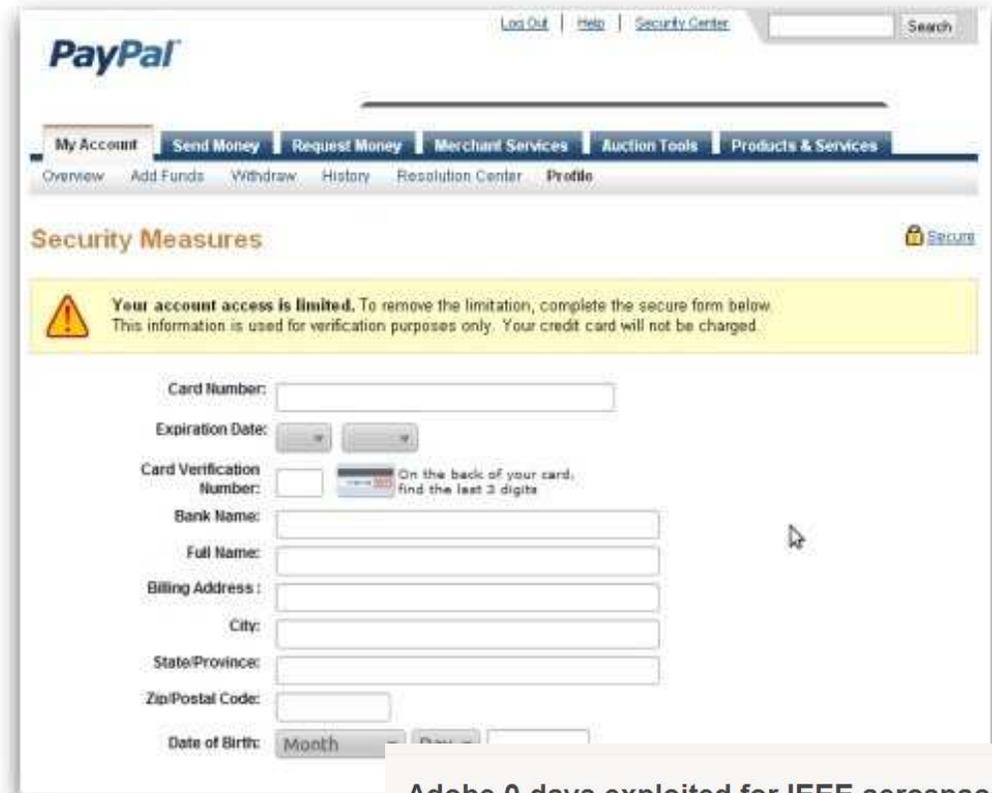
The story so far...

- Phishing



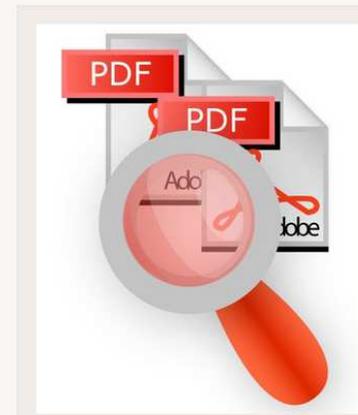
Beware fake emails: Phishing

Another way to help protect your identity, and your PayPal account, online is to be on the lookout for phishing emails. These emails are made to look like official communications from familiar companies. Fraudsters produce these emails and send them to millions of addresses in the hopes that someone will follow the links or call the phone number they've included and share sensitive information that the scammers can then exploit. Telltale signs of a phishing email include:



Adobe 0-days exploited for IEEE aerospace spearphishing attacks

by paganinip on February 12th, 2013



Last week **Adobe released a patch for Adobe Flash** that fixed a **zero day vulnerability**, CVE-2013-0633, that is being exploited using Microsoft Office files with embedded flash content delivered via email. The vulnerability is not isolated, it is circulating the news of a new one coded CVE-2013-0634 being exploited through web browsers such as Firefox and Safari on Mac OS X that has been identified by **FireEye** security firm.

Adobe credited the CERT of aerospace company Lockheed Martin for discovering that exploit,

The story so far...

- Application vulnerabilities



12 Fat Patch Tuesday

FEB 13

Adobe and Microsoft each have issued security updates to fix multiple critical vulnerabilities in their products. Adobe released updates for **Flash Player**, **AIR** and **Shockwave**; Microsoft pushed out a dozen patches addressing at least 57 security holes in **Windows**, **Office**, **Internet Explorer**, **Exchange** and **.NET Framework**.

Five of the **12 patches** Microsoft released today earned its most dire "critical" label, meaning these updates fix vulnerabilities that attackers or malware could exploit to seize complete control over a PC with no help from users.

Adobe to patch Reader zero-day this week with rush update

Hackers exploiting sandbox-bypass bug

Gregg Keizer (Computerworld (US)) | 17 February, 2013 22:59 | [Comments](#)



Examining How Facebook Got Hacked

Zero-Day Exploit Bypassed Java Protections to Install Malware

By Eric Chabrow, February 16, 2013. Follow Eric @GovInfoSecurity

Credit Eligible



Email



Like



Even the most savvy information technologists aren't immune from cyber-attacks. Just ask Facebook. The social-media titan was a victim to a sophisticated attack discovered by researchers. The exploit allowed malware to be installed on users' devices.

Exclusive: Apple, Macs hit by hackers who targeted Facebook

Recommend

3,009 people recommend this. Sign Up to see what your friends recommend.

Tweet 1,581

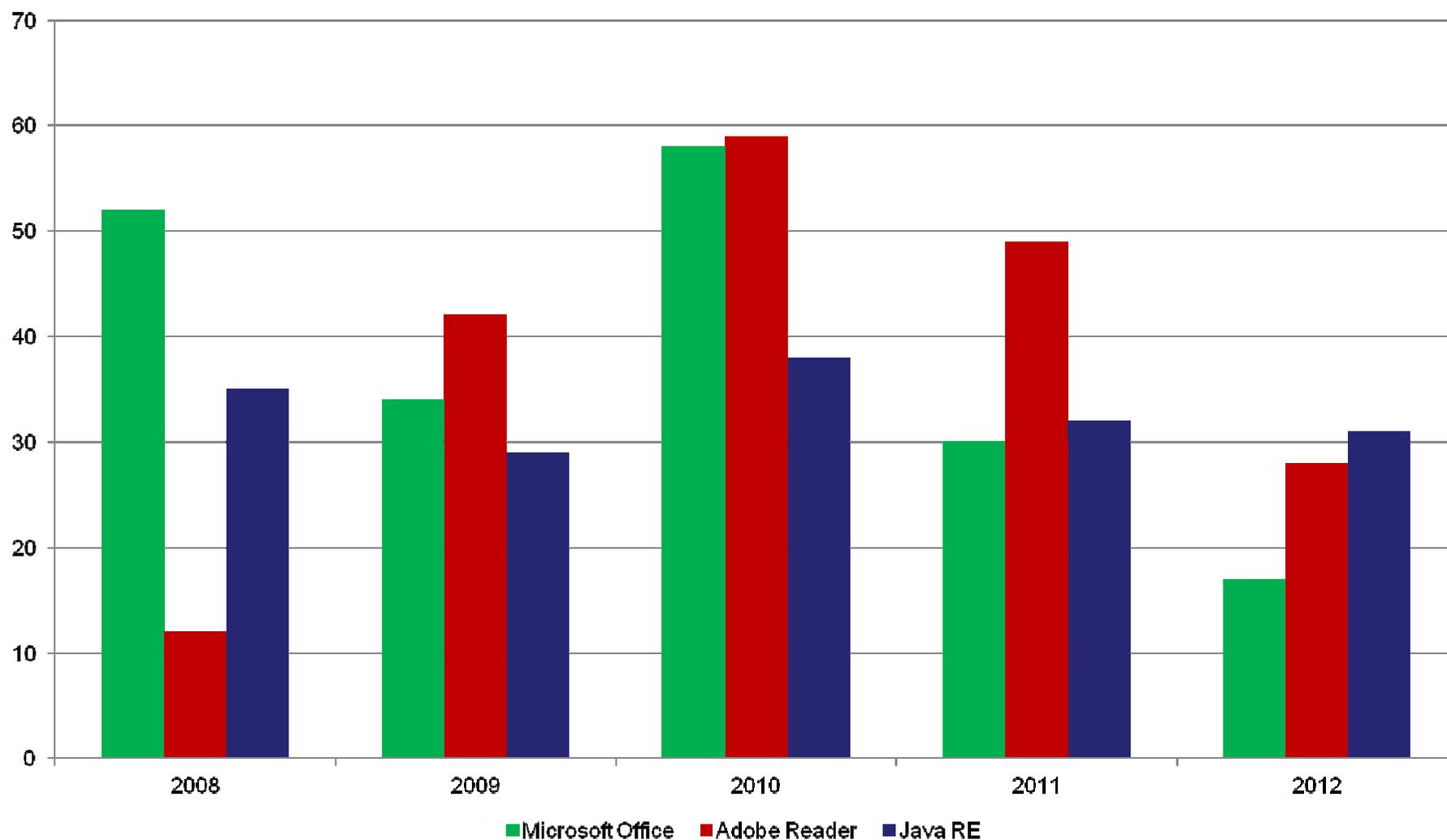
Share 165

Share this

+1 341

Email

Critical vulnerabilities



Source: NIST National Vulnerability Database

The story so far...

- Exploit kits and drive-by exploits



July 16, 2012, 9:54AM

Black Hole Exploit Kit Targeting Java CVE-2012-1723 Flaw

by Dennis Fisher

Follow @DennisF



Comment

Exploit Kits

A new fork of the [Black Hole exploit kit](#) is making quick work of a recently patched Java vulnerability and security researchers say that the attackers are registering new sites quickly to exploit users with vulnerable browsers.

13 November 2012

CVE-2012-4969 and the Unnamed Admin Panel

While [CVE-2012-4969](#) isn't new, we are still curious about the various ways this vulnerability can be exploited. Today we've stumbled upon a new instance of it. Let's have a look.

```
<html>
<body>
  <SCRIPT>
    var imgx = window.document.createElement("img");
    imgx.src = "a";
  </SCRIPT>
  <iframe src='ie.html' width='1' height='1'></iframe>
</body>
</html>
```

COMES WITH TRIPPLE SYSTEM

Operation systems statistics			Advanced browsers statistics		
OS	Visits Exploited	Percent	Browser	Visits Exploited	Percent
Windows Vista	6371 957	15.02%	MSIE v8.0	3717 437	11.76%
Windows XP	7135 807	11.31%	Firefox v3.5.9	2287 381	16.66%

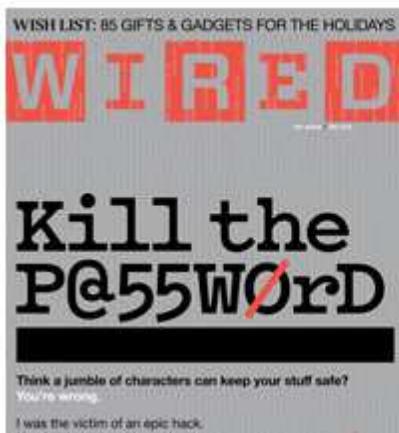
The story so far...

- Mobile devices and BYOD



The story so far...

- Targeted attacks



Your email. Your bank account. Your address and credit card number. Photos of your kids or, worse, of yourself, naked. The precise location where you're sitting right now as you read these words. Since the dawn of the information age, we've bought into the idea that a password, so long as it's elaborate enough, is an adequate means of protecting all this precious data. But in 2012 that's a fallacy, a fantasy, an outdated sales pitch. And anyone who still mouths it is a sucker—or someone who takes *you* for one.

No matter how complex, no matter how unique, your passwords can no longer protect you.



ar Phishing

Share

Spear Phishers lling to Steal Your Financial Info

Customers of a telecommunications firm received an e-mail recently explaining a problem with their latest order. They were asked to go to the company website, via a link in the e-mail, to provide personal information—like their birthdates and Social Security numbers. But both the e-mail and the website were bogus.

It's a real-life, classic case of "phishing"—a virtual trap set by cyber thieves that uses official-looking e-mails to lure you to fake websites and trick you into revealing your personal information.

It's also an example of an even more mischievous thing known as "spear phishing"—a rising cyber threat that you need to know about.



SECURITY ALERT Practical security advice

ANTIVIRUS SOFTWARE malware

Lockheed-Martin Attack Signals New Era of Cyber Espionage

By [Tony Bradley](#), PCWorld | May 28, 2011 9:40 PM

The network of defense contractor Lockheed-Martin was attacked using counterfeit electronic keys. Since the [RSA Security network was hacked](#) and the keys to its SecurID tokens were compromised a few months ago, the world has been waiting for the proverbial other shoe to drop. Well, it dropped.



The story continues...

- On light side you stay



IT security principles

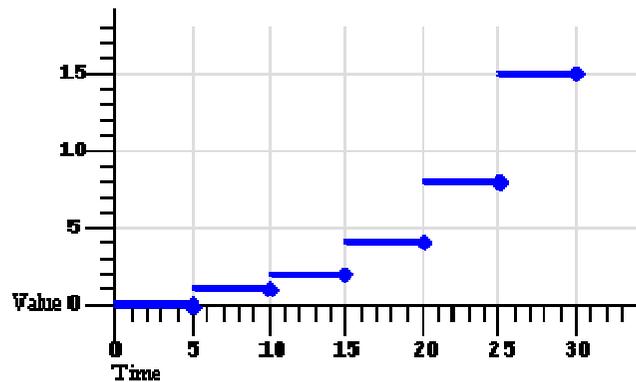
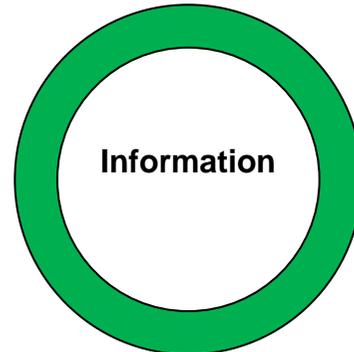
IT security principles

- What is security?

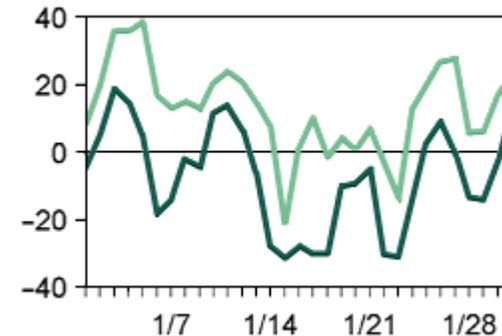


IT security principles

- What is Information Systems and Information Technology security?



Static / State



Dynamic / Process

IT security principles

- Security trade-off

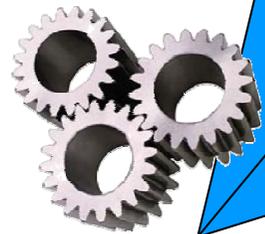


Expenses

Security



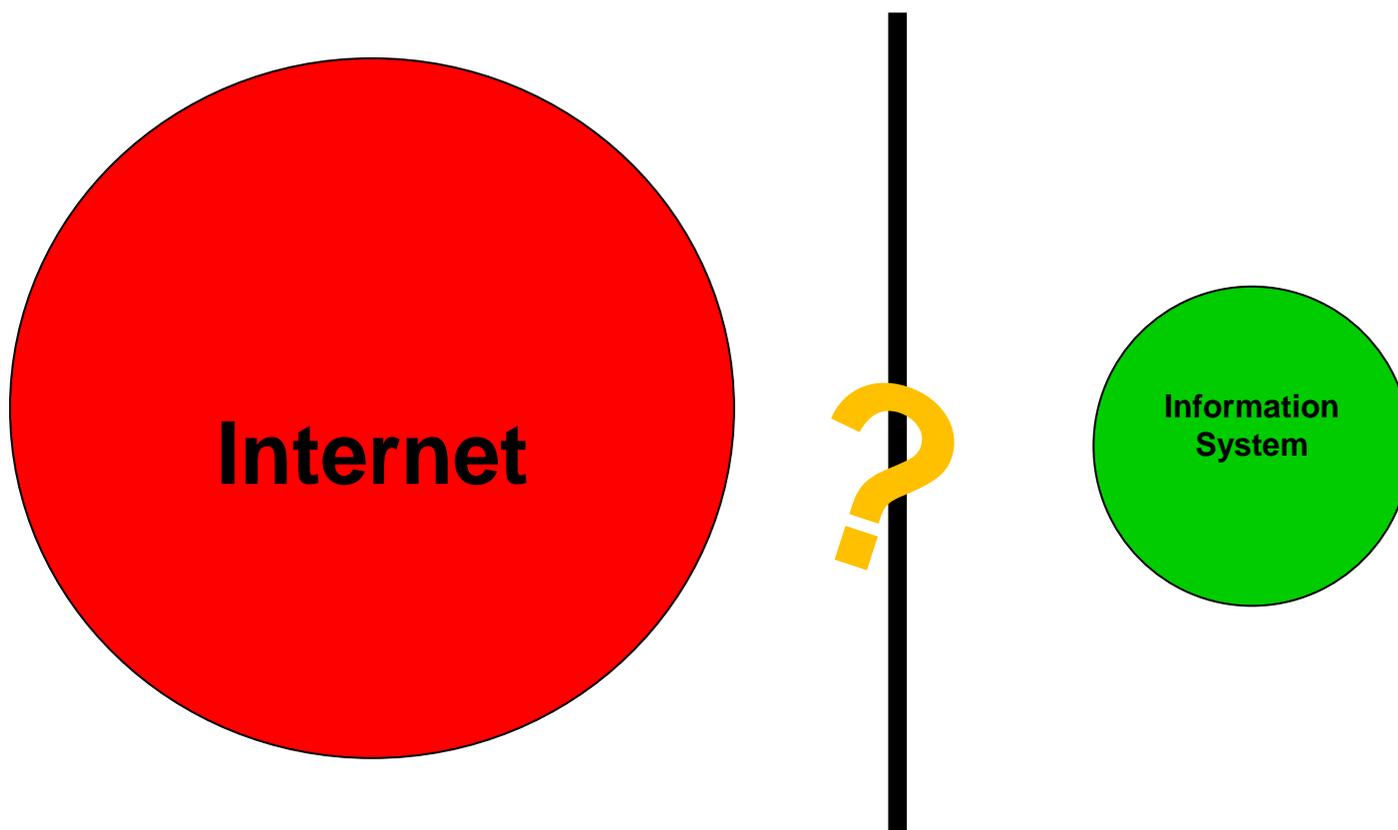
Usability



Functionality

IT security principles

- Information System perimeter

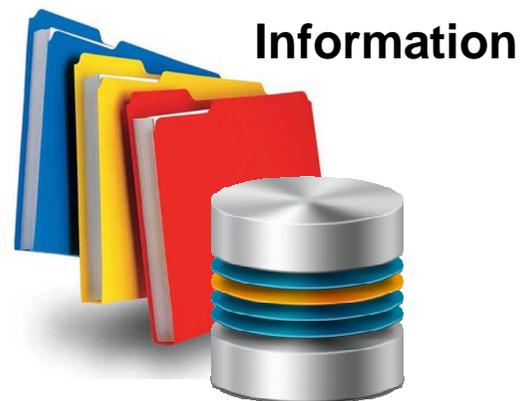


IT security principles

- Information System elements



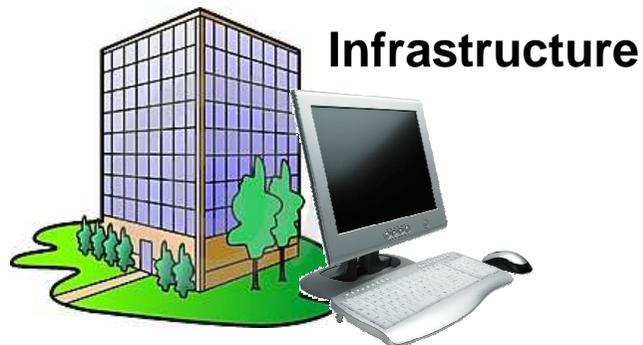
Users



Information



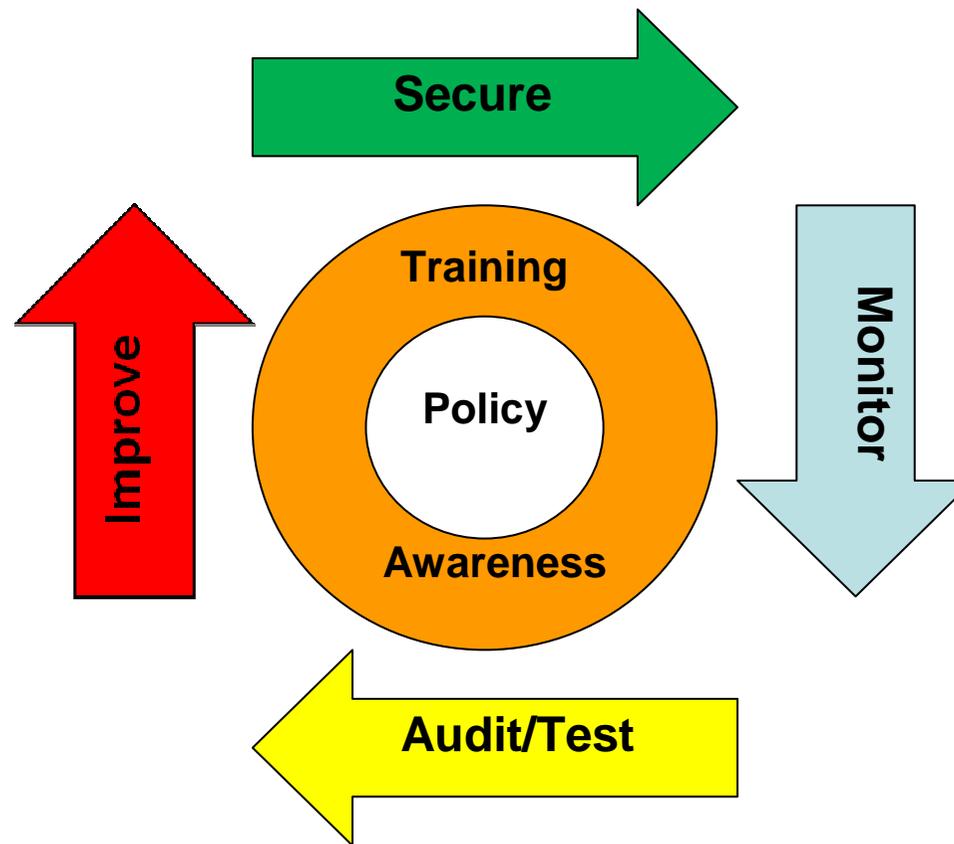
Applications

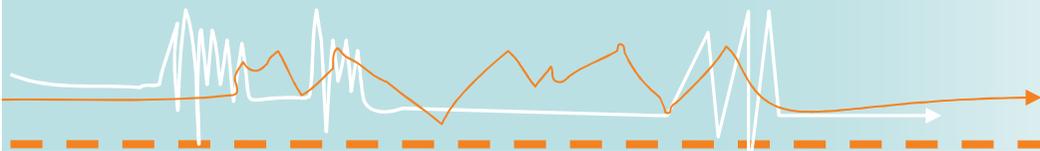


Infrastructure

IT security principles

- Security lifecycle



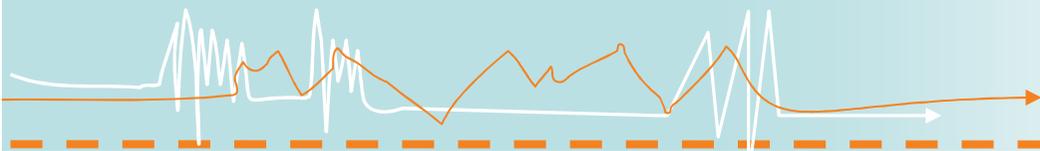


IT security principles

- The need for IT security testing

Video on «Cyber Security Evolved»

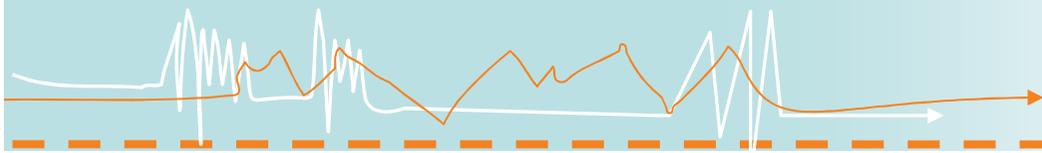




IT security principles

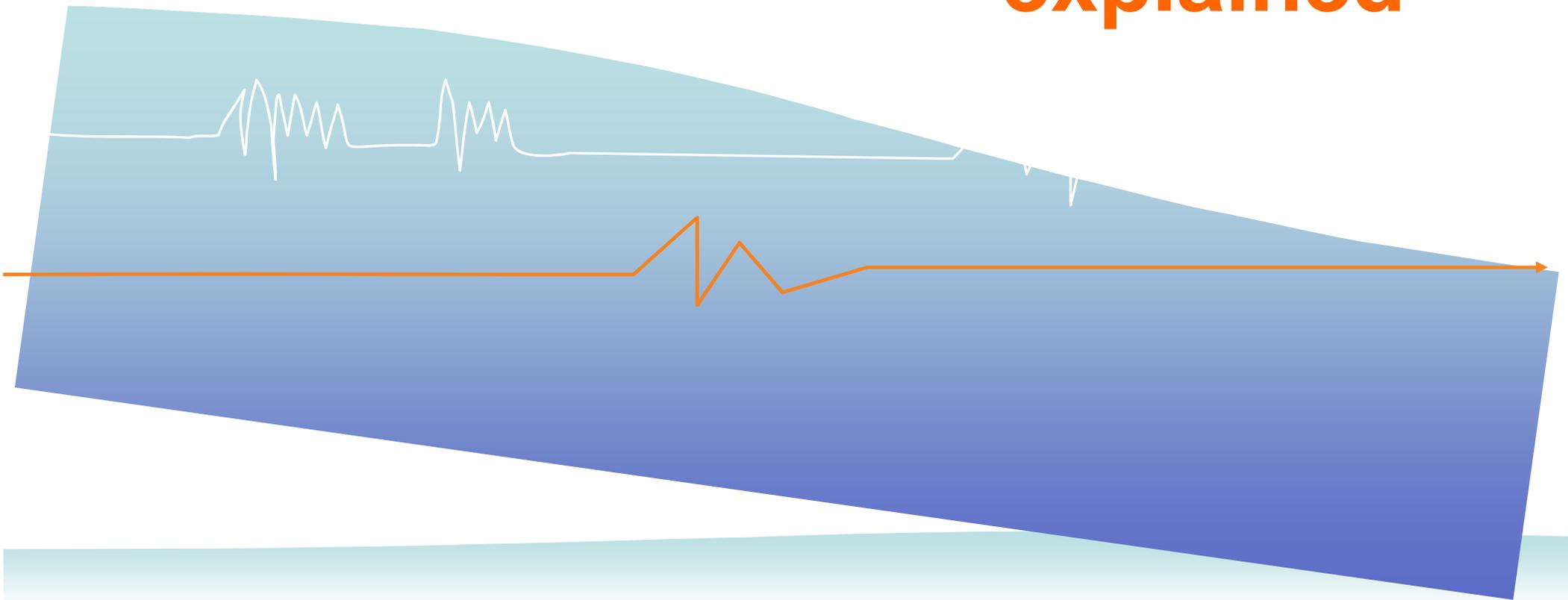
- So what is security?

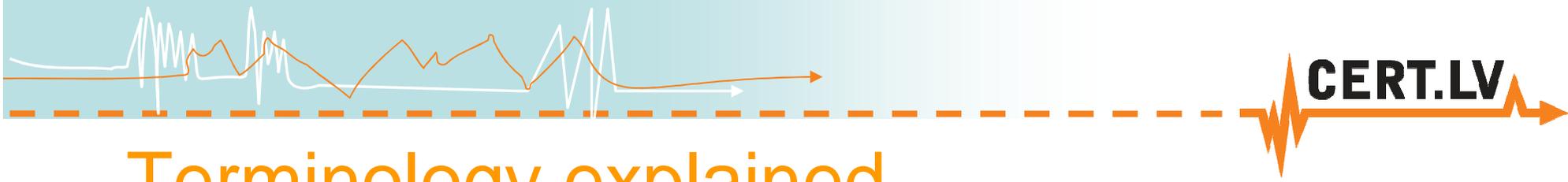




CERT.LV

Terminology explained





Terminology explained

w00t

1337

5(R1p7 |<1D|)13

H4XX0r

pwned!!!111

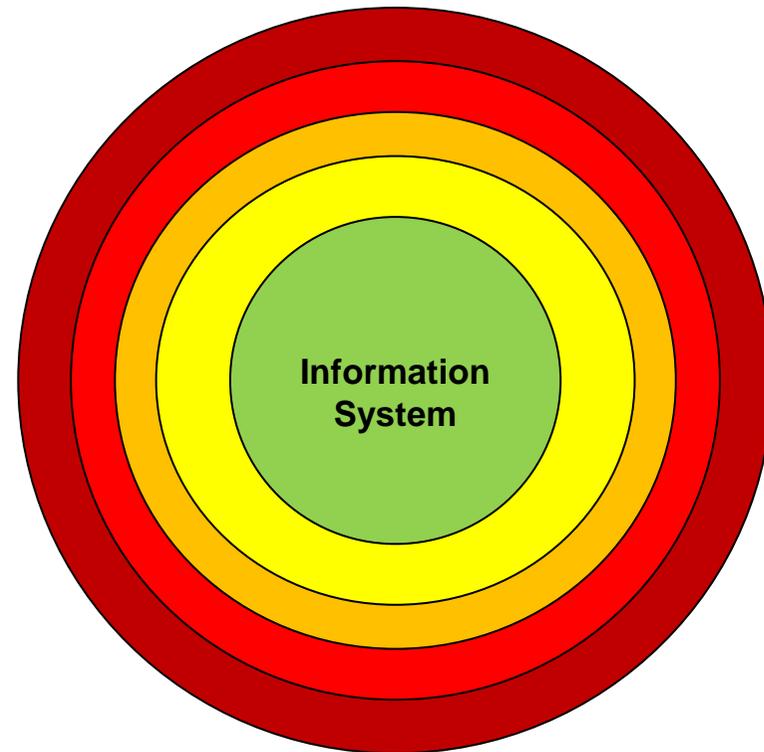
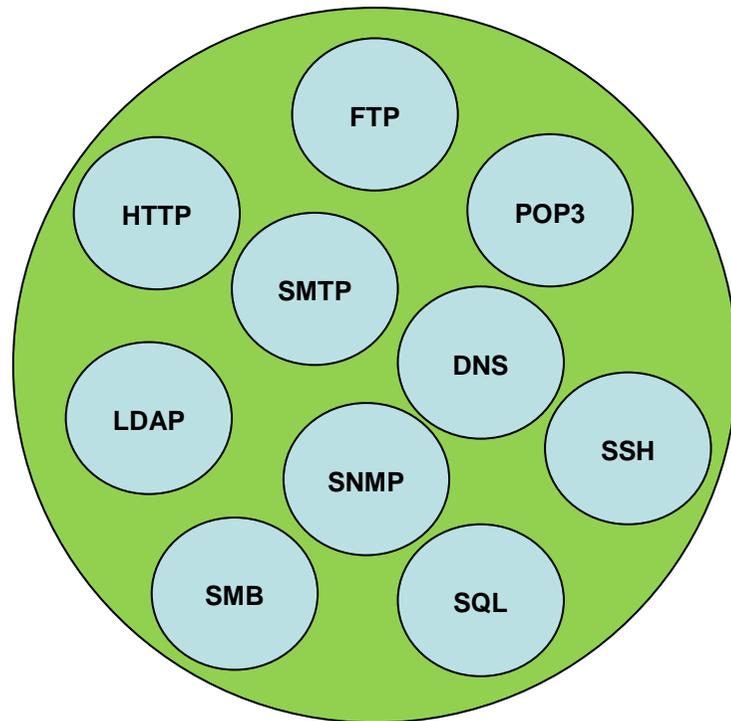
L@m3r

all your base are belong to us



Terminology explained

- Attack surface and defense-in-depth

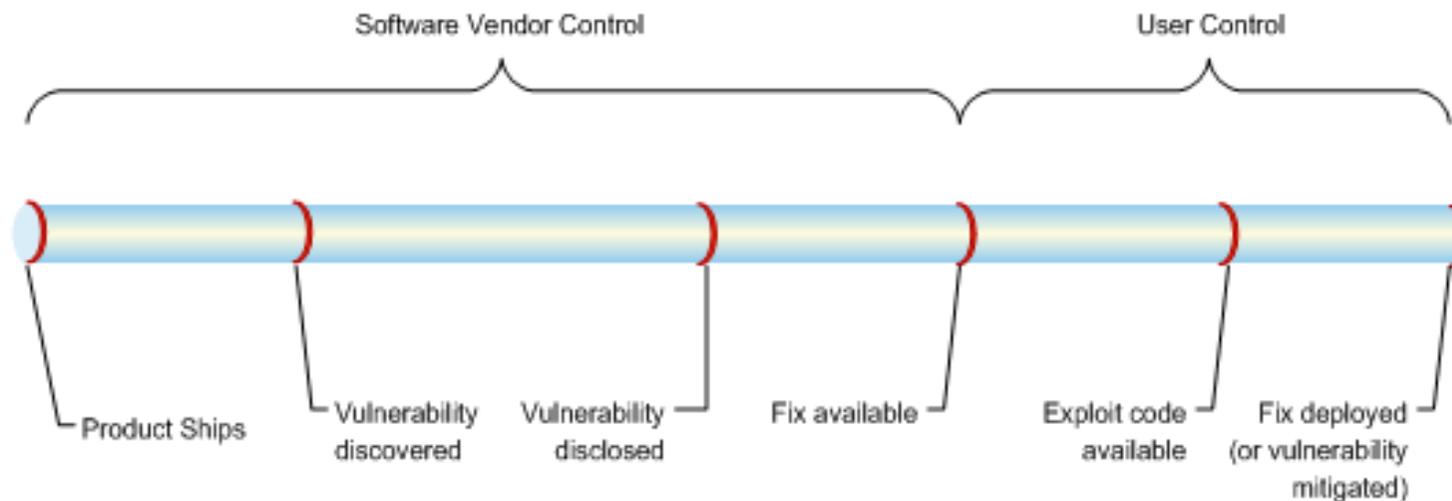


Terminology explained

- **Weakness**
 - A flaw, that leaves asset vulnerable to attack
 - **Exposure**
 - A point of access to the weakness
 - **Vulnerability**
 - An instance of the exposure of a weakness
 - **Exploit**
 - The act of taking advantage of a vulnerability
- 

Terminology explained

- Vulnerability lifecycle



- 0-Day

Terminology explained

- **Threat**
 - Potential event endangering a system
- **Risk**
 - A probability of threat becoming true
- **Risk management**
 - Process of risk assessment and analysis
 - Affect on Confidentiality, Integrity, Availability, Accounting
 - Accept, mitigate, eliminate, transfer

Terminology explained

- Types of hackers

- Hacktivists
- Black-hat hackers
- White-hat hackers
- Grey-hat hackers
- Suicide hackers



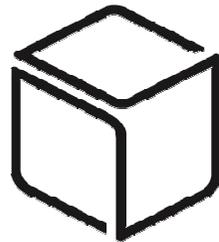
Terminology explained

- Types of system vulnerability tests

- Black-box



- White-box



- Grey-box



- Announced and unannounced

Network penetration testing models

Testing methodology

- Applicable standards
 - NIST 800-115
 - EC-Council, CE|H
 - PTES
 - Open Source Security Testing Methodology Manual (OSSTMM)
 - ISO/IEC 17799:2005 and 27000-series
 - Payment Card Industry Data Security Standard (PCI DSS)

Testing methodology

- Accepted penetration testing approach

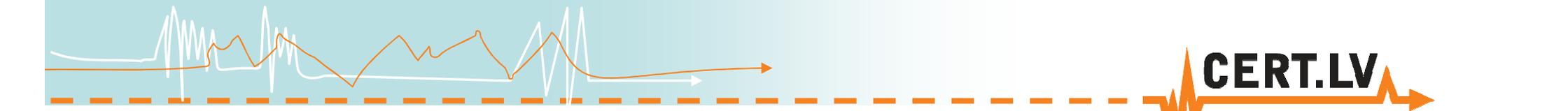
NIST	PTES	CEH
Planning	Pre-engagement Interactions	Reconnaissance
	Intelligence Gathering	
Discovery	Threat Modeling	
	Vulnerability Analysis	Scanning
Attack	Exploitation	Gaining access
	Post Exploitation	Maintaining access
		Clearing tracks
Reporting	Reporting	Reporting

Reporting results

- Outcome and reporting
 - Meets the predefined scope and goals
 - Answers to the stakeholder's questions or provides basis for decision making
 - Methodological, can be recreated or have proof-of-concept
 - Is well formed and understandable to the stakeholders

Reporting results

- Sample structure of a PT report:
 - Executive summary
 - Scope and objectives
 - Summary of findings and recommendations
 - Methodology used and test execution
 - Detailed findings
 - Appendixes: vulnerability reports, scan results and other technical data



CERT.LV

Thank you!

**<http://www.cert.lv/>
cert@cert.lv**

