I nuovi scenari del cybercrime: anche la PA e il sistema delle infrastrutture critiche sono a rischio

Emilio Montolivo
Elsag Datamat
Business Unit Cyber Security

Roma, 9, 11 e 12 maggio 2011

ELSAG DATAMAT
A Finmeccanica Company

Contenuti del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti

- Ma come è possibile? Vulnerabilità ... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Struttura del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità ... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Definizioni di cybersecurity

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet

  Fonte: TechTerms.com

- Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access

  Fonte: *Whatis?com* encyclopedia

- Cyber-security risks may include those that
  - damage stakeholder trust and confidence
  - affect customer retention and growth
  - violate customer and partner identity and privacy protections
  - adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.

  Fonte: DOD cyberspace glossary

Il crimine informatico negli ultimi 30 anni

ELSAG DATAMAT
A Finmeccanica Company

- 1980-2000: il fenomeno è prevalentemente paragonabile al vandalismo giovanile, l'hacker opera quasi sempre per "divertimento" e per dimostrare "quanto è bravo", perché si parli di lui, raramente lo fa per ottenere vantaggi economici
- 2000 -2005: si comincia a parlare di **criminale informatico professionista**, gli attacchi diventano più mirati e puntano ad ottenere vantaggi criminali, le tecniche diventano più complesse
  - Grande diffusione di Worm, BotNet e ad/spyware
  - **Primi segnali dell'esistenza di cyber criminali che vendono i loro servizi e "affittano" le loro BotNet anche per azioni di spionaggio**
- 2005 -2010: la tendenza emersa nel quinquennio precedente si rafforza. Si assiste ad attacchi eclatanti
  - Le tecniche di attacco non cambiano nella sostanza ma vengono usate in modo integrato e sempre più mirato
  - Si comincia a parlare di **Cybercrime, cyberespionage , cyberterrorism, cyberwar, Advanced Persistent Threat (APT)**
  - Si comincia a sospettare che alcuni attacchi provengano da enti governativi
  - I bersagli non sono più soltanto singoli individui, banche o gruppi industriali ma anche intere nazioni. La criminalità informatica può mettere a rischio la sicurezza nazionale

Struttura del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Cyber Attack contro il programma nucleare Iraniano

ELSAG DATAMAT
A Finmeccanica Company

lunedì 27 settembre 2010

Stuxnet, il worm all'assalto del nucleare iraniano

- Esperti di sicurezza presi in contropiede, altissimo livello di sofisticazione e un obiettivo apparentemente ben definito sono gli ingredienti dell'affaire Stuxnet, la nuova superstar del variopinto bestiario del malware
- Roma - Come già ampiamente previsto qualche mese fa, il worm Stuxnet si è trasformato nel nuovo "caso mediatico" capace di impensierire le società di sicurezza e sollevare polverone in seno alla stampa *mainstream*, generalmente poco accorta alla proliferazione di questo o quel pezzetto di codice malevolo. Ma Stuxnet fa molto, molto di più oltre a proliferare, e il malware ha tali e tante caratteristiche da far sorgere più di un dubbio sul fatto si tratti di un vero e proprio attacco organizzato contro il programma nucleare iraniano.
- Stuxnet è talmente complesso che security company ed esperti indipendenti sono sostanzialmente unanimi nell'assegnarne la paternità a uno stato organizzato dotato di fondi illimitati e forti motivazioni politico-militari

Fonte: www.punto-informatico.it

Stuxnet

ELSAG DATAMAT
A Finmeccanica Company

- Stuxnet prende di mira i programmi di monitoraggio e controllo industriale SCADA/WinCC e PCS 7.
- La diffusione iniziale avviene tramite penna USB infetta per poi contaminare gli altri PC collegati alla rete WinCC. Dopo aver raggiunto l'ingresso del sistema, Stuxnet utilizza parole d'ordine di default per ottenerne il controllo: per questo il produttore, Siemens, consiglia di modificare la parola d'ordine originale.
- La complessità di Stuxnet è insolita per un virus informatico in quanto l'attacco richiede la conoscenza dei processi industriali e mira all'attacco a infrastrutture industriali.
- Vista la complessità del virus, per la sua realizzazione si sarebbe dovuto impiegare un team di programmatori di diverse discipline e la verifica di sistemi reali per evitare di bloccare il funzionamento del PLC. Secondo tecnici Siemens la creazione di questo malware avrebbe richiesto mesi se non anni di lavoro se eseguita da una sola persona.

Cyber attack ad un generatore elettrico

ELSAG DATAMAT
A Finmeccanica Company

Staged cyber attack reveals vulnerability in power grid

- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned. Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power. Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.
- CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab In a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

Fonte: CNN, 26 settembre 2007

Video dell’esperimento

http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US

Cyberspace declared the 5th domain

ELSAG DATAMAT
A Finmeccanica Company

- In May 2010, the final disappearance of the line between physical and virtual security became official when Defense Secretary Robert Gates announced the activation of the U.S. Cyber Command, or CYBERCOM.

  Cyberspace, Gates declared, was the fifth domain of security, alongside land, sea, air and space. When it comes to the transformation of military culture that CYBERCOM represents, it's hard to overemphasize the importance of the Secretary's summation. Only a year before CYBERCOM came into being, two leading Army officers, Lt. Col. Gregory Conti and Col. John Surdu, had shown their dissatisfaction with the lack of recognition given to technical expertise in the U.S. military, despite the growing threat from cyberspace.

Gen. Keith Alexander (far right), first U.S. cyber-commander

Fonte: http://www.govtech.com/security/Defense-Secretary-Robert-Gates-Announces-Nations.html

25 maggio 2010

Struttura del master

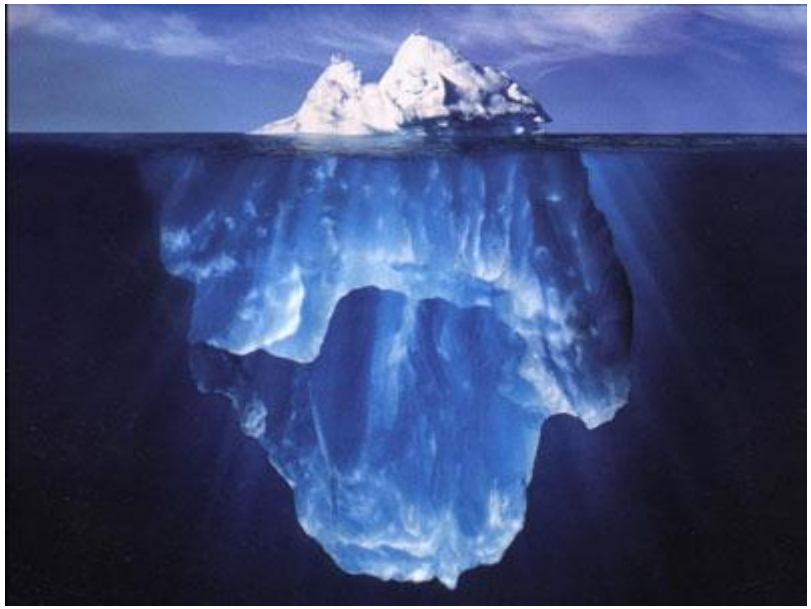
ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Le dimensioni del fenomeno

ELSAG DATAMAT
A Finmeccanica Company

- Non è facile reperire statistiche sul numero e sulle tipologie di attacchi informatici che si verificano nel mondo
  - Le vittime spesso non denunciano gli incidenti per motivi di immagine
  - E' assai probabile che nella maggior parte dei casi la vittima non sappia di nemmeno essere sotto attacco
    - nel caso del *cyberespionage*, l'attaccante cerca in ogni modo di passare inosservato
    - Il *malware* che trasforma un PC in un *robot* di una BotNet è spesso dotato di *rootkit* che modificano il sistema operativo ospite per nascondere la propria presenza e rendere impossibile la propria disinstallazione senza re-installare il sistema operativo stesso
- Solo i casi più eclatanti diventano di pubblico dominio



Un fenomeno in crescita

ELSAG DATAMAT
A Finmeccanica Company

- Secondo fonti governative USA, i sistemi informatici delle varie agenzie subiscono in media 1,8 miliardi di tentativi di attacco al mese, gli attacchi conclamati sono passati dai 30.000 del 2009 ai circa 42.000 del 2010
- Il Segretario per gli affari esteri UK (William Hague) ha ammesso che i sistemi informatici governativi inglesi hanno subito nel 2010 infezioni da malware riconducibili ad azioni mirate di gruppi ostili.
- Una ricerca condotta nel 2010 da ArcSight ha stimato in 3.5M$ il danno medio annuo subito a causa di atti di cybercrime dalle grandi aziende in USA
- Una ricerca condotta dai Kaspersky Lab. Ha stimato in circa 500$ annui la perdita media subita da ciascun utente della rete Internet a causa di truffe attuate tramite mail scamming e azioni di phishing
- Secondo un rapporto congiunto governo/industria la perdita annua in UK imputabile al cyber crime è di circa 27 miliardi di Sterline dei quali 21 riguardano il settore commerciale

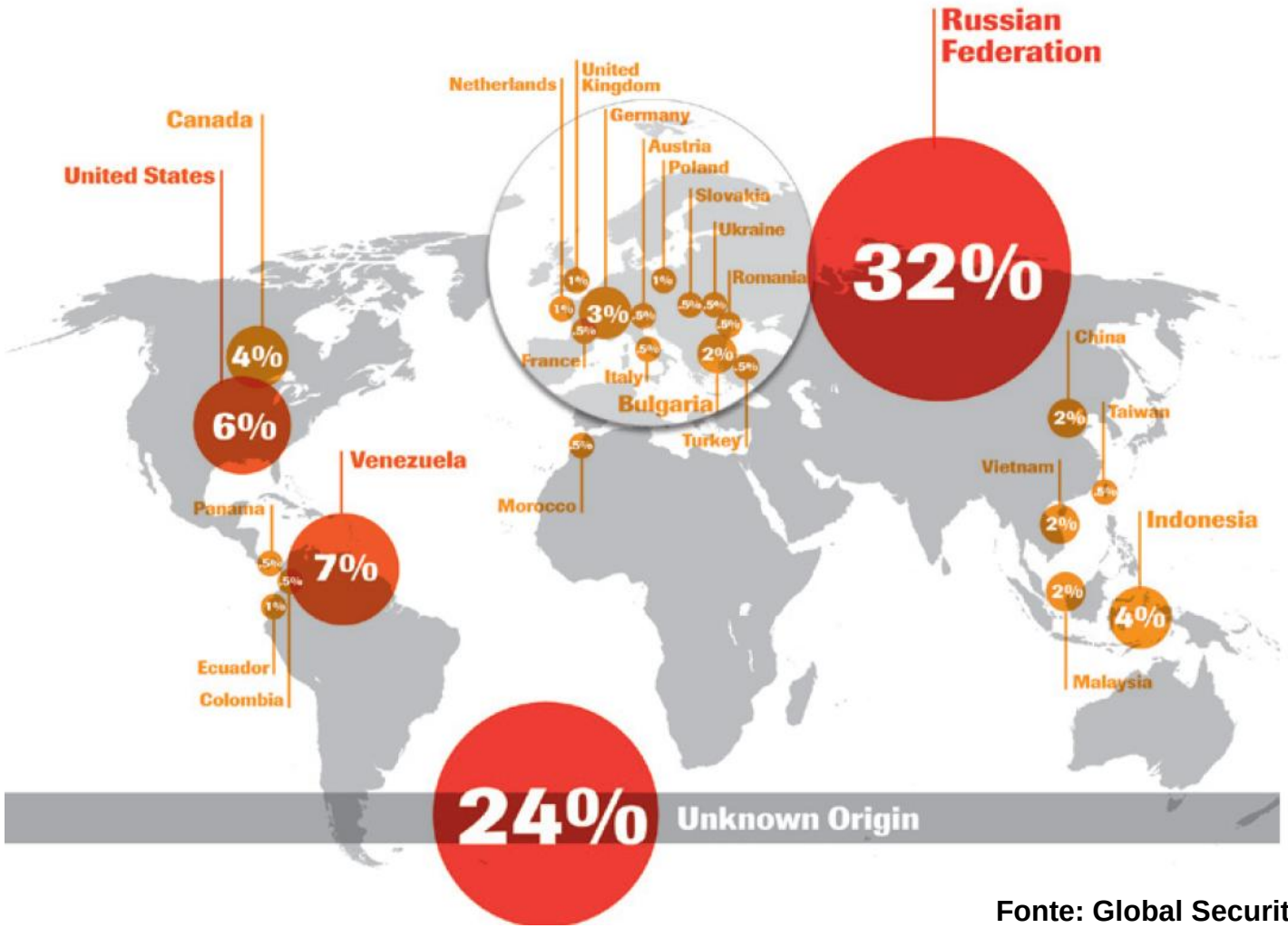
Alcuni attacchi famosi

ELSAG DATAMAT
A Finmeccanica Company

- Nel mondo
  - Estonia (aprile 2007) - DDoS (Distributed Denial of service)
  - Georgia (agosto 2008) - DDoS, alcuni siti istituzionali hanno subito il anche defacement
  - Siti istituzionali e commerciali in USA (luglio 2009) - DDoS
  - Amazon, MasterCard, Visa, Paypal (dicembre 2010) DDoS
  - Commissione Europea (marzo 2011) – DoS di servizio e-mail e siti istituzionali
  - Sony (aprile 2011) - intrusione con furto di dati personali
- In Italia
  - Poste Italiane (ottobre 2009) – defacement del sito
  - Finmeccanica, ENI, Unicredit (marzo 2011) – DDoS

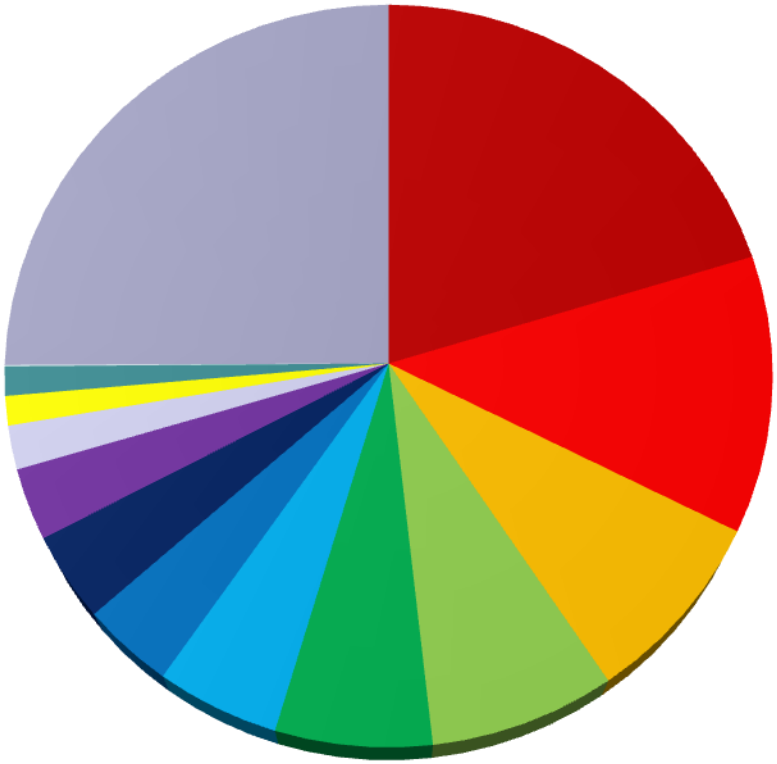
Origine degli attacchi su scala globale (dati riferiti al 2010)

ELSAG DATAMAT
A Finmeccanica Company



Fonte: Global Security Report 2011
TrustWave Cyberlabs

Organizzazioni più frequentemente attaccate



Fonte: The Web Hacking Incident Database 2010
Semiannual Report
January to June 2010
TrustWave Spiderlabs

Il caso Estonia

ELSAG DATAMAT
A Finmeccanica Company

- Il 27 aprile del 2007 è iniziato un violento attacco informatico all'Estonia. **Le caratteristiche e la durata dell'attacco hanno fatto parlare di un atto di cyberwar**
- L'attacco si è protratto per tre settimane ed ha interessato l'intera nazione.
- Gli effetti dell'attacco sono stati drammatici ed hanno bloccato ogni attività economica in quanto l'Estonia è uno dei paesi mondiali più dipendente da Internet
  - La maggior parte dei servizi governativi sono offerti via rete
  - I pagamenti elettronici via Internet hanno sostituito quasi completamente quelli in moneta nella maggior parte degli esercizi commerciali
- **La maggior parte degli attacchi è stata di tipo Denial of Service distribuito (DDoS).** Le tecniche usate sono andate dal semplice Ping Flood attuato da singoli individui fino all'impiego di BotNet, probabilmente prese in affitto da organizzazioni criminali che le usano per la distribuzione di spam e-mail. **Alcuni siti governativi hanno subito anche azioni di defacement**. Inoltre, sembra che alcuni sistemi IT definiti mission-critical, come quelli di alcune centrali telefoniche, siano stati oggetto di attacco.
- Gli attacchi sono stati messi in relazione con un incidente politico tra Estonia e Russia. In realtà il coinvolgimento della Russia come nazione non è mai stato provato

Il caso Georgia

ELSAG DATAMAT
A Finmeccanica Company

- Nell'agosto del 2008, la Georgia, poco prima e durante il conflitto armato con la Russia, ha subito un attacco informatico di ampie proporzioni
- **La maggior parte degli attacchi è stata di tipo DDoS.** Inoltre, **alcuni siti web istituzionali hanno subito azioni di defacement** (il sito del Presidente della Repubblica, il sito della Banca Nazionale e il sito del Ministero degli Affari Esteri). Le modalità di attacco sono state simili a quelle dell'attacco in Estonia
- Gli attacchi hanno colpito siti governativi, istituti finanziari, siti di organi di informazione
- Come nel caso dell'Estonia, non è stato possibile identificare gli autori dell'attacco

Gli attacchi del 4 luglio 2009

ELSAG DATAMAT
A Finmeccanica Company

- Dal 4 al 9 luglio del 2009 alcuni siti web finanziari, informativi e governativi in USA e nella Corea del Sud sono stati oggetto di varie ondate di **attacchi di tipo Distributed Denial of Service (DDoS)**
- Gli attacchi hanno interessato, tra gli altri, il sito web della Casa Bianca e del Pentangono, il sito web del Ministero della Difesa Sud Coreano e il sito web dell'Agenzia di Inteligence Sud Coreana
- **L'attacco è avvenuto attraverso l'attivazione di una BotNet** che si ritiene fosse costituita da almeno 20.000 computer
- La maggior parte dei computer della BotNet erano situati in Corea del sud
- I responsabili degli attacchi non sono mai stati individuati

Alcuni casi cyber-espionage divenuti di pubblico dominio

ELSAG DATAMAT
A Finmeccanica Company

- December 3, 2007 THE TIMES THE SUNDAY TIMES
  - Secrets of Shell and Rolls-Royce come under attack from China's spies

- January 14, 2010 The Washington Post
  - Google China cyberattack part of vast espionage campaign, experts say
  - At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail accounts of Chinese human rights advocates in the United States, Europe and China, threatened to shutter its operations in the country as a result.

Il DDOS italiano (4 marzo 2011)

ELSAG DATAMAT
A Finmeccanica Company

Anonymous, i giorni del DDoS italiano

- Un'aggressiva ondata di cyberattacchi ha investito numerosi spazi online. Il più violento ha messo KO la piattaforma di blogging WordPress. Gli Anonymous avrebbero poi colpito i siti di Finmeccanica ed ENI. Il movente sarebbe politico

- Ad agire sarebbe stato un gruppo di circa un centinaio di persone coordinatisi via IRC e armati del cosiddetto Low Orbit Ion Cannon (LOIC).

Fonte: Punto Informatico

Attacco del 24/3/2011 alla Commissione europea

ELSAG DATAMAT
A Finmeccanica Company

- La Commissione Europea sotto il fuoco dei pirati informatici. I servizi di posta elettronica e diverse pagine del sito internet della Commissione sono rimasti bloccati a causa di un cyber-attacco la cui origine non è stata individuata. Direttamente colpiti anche i servizi della rappresentante della politica estera europea Catherine Ashton.
- L'episodio è arrivato alla vigilia del vertice nel quale oggi verranno affrontati dossier cruciali come la nuova governance economica europea, le misure di verifica per le centrali nucleari europee all'indomani della crisi giapponese e la guerra in Libia.

Fonte: it.euronewe.net, 24/3/2011

Attacco alla SONY (aprile 2011)

- **Colpo grosso alla Sony. La società ammette: a rischio i dati di 77 milioni di utenti PlayStation**
- *I servizi PlayStation Network e Qriocity sono stati disattivati una settimana fa, in seguito a un massiccio attacco hacker: una 'ritorsione' provocata, si ritiene, dalla decisione di Sony di citare in giudizio il noto hacker George Hotz.*
- Tra il 17 e il 19 di aprile, in seguito a intrusioni illegali e non autorizzate nel sistema **PlayStation Network**, un hacker è riuscito a trafugare le informazioni personali - nome, indirizzo (città, stato/provincia, codice postale), nazione, indirizzo email, data di nascita, password, login e online ID di PSN/portatile - di circa 77 milioni di utenti della console PlayStation della **Sony**.

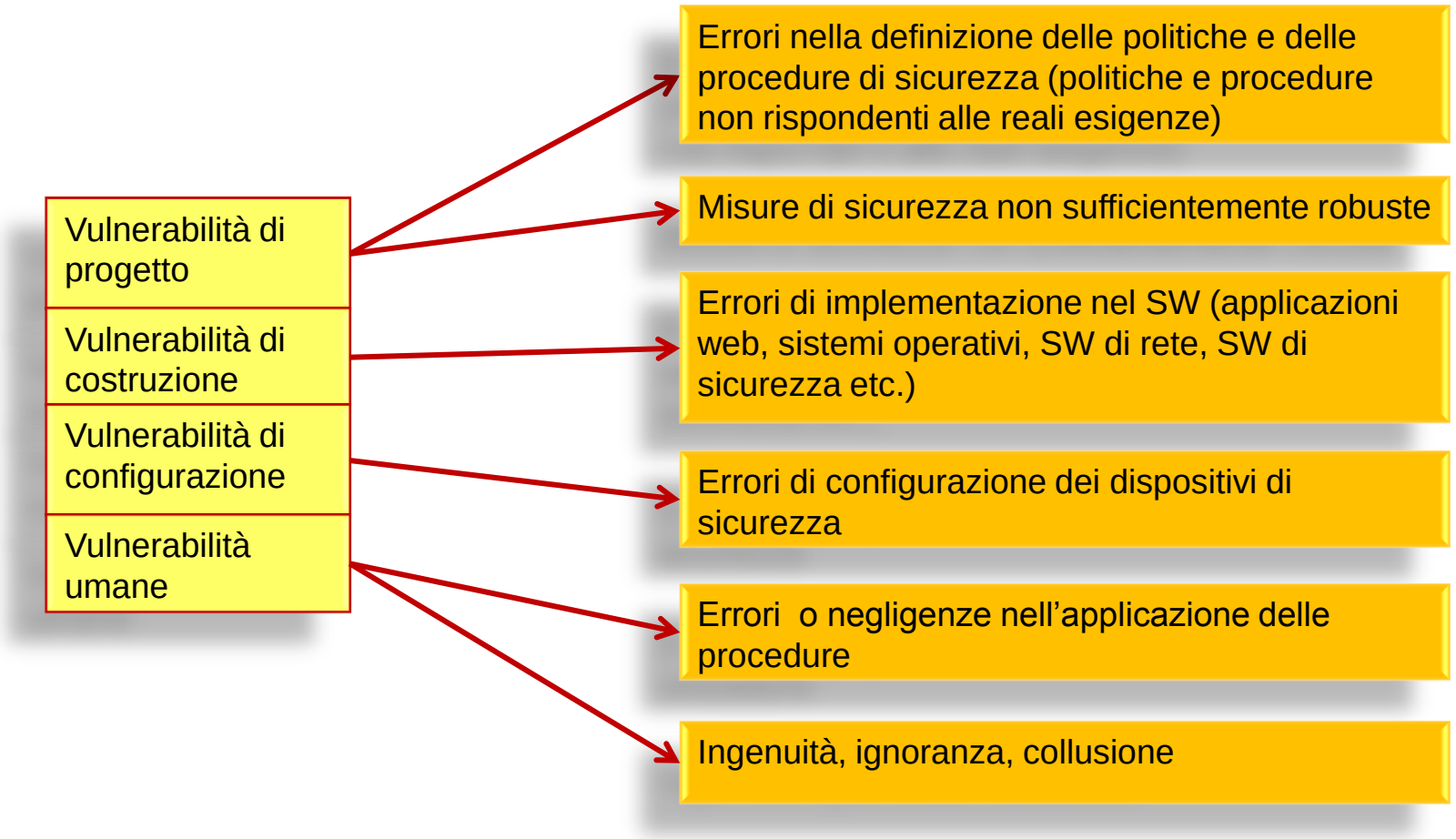
Fonte: Key4biz.it®

Struttura del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Perché i sistemi sono vulnerabili?



Perché è così difficile eliminare le vulnerabilità?

ELSAG DATAMAT
A Finmeccanica Company

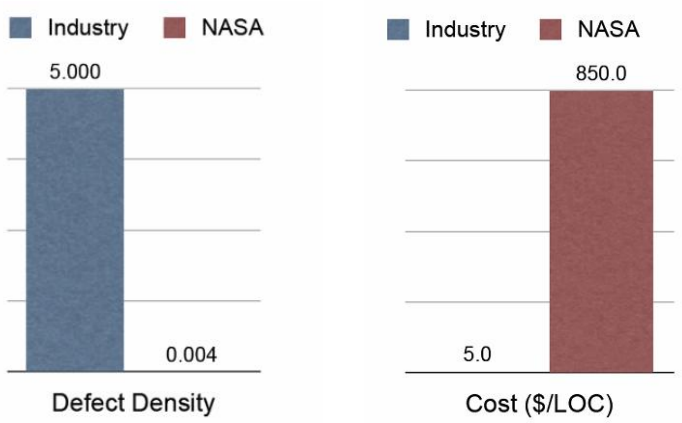
- Top reasons why computer systems are so vulnerable (Eugene Spafford, a professor and executive director at the Purdue University Center for Education and Research in Information Assurance and Security - The Wharton School, University of Pennsylvania)
  - Corporations and individuals have placed too much faith in the marketplace to develop defenses and forces to develop solutions. The strategy, has failed largely because ***there is no liability for poor quality, and there is no penalty of consequence for continuing to sell faulty products***.
  - Technology departments are under pressure **to maintain legacy systems and compatibility even when they know they have components that have security issues**. To maintain those legacy systems, computer managers have to buy add-on security products to patch holes, entering the never-ending penetrate-and-patchcycle.
  - **Little effort is made to consider security and robustness as central design criteria**, leading to implementation of software and hardware developed by vendors that have not been completely vetted. Companies are under the misguided assumption that add-on security will address any problems.
  - A misperception that security involves a fixed set of problems that can be "solved." The reality is that systems continue to change and face adversaries that attack in novel ways to test evolving systems. ***Computers and networks are designed to provide speed and power at the lowest cost rather than implementing known, basic security principles.***
  - **Law enforcement does not have the resources necessary to conduct forensic computing investigations.**
  - There is no political awareness to secure international cooperation to investigate and pursue cyber criminals operating outside national borders (USA point of view – see Budapest Convention on Cybercrime). As a result, **there is no effective deterrent to computer crime**.
  - Over-classification and **restrictions on data and incidents make it difficult to gain an accurate view of the scope or nature of some problems**. That also means that some research efforts might be inherently naive in focus because the researchers do not understand the true level of sophistication of their adversaries.
  - **There exists a critical misconception that the primary goal of intruders is to steal information or crash our systems. In reality, many adversaries seek to alter critical applications or data so that systems do not appear to be corrupted but fail at critical times — or worse, operate against our interests.**
  - We have **too few people in government, industry and the general public who understand what good security is** and this has a negative impact on the way computing is taught, designed, marketed and operated.

Fonte: Cyber attacks: what can be done to stem the tide of defense technology theft (March 2009)
http://executiveeducation.wharton.upenn.edu/wharton-aerospace-defense-report/upload/Cyber-Attacks.pdf

Errori nel SW e vulnerabilità

- Difetti nel SW, non soltanto in quello che svolge funzioni di sicurezza, possono tradursi in vulnerabilità sfruttabili da un hacker
  - La densità stimata degli errori nel SW commerciale è di circa 5 bugs/KLOC. Il costo medio di sviluppo è di $5./LOC
  - Il SW sviluppato per la NASA ha una densità di errori stimata in 0.004 bugs/KLOC* ed un costo di sviluppo di $850/LOC

*KLOC=1000 Lines of Codes



Costo del SW rispetto alla densità di errori

Fonte: http://agileindia.org/agilecoimbatore07/ (2009)

I top 25 errori di programmazione

ELSAG DATAMAT
A Finmeccanica Company

- **Category 1: Insecure Interaction Between Components**
  - **Improper input validation**
  - Improper encoding or escaping of output
  - ***Failure to preserve SQL query structure (aka "SQL injection")***
  - ***Failure to preserve Web page structure (aka "cross-site scripting")***
  - Failure to preserve operating system command structure (aka "OS command injection")
  - Cleartext transmission of sensitive information
  - Cross-site request forgery (CSRF)
  - Race condition
  - **Error message information leak**
- **Category 2: Risky Resource Management**
  - ***Failure to constrain operations within the bounds of a memory buffer***
  - External control of critical state data
  - External control of file name or path
  - Untrusted search path
  - **Failure to control generation of code (aka "code injection")**
  - Download of code without integrity check
  - Improper resource shutdown or release
  - Improper initialization
  - **Incorrect calculation**
- **Category 3: Porous Defenses**
  - **Improper access control (authorization)**
  - **Use of a broken or risky cryptographic algorithm**
  - **Hard-coded password**
  - Insecure permission assignment for critical resource
  - Use of insufficiently random values
  - Execution with unnecessary privileges
  - **Client-side enforcement of server-side security**

Fonte: SANS institute, 2010

Il database delle CVE (Common Vulnerability and Exposure)

ELSAG DATAMAT
A Finmeccanica Company

- Il MITRE, un istituto no-profit in USA, mantiene dal 1999 un database delle vulnerabilità via via scoperte nei principali sistemi operativi, DBMS, SW applicativi, etc., che hanno rilevanza ai fini della sicurezza
- **Ad oggi (maggio 2011) il database contiene circa 46.000 vulnerabilità**, per ciascuna delle quali vengono fornite indicazioni dettagliate circa i rischi connessi e la disponibilità di patch e/o work-around rilasciati dagli sviluppatori

Un esempio di vulnerabilità presente nel DB del MITRE

ELSAG DATAMAT
A Finmeccanica Company

Vulnerability Summary for CVE-2010-3791

Original release date: 11/16/2010

Last revised: 12/11/2010

Source: US-CERT/NIST

Overview

Buffer overflow in QuickTime in Apple Mac OS X 10.6.x before 10.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted MPEG movie file.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) (legend)

Impact Subscore: 6.4

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

Access Complexity: Medium

Authentication: Not required to exploit

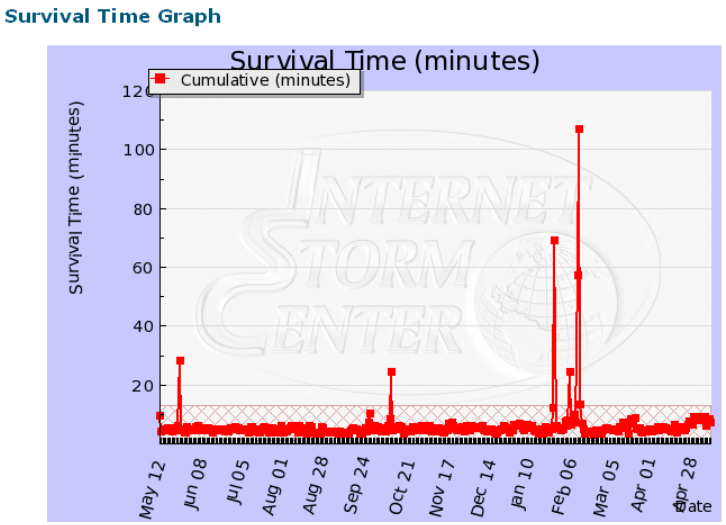
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

Tempo medio di sopravvivenza di un PC connesso ad Internet privo di patch

ELSAG DATAMAT
A Finmeccanica Company

- Il PC viene collegato alla rete dopo aver installato su di esso il sistema operativo ed altro SW così come viene distribuito dai fornitori al momento dell'esperimento (quindi privo delle patch rese disponibili dopo il rilascio della versione di SW utilizzata)
- Il tempo di sopravvivenza è calcolato sulla base dell'intervallo di tempo medio tra due "probe" rilevati dal PC direttamente collegato ad Internet. Se si assume che questi "probe" siano originati da worm che tentano di propagarsi sfruttando una vulnerabilità nota del sistema, in assenza di patch tutti i "probe" avrebbero successo.
- Il tempo medio di sopravvivenza negli ultimi 12 mesi è risultato di pochi minuti
- La situazione non è cambiata significativamente negli ultimi 10 anni



maggio 2010 – maggio 2011

Fonte: http://isc.sans.edu/survivaltime.html (SANS Institute - Internet storm Center)

Le vulnerabilità più sfruttate

ELSAG DATAMAT
A Finmeccanica Company

- La maggior parte degli attacchi che sfruttano vulnerabilità del SW di sistema o applicativo fanno uso di varie forme di buffer overflow
  - Secondo un report del SANS Insititute, nel periodo marzo-settembre 2009, **il 90% degli attacchi a MS Windows** è stato condotto sfruttando la vulnerabilità di **buffer overflow** (descritta nel Microsoft Security Bulletin MS08-067 dell'ottobre 2008)
- Le vulnerabilità delle Web application rappresentano uno dei mezzi più usati per penetrare nei sistemi informativi delle aziende
  - **I più diffusi errori che ancora si riscontrano nelle applicazioni web sono l'assenza di protezione nei confronti di attacchi di tipo Cross-Site Scripting e SQL Injection (rispettivamente il 19% e 17% di tutte le vulnerabilità rilevate) o di altre forme di code injection**

Buffer overflow

- Circa il 12% delle CVE è relativa a questo tipo di vulnerabilità
  - Il fenomeno del buffer overflow si manifesta ogni qualvolta i dati scritti in un buffer di memoria eccedono le dimensioni attese dal programmatore e, in assenza di controlli da parte del programma, debordano in aree di memoria adiacenti sovrascrivendone il contenuto
  - Gli effetti di questo fenomeno sono in genere imprevedibili. Possono portare al blocco del programma. Se i dati in eccesso sono inseriti ad arte, possono consentire all'hacker di far eseguire alla macchina un proprio codice

Memoria prima dell'overflow, la variabile B contiene il numero 4133

Variabile	A								B	
Valore									4133	
hex	00	00	00	00	00	00	00	60	10	25

Se si inserisce nella variabile A la stringa "Nome lungo" le ultime due lettere debordano nell'area riservata alla variabile B modificandone il valore

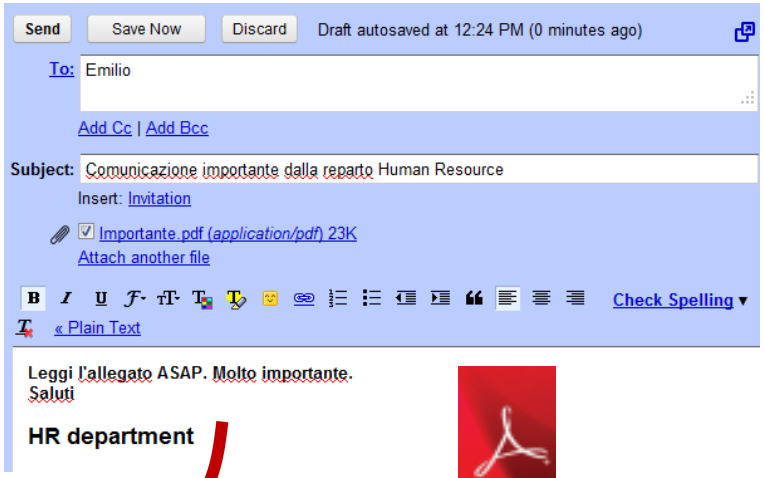
Variabile	A								B	
Valore	N	o	m	e		l	u	n	26479	
hex	4e	6f	6d	65	20	6c	75	6e	67	6f

- Il primo caso documentato di buffer overflow risale al 1988. Questa tecnica di attacco fu infatti sfruttata da Robert Morris per creare il primo malware di cui si abbia notizia con il quale infettò circa 6000 computer Unix collegati alla rete Arpanet (circa il 10% del totale).

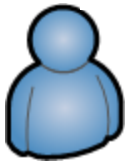
Buffer overflow – esempio di sfruttamento

Emilio@---.com
Maria@---.org
Giuseppe@---.it

Giovanni@---.it



La vittima scarica l'attachment e lo apre. Il file, appositamento creato dall'hacker, installa SW malevolo sul PC della vittima



- Il SW malevolo comunica con l'hacker trasferendogli password, numeri di carta di credito, informazioni riservate, etc. prelevate da PC della vittima
- Il SW malevolo può anche trasformare il PC in uno dei robot o zombie di una Botnet controllabile dall'hacker

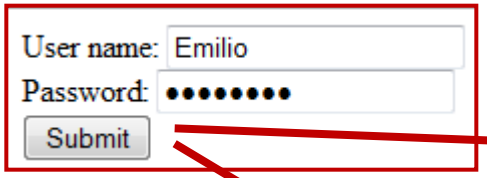
CVE-2011-0595 Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0600.

Cross Site Scripting

ELSAG DATAMAT
A Finmeccanica Company

- Circa il 13% delle CVE è relativa a questo tipo di vulnerabilità (il dato riguarda le applicazioni Web commerciali). Secondo alcune stime tra il 30% e l'80% dei siti web è in qualche misura esposto ad attacchi che sfruttano questo tipo di vulnerabilità
  - Sono suscettibili al Cross Site Scritpting (XSS) le pagine Web che permettono all'utente di inserire dati in un form e che non verificano adeguatamente i dati inseriti. Nella maggior parte dei casi la vittima dell'attacco, però, non è il sito Web ma chi lo visita. Il sito Web è soltanto il tramite dell'attacco
  - L'attacco si attua inducendo la vittima a cliccare su un link apparentemente fidato (ad esempio quello della propria banca) reso disponibile attraverso azioni di phishing. Il link è in realtà modificato nella parte finale in modo da inviare al server (quello della banca della vittima, nell'esempio considerato) dati confezionati in modo tale da far apparire sul browser della vittima dell'attacco informazioni false o pagine di raccolta dati che saranno inviati all'hacker
  - Nella maggior parte dei casi questo metodo è utilizzato per rubare dati di login e di carte di credito, introducendo una pagina di phishing in un indirizzo Web degno di fiducia
  - Alcuni tipi di XSS di recente ideazione sono in grado di creare danni permanenti anche al sito tramite dell'attacco

Dimostrazione XSS (1/2)



http://127.0.0.1/Belsito/form_action.php?FirstName=Emilio&PWD=password

```
<html>
<body>

<form name="input" action="form_action.php" method="get">
User name: <input type="text" name="FirstName" value="User name" /><br />
Password: <input type="password" name="PWD" value="password" /><br />
<input type="submit" value="Submit" />
</form>

</body>
</html>
```

form_action.php

```
<html>
Welcome
<?php echo $_GET["FirstName"]; ?>.<br />
<?php if ($_GET["PWD"]=="123456") {echo("Accesso
autorizzato");} else {echo ("Inserisci la password");} ?>
</html>
```

Dimostrazione XSS (2/2)

ELSAG DATAMAT
A Finmeccanica Company

Ho scoperto un sito meraviglioso.

Questo è il link.

Provalo!

Belsito

Sito o e-mail di phishing

```
<body style="text-align:center;
background-image: url('Pace.jpg')">
<h1> Ho scoperto un sito meraviglioso.</h1><h1> Questo è il link.</h1>
<h2>Provalo!</h2>
<a href='http://127.0.0.1/belsito/form_action.php?FirstName=<h2>Inserisci i tuoi dati</h2>
<form name="input" action="../bad_site.php" method="get">
User name: <input type="text" name="FirstName" value="User name" /><br />
Password: <input type="password" name="PWD" value="password" /><br />
<input type="submit" value="Submit" />
</form> &PWD=password'><h1>Belsito</h1></a>
</body>
```

Sito fidato

Benvenuto

Inserisci i tuoi dati

User name: User name

Password: ••••••••

Submit

Inserisci la password

Informazioni per l'hacker

Il nome dell'utente è Emilio
La sua password è 123456

Contenuto malevolo inserito nel sito fidato

Trasferimento delle informazioni sottratte all'hacker (ad es. via e-mail)

Un esempio reale di Cross-Site Scripting

Pagina Web della Presidenza spagnola della UE www.eu2010.es (gennaio 2010) come appariva a chi vi accedeva attraverso i link pubblicati su numerosi blog e poi circolati in tutta Europa via e-mail e social forum.

Al posto della foto del presidente Zapatero appariva quella del comico inglese Mr. Bean.

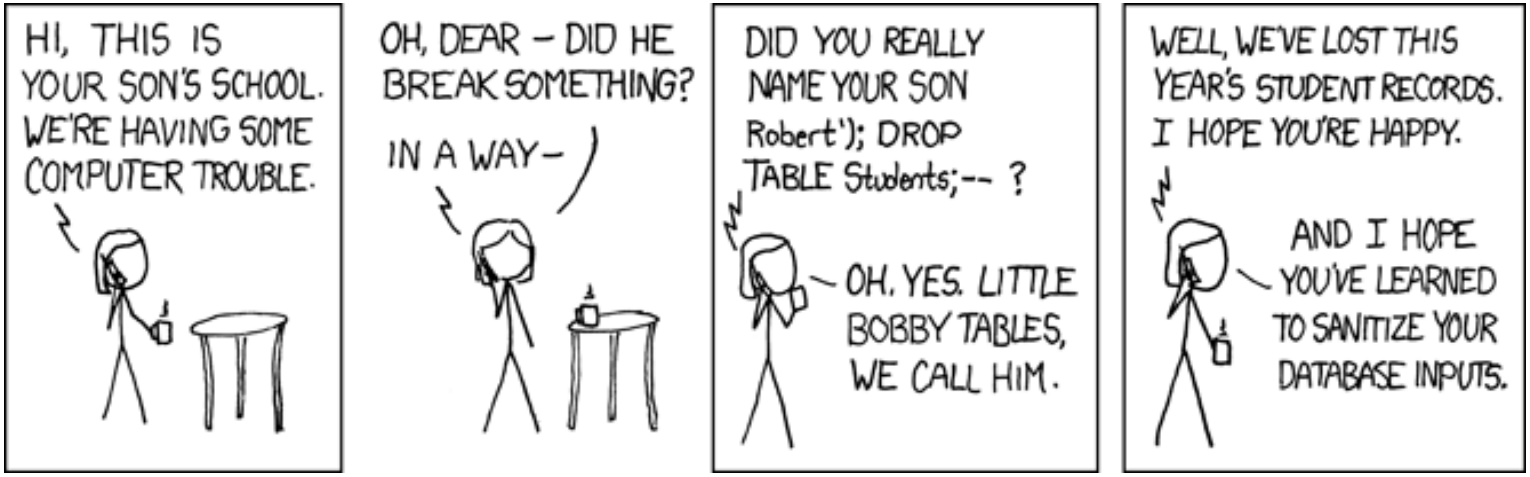
Lo script malevolo è stato probabilmente veicolato sfruttando la funzione di ricerca della pagina

In realtà il sito web non ha subito modifiche, ma a causa dell'enorme traffico che lo ha interessato è rimasto inaccessibile per ore

SQL injection

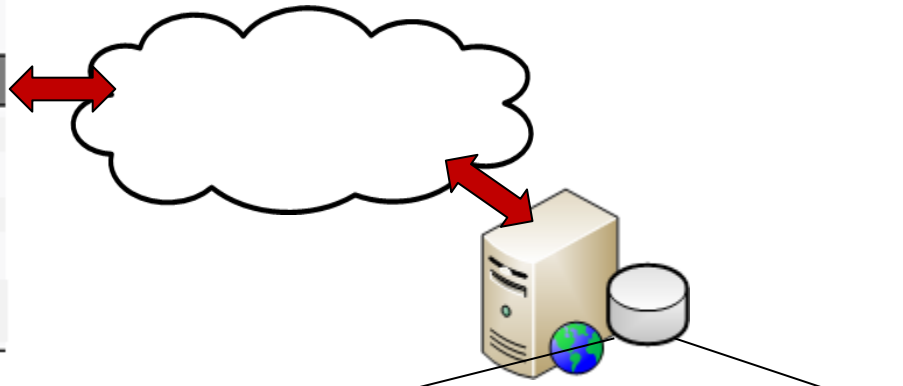
ELSAG DATAMAT
A Finmeccanica Company

- Circa il 13% delle CVE è relativa a questo tipo di vulnerabilità (il dato riguarda le applicazioni Web commerciali). Secondo alcune stime tra il 30% e l'80% dei siti web è in qualche misura esposto ad attacchi che sfruttano l'SQL injection
  - Sono suscettibili di SQL injection le applicazioni Web che si appoggiano ad un database SQL e che non bonificano in modo adeguato i dati inseriti dall'utente
  - L'attacco consiste nell'inserire (injection) una query SQL tra i dati passati all'applicazione web tramite il client. I dati sono organizzati in modo tale la query venga eseguita dal server. Gli attacchi basati su SQL injection hanno come risultato l'estrazione, la modifica o la cancellazione di dati dal database. In alcuni casi, l'hacker riesce anche ad ottenere diritti di Amministratore sul DBMS (e quindi ad esempio può effettuare uno shutdown) o addirittura dare comandi al sistema operativo del server attaccato.



Fonte: http://imgs.xkcd.com/comics/exploits_of_a_mom.png

SQL injection – esempio di sfruttamento



- L'inserimento di questi dati nel form si traduce sul server in un comando che ha come risultato la cancellazione della Tabella "Customers" del database
- Confezionando in modo opportuno la stringa di input è possibile anche leggere i dati nel database e/o modificarli

Customer		
Nome	**Indirizzo**	**Credit card #**
Emilio	Via xxx	21212
Maria	P.zza yxw	56789
Giuseppe	V.Le zxw	54714

Codice PHP

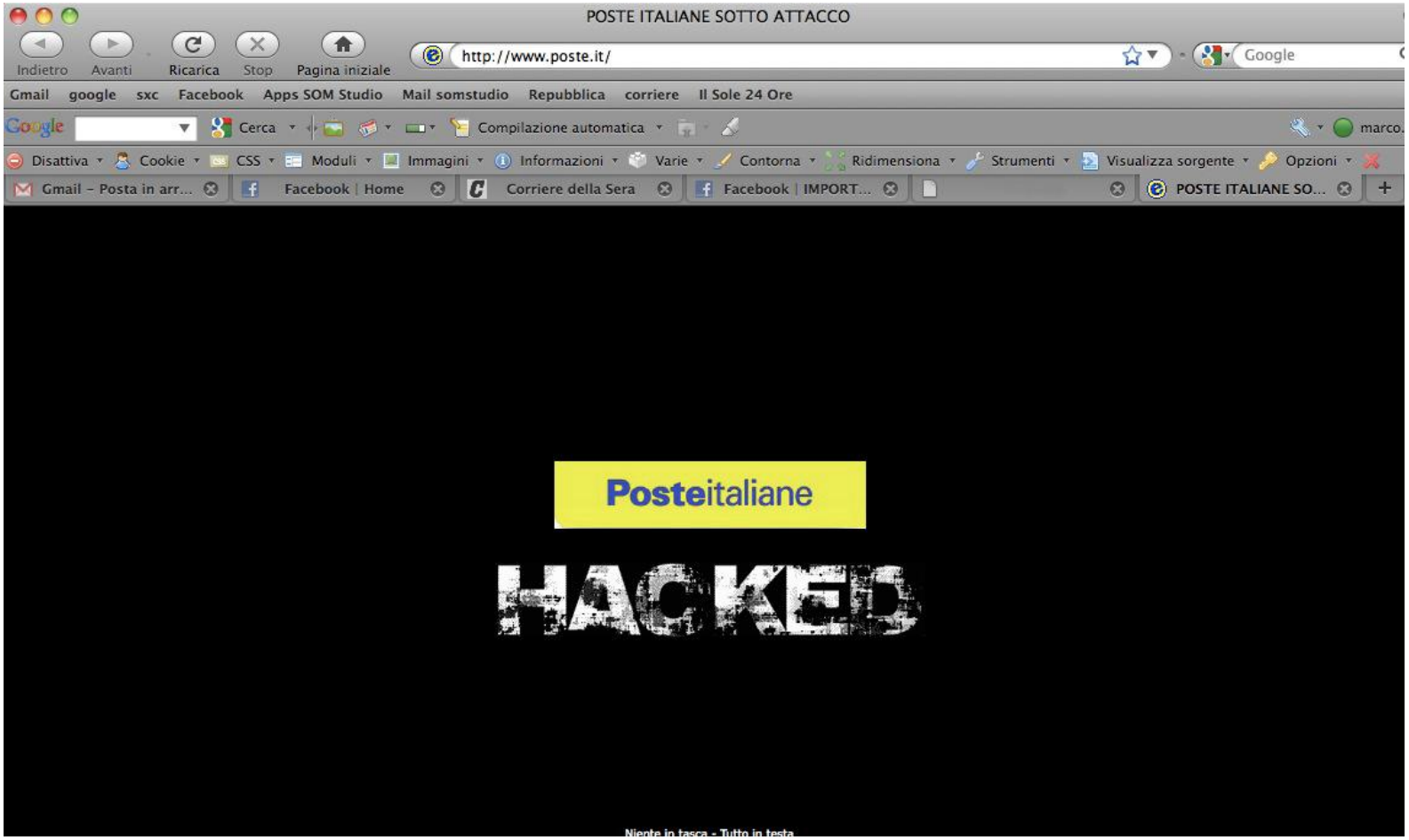
$risposta= SELECT * FROM `Customers` WHERE `Nome` = ' " +Name + "';

SELECT * FROM `Customer` WHERE `Nome` = 'a'; DROP TABLE `Customers';

Un caso reale di SQL injection

ELSAG DATAMAT
A Finmeccanica Company

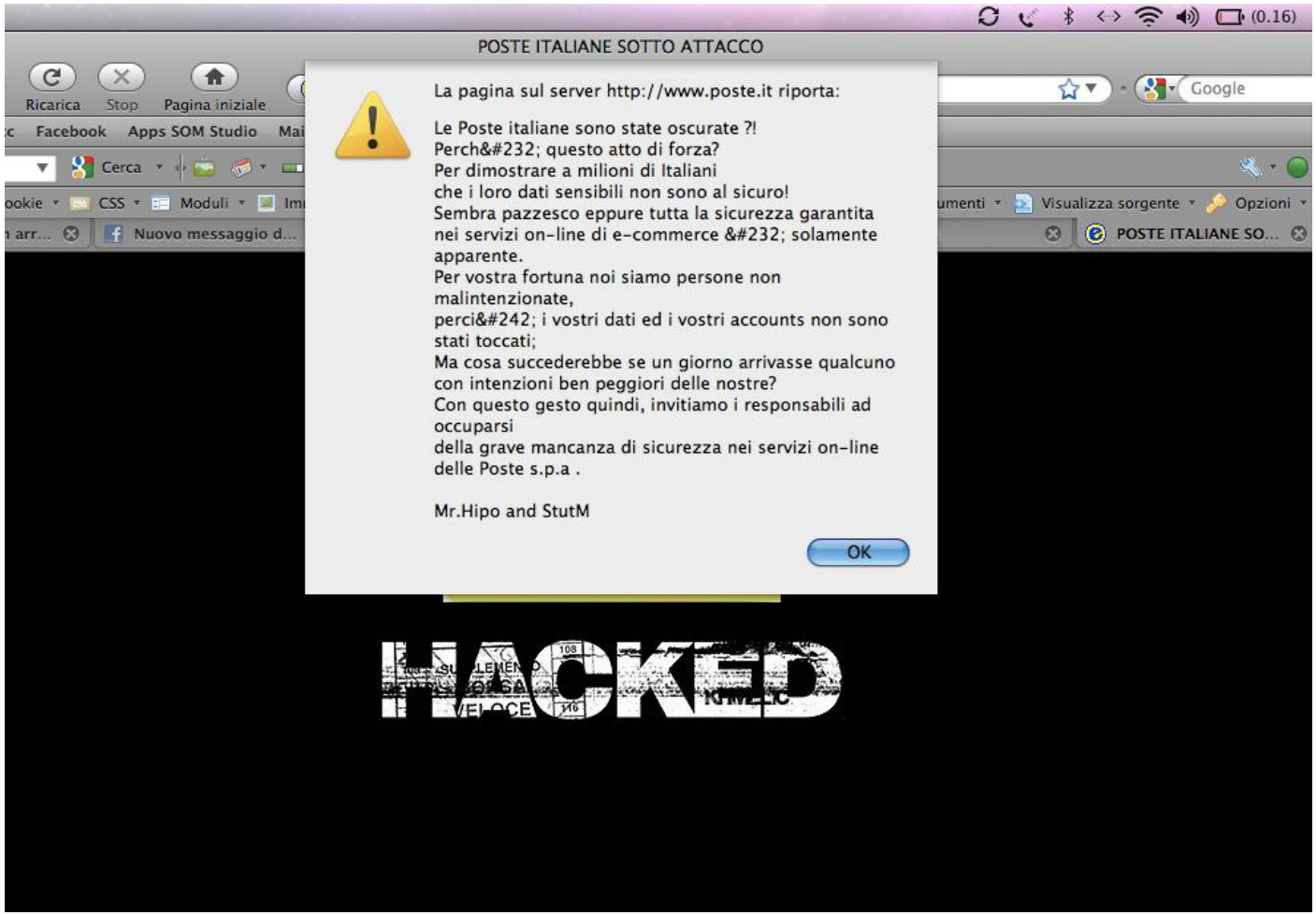
Sabato 10/10/2009 alle ore 19:00



L’attacco al sito poste.it (1/2)

ELSAG DATAMAT
A Finmeccanica Company

Sabato 10/10/2009 alle ore 19:00



L’attacco al sito poste.it (2/2)

ELSAG DATAMAT
A Finmeccanica Company

Il sito delle poste è stato attaccato utilizzando uno strumento SW che automatiza il processo di individuazione delle vulnerabilità all’SQL iniection delle applicazioni Web. Viene commercializzato come strumento di test e raccomandato anche da organizzazioni come l’OWASP

Pangolin - Automated SQL Injection Test Tool

Introduction

Pangolin is an automatic SQL injection penetration testing tool developed by NOSEC.
Its goal is to detect and take advantage of SQL injection vulnerabilities on web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user"s specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.

Video Demonstration

- Inject SQL Server
- Inject MySQL
- More Demos Here

Documentation

- Pangolin White Paper
- Pangolin Data Sheet
- Pangolin User Guide

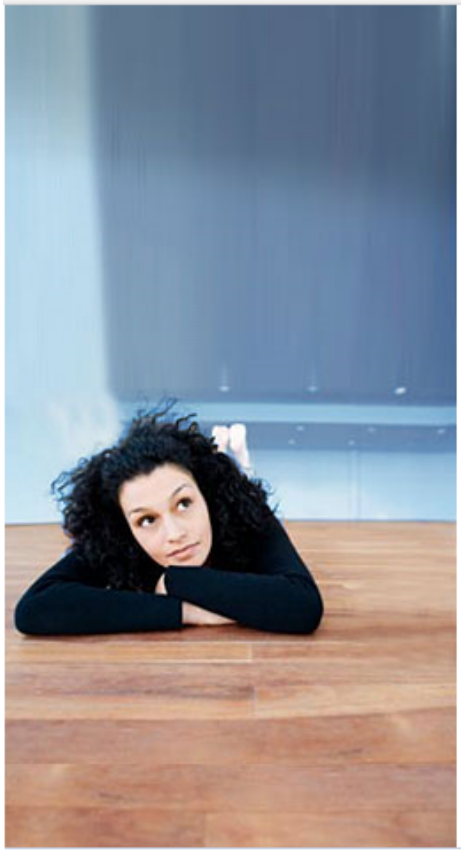
L’home page di poste.it dopo il ripristino

ELSAG DATAMAT
A Finmeccanica Company

Posteitaliane

Home | Chi siamo | Sala stampa | English . Registrazione . Accedi

SOLUZIONI PER... | PRODOTTI | BUSINESS | SERVIZI ONLINE

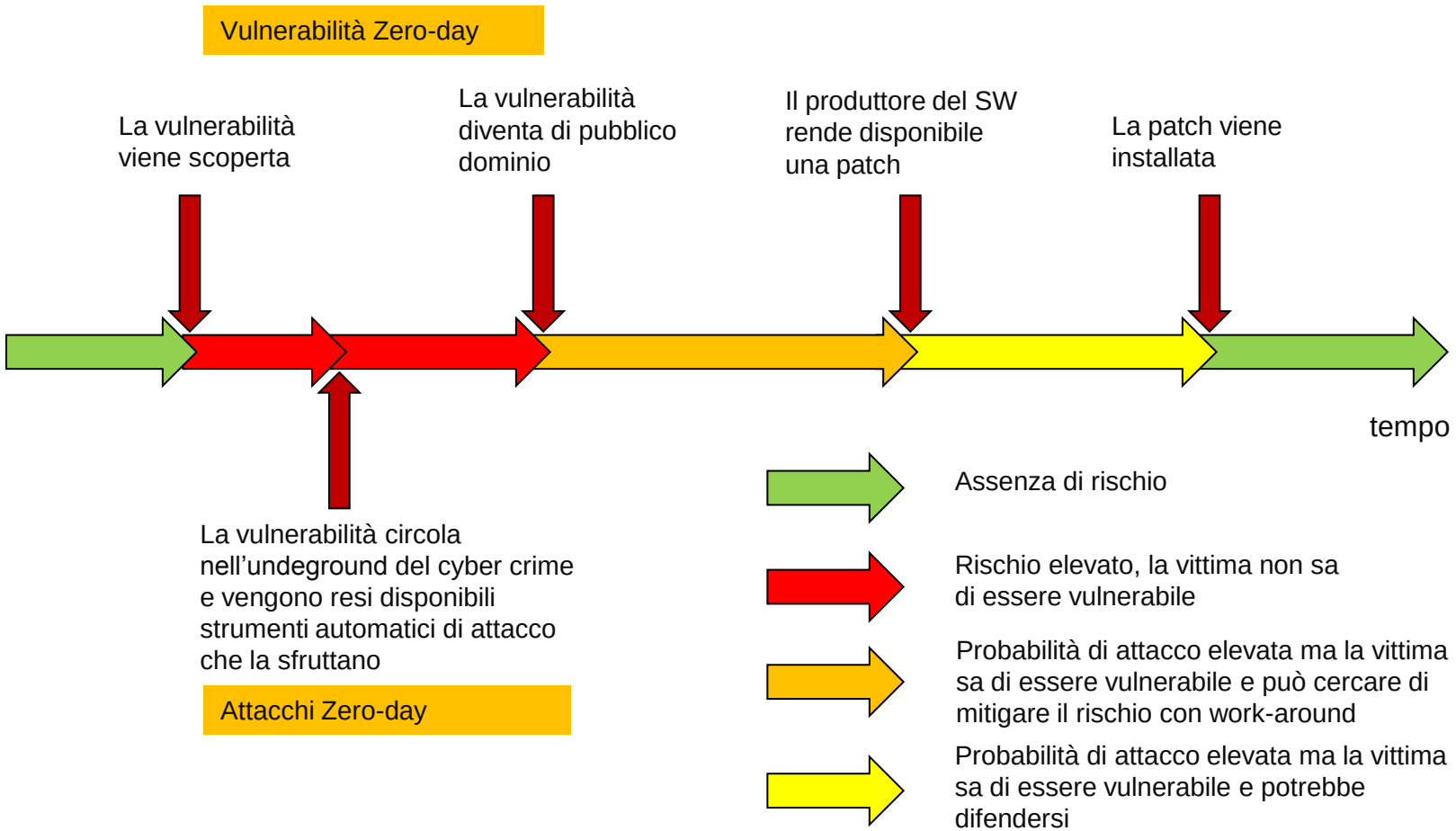


Ripristinata l'home page del sito dopo l'attacco di defacement. Mai stati in pericolo i dati dei correntisti

Un attacco solo superficiale che non ha intaccato minimamente i server con i dati personali degli utenti": è quanto emerge dall'analisi dell'azione di defacement messa in atto sabato sera intorno alle 20 da alcuni hacker che si firmano Mr Hipo e StutM.
Il defacement è un'azione dimostrativa abbastanza comune, che consiste nello sfregiare un sito. In questo caso l'home page di www.poste.it è stata sostituita dai pirati informatici con una pagina dove campeggiava la parola HACKED accompagnata da una nota in cui gli hacker spiegavano che si trattava di un'azione dimostrativa.
Grazie al potente sistema di controlli che garantisce 24 ore su 24 la sicurezza informatica di Poste Italiane, le squadre di ingegneri delle control room sono intervenute in pochi minuti rafforzando i controlli di sicurezza sull'intero sito e mettendosi insieme alla polizia postale sulle tracce dei pirati informatici. "È solo un 'defacement' che riguarda il sito informativo di Poste.it. Non sono stati violati i server con i dati personali degli utenti, che quindi non sono mai stati in pericolo" afferma Gerardo Costabile, responsabile Sicurezza Logica, Poste Italiane. E aggiunge: "I defacement comunque sono un fenomeno abbastanza fisiologico su internet. Negli anni si contano azioni simili contro siti di varie levature, anche istituzionali

| Contattaci | Privacy | Mappa | Trasparenza bancaria | Forniture e gare | Scadenzario fiscale | © Poste italiane 2009

Ciclo di vita delle vulnerabilità

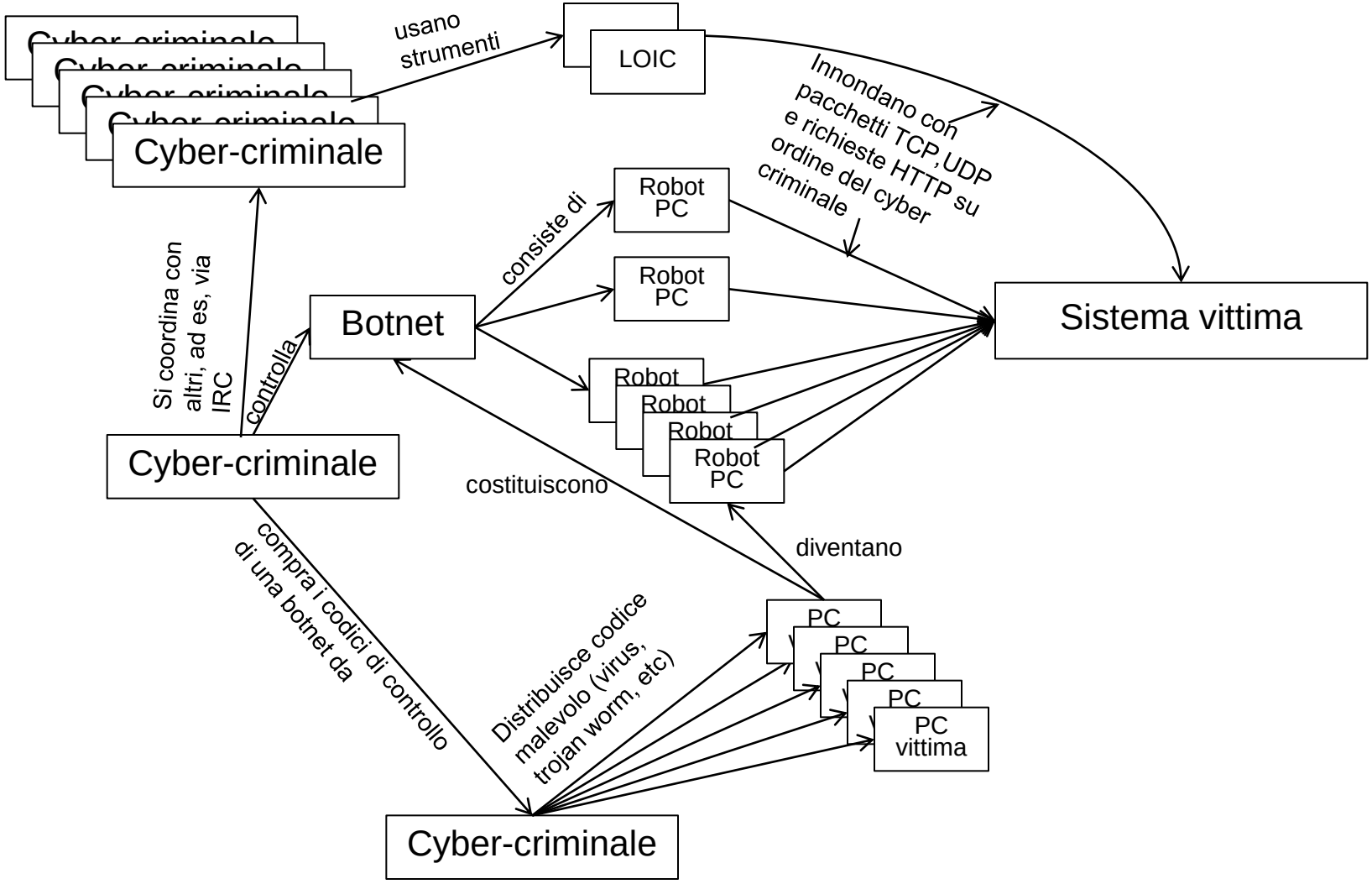


Gli attacchi DoS e DDoS

ELSAG DATAMAT
A Finmeccanica Company

- Gli attaccchi puntano a rendere inaccessibile un Web server in genere a fini dimostrativi, terroristici, politici o ritorsivi
- Si attuano innondando il sistema vittima di richieste, in alcuni casi malformate nel tentativo di far andare in crash il Web server, che ne saturano le risorse di calcolo e di comunicazione
- I primi attacchi DoS erano di norma originati da un'unica fonte (e quindi più facilmente rintracciabile e filtrabile)
- Si parla di DDoS (Distributed Denial of Service) quando l'attacco viene lanciato utilizzando un elevato numero di PC
- Gli attacchi DDoS possono avvenire
  - coinvolgendo molte persone che usano i propri PC e opportuni strumenti SW per inviare le richieste al sistema vittima
  - utilizzando botnet controllate dall'hacker

Modello comportamentale del cyber criminale – attacchi DoS e DDoS



Uno strumento di test utilizzato per attacchi DDoS

ELSAG DATAMAT
A Finmeccanica Company

- **LOIC** è un software Open-source per generare grandi quantità di traffico di rete verso un sistema target e testare la sua risposta sotto carico
- LOIC può essere usato per lanciare attacchi di tipo distributed denial-of-service (DDoS) contro un server inondandolo con pacchetti TCP, UDP o richieste HTTP, nell'intento di interrompere il servizio.
- LOIC è stato utilizzato da Project Chanology, un gruppo derivato dagli Anonymous group, per attaccare il sito web di Scientology, e dagli stessi Anonymous per attaccare con successo il sito web della Recording Industry Association of America nellOttobre del 2010 e di nuovo durante l'operazione Payback nel Dicembre 2010 per attaccare i siti web di società e organizzazioni che hanno osteggiato WikiLeaks
- LOIC è stato usato anche negli attacchi contro Finmeccanica, Eni ed Unicredit del marzo 2011

Struttura del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

Spamming …


« Back to Spam
Delete forever
Not spam
Move to ▾
Labels ▾
More actions ▾
10 FreeViagra for all orders with 90 ED Pills, ED Trial Pack for all orders with 120 ED Pills, Free Shipping, We accept VISA & MasterCard
Spam | X
« Back to Spam
Delete forever
Not spam
Move to ▾
Labels ▾
More actions ▾
Can You Add 4 Inches? Doctors Give You The Truth.
Spam | X
Estella Dorthy to me
show details Apr 14
Reply
« Back to Spam
Delete forever
Not spam
Move to ▾
Labels ▾
More actions ▾
start fr $150 - RolexOmega Tag-Heuer Breitling Chopard Bvlgari Panerai Hublot Zenith Dolce-Gabbana Burberry Cartier Armani Mont-Blanc ...
Spam | X
Gayla Dianna to me
show details Apr 17
Reply
Rep1icaWatches cheap Sale
RolexOmega Tag-Heuer Breitling Chopard Bvlgari Panerai Hublot Zenith Dolce-Gabbana Burberry Cartier Armani Mont-Blanc ...
Cheap Rep1icaWatches is proud to present 6000+ Rep1icaWatches
Reply
Forward

Phishing …

ELSAG DATAMAT
A Finmeccanica Company

PC Kraun Premium NQCD - Con 2a generazione Intel® Core™ i3 - Sconto 50€ fino al 19/4, solo 599€! - www.computerdiscount.it/pc

« Back to Search Results | Archive | Report spam | Delete | Move to Inbox | Labels ▾ | More actions ▾

Riparty con Postepay Inbox | X

servizio clienti postepay to office — show details 11/25/10 — Reply

Concorso "Riparty con Postepay"

Promozioni *postepay* **Dal 1° ottobre 2010 al 31 maggio 2011 ricarica la tua carta postepay* e parteciperai al concorso!**


+


In palio per te ogni mese un fantastico premio!
Scrigno Elation long week end tra arte e sapori per due persone + Fotocamera Digitale Samsung WP 10

E se fai almeno **3 pagamenti sul circuito Visa** durante il periodo del concorso, potrai partecipare all'estrazione finale e vincere una Vespa 125 GTS Giallo Lime.

Ma non solo: effettua una ricarica da 10 euro sul tuo telefonino dalla tua carta postepay entro il 30/11/2010: Postepay, te la regala* !!!

Allora cosa aspetti? Entra subito nel sito: postepay.it

**Partecipano alle estrazioni mensili i titolari che avranno effettuato almeno una transazione Visa nello stesso mese. Sono escluse le transazioni effettuate sul circuito Postamat (es. ricarica carta, pagamento bollettini o altri acquisti sul sito poste.it o presso gli uffici postali)*

http://portale-postepay.serveftp.com/
http://concorso-riparty.servehttp.com/

Phishing

ELSAG DATAMAT
A Finmeccanica Company

Mercato Forex - No Commissioni, Trading Con 1 Clic. - 100.000 € sul tuo Conto Demo - www.CmcMarkets.it

« Back to Spam | Delete forever | Not spam | Move to ▾ | Labels ▾ | More actions ▾

Un regalo per i nostri fedeli Clienti Spam | X

Fineco: The New Bank to amministrazione show details Mar 7 Reply

HAI VINTO UNA RICARICA TELEFONICA DI 50,00 EURO !!!

APPROFITTANE!!!

La campagna regali continua, vai alla sezione, e leggi il regolamento !!!

SALDO POSITIVO: ACCEDI AL TUO CONTO!

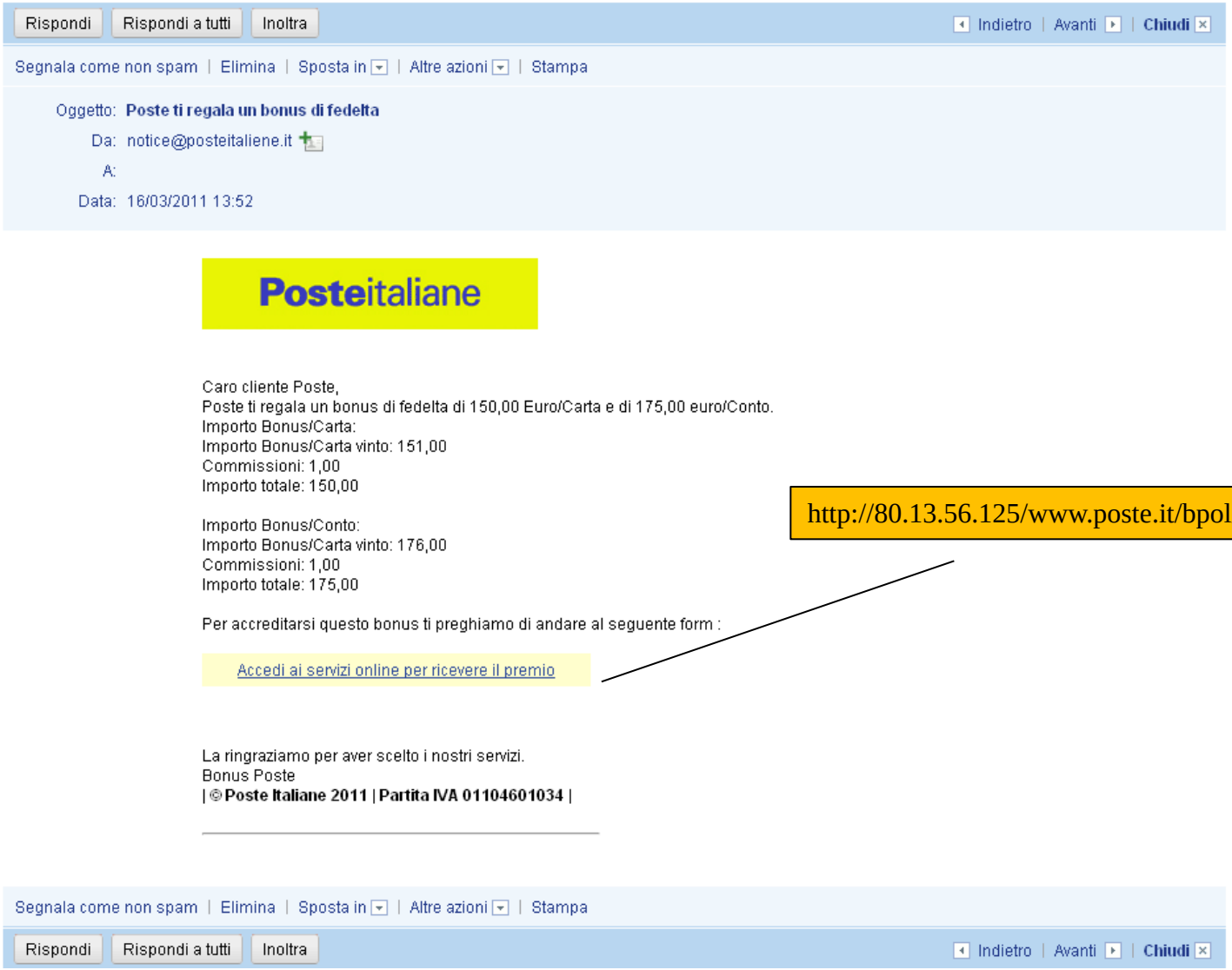
http://fineco.totalh.com/https:/www.fineco.it/fineco.html

RICEVERAI SUL TUO TELEFONINO, UNA RICARICA DEL VALORE DI 50,00 EURO.

GRAZIE PER LA FIDUCIA ACCORDATA AL NOSTRO ISTITUTO.

FinecoBank S.p.A. – Società con socio unico soggetta all'attività di direzione e coordinamento di UniCredit S.p.A. e appartenente al Gruppo Bancario UniCredit - Sede legale: 20131 Milano - P.zza Durante, 11 - Cap.Soc. versato 200.070.430,89 euro, così come risultante dall'ultimo bilancio - N. iscr. R.I. Milano 01392970404.

Phishing



http://80.13.56.125/www.poste.it/bpol/bancoposta/index.html

Tempo di operatività di un sito infetto

- Nel 2008, il tempo medio di operatività di un sito che distribuisce malware (a seguito di un attacco) è stato di 4 ore. Gli attacchi portati con questa tecnica sono brevi perché
  - I programmi malevoli sono prontamente rimossi non appena scoperti
  - I cyber criminali tendono a spostarsi frequentemente da un sito ad un altro per eludere le black list e per cercare di evitare che le nuove varianti del SW malevolo vengano scoperte fornendo utili informazioni agli sviluppatori di antivirus, antispyware, etc.

Fonte

Kaspersky Security Bulletin: Statistics 2008

Struttura del master

ELSAG DATAMAT
A Finmeccanica Company

- Cybercrime e cybersecurity: un nome nuovo per un vecchio problema, ma qualcosa è cambiato ...
- Furto di dati, blocco di sistemi, frodi informatiche: il cybercrime non è solo questo
- Le dimensioni del problema: alcuni incidenti eclatanti
- Ma come è possibile? Vulnerabilità ... e come si sfruttano
- Non solo i sistemi sono vulnerabili: spamming, phishing e altre amenità
- Come difendersi

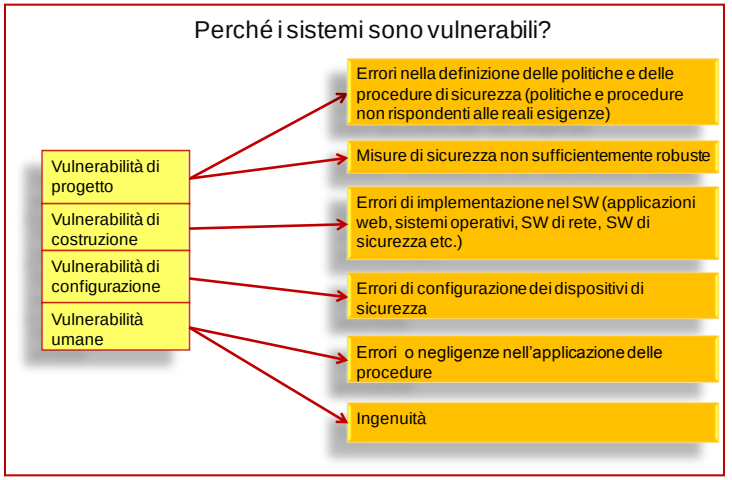
Come difendersi?

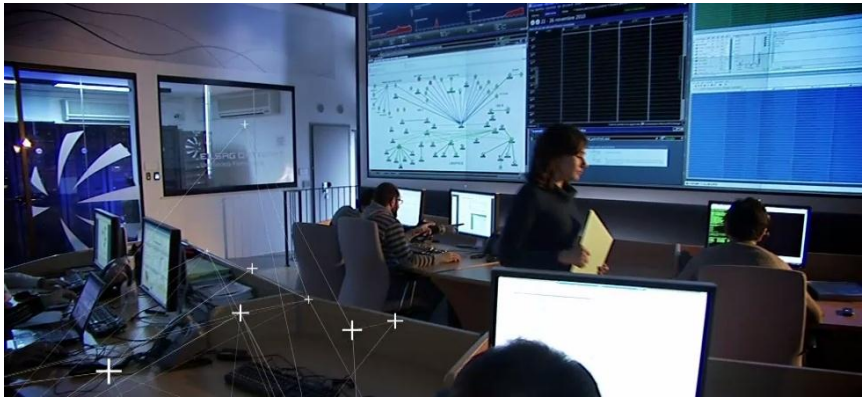
Prima di tutto capire il problema, comprenderne la complessità e le dimensioni

- la sicurezza non è soltanto un problema tecnologico
- un sistema non può essere sicuro in eterno, nuove vulnerabilità vengono scoperte e rese pubbliche continuamente

Il cyber criminale è diventato un professionista e bisogna sapersi difendere da professionisti

- Il monitoraggio continuo e il real time assessment dei sistemi e delle applicazioni è ormai uno strumento indispensabile per la sicurezza raccomandato anche da istituti di ricerca internazionali come il NIST
- Grandi aziende, tra le quali anche Elsag Datamat, offrono servizi di real time managing, monitoring e security assessment attraverso Security Operation Centers (SOCs) nel quale operano team di esperti di sicurezza di elevato livello





Il SOC di Elsag Datamat nella sede di Pescara

Grazie per l’attenzione