Indice

1. NUOVI SOCI
2. INVITO A INFOSECURITY ITALIA 2008
3. CYBERCRIME
4. RAPPORTO CLUSIF SUL CYBERCRIME: BILANCIO DEL 2007
5. BLOG DEL CLUSIT
6. WORKSHOP EUROPEO SUI "GRANDI ATTACCHI"
7. NUOVI OBBLIGHI DI INFORMATION SECURITY PER LE CENTRALI USA
8. NOTIZIE E SEGNALAZIONI DAI SOCI
9. EVENTI SICUREZZA

1. NUOVI SOCI

Hanno aderito al Clusit:

- INFORAV (Roma)
- PROTIVITI (Milano)

2. INVITO A INFOSECURITY ITALIA 2008

Dal 5 al 7 febbraio prossimo si terrà l'ottava edizione di Infosecurity Italia, alla Fiera di Milano.

Durante i tre giorni della manifestazione, il nostro staff sarà presente allo Stand C28 e speriamo di incontrarvi numerosi.

Disponiamo ancora di alcuni codici di accesso, validi per ottenere l'ingresso gratuito in fiera.

Chi fosse interessato può farne richiesta a info@clusit.it.

Il programma dei convegni e seminari organizzati dal Clusit è disponibile su www.clusit.it/docs/infosecMI08A4.pdf.

Troverete tutte le informazioni utili su Infosecurity Italia 2008, oltre al programma dei convegni non direttamente organizzati dal Clusit, all'indirizzo www.infosecurity.it.

3. CYBERCRIME

Il worm Storm si evolve

L'attacco del worm Storm prosegue, e si conferma come uno degli worm più persistenti degli ultimi anni.

Come riportato da Network World
www.networkworld.com/news/2007/122807-storm-switches-tactics-third-

time.html, Storm continua ad evolvere aggiungendo nuove minacce (in particolare un rootkit) ed incrementando la propria pericolosità.

Per quanto, come scrive NW, il rootkit installato da Storm è relativamente "vecchio", e quindi rilevabile da alcuni software di sicurezza (anche se non si dice da quali, e quali versioni), non è un problema da sottovalutare.

Invitiamo quindi nuovamente i nostri lettori alla massima cautela, e a trattare i messaggi di posta elettronica "sospetti" con grande attenzione.

Autore: Mauro Cicognini

Campioni del mondo ma perdenti nel quotidiano

Un incidente informatico al Tribunale di Genova riporta alla cruda realtà: vinciamo i campionati del mondo di security ma non difendiamo le risorse preziose che abbiamo attorno a noi.

L'ho detto su Nova100 http://gigitagliapietra.nova100.ilsole24ore.com/2008/01/e-se-non-fosser.html, si dice "intrusione di hacker" ma ho l'impressione che sia un "semplice" worm che si diffonde per la mancanza di regole minime di sicurezza, per mancanza di formazione di chi usa i sistemi, per mancanza di consapevolezza dell'importanza che ha la difesa dei sistemi informativi per la nostra vita di tutti i giorni.

Cosa mi fa dire che non penso si tratti di una intrusione di hacker? Perchè ho grande rispetto dei "nemici", se fossero stati hacker, che sono sì dei banditi ma sono bravi, preparati, intelligenti, determinati, il sistema sarebbe stato devastato.

Autore: Gigi Tagliapietra

Email di phishing: la situazione attuale.

Lo spamming sta aumentando l'intensità dei suoi picchi (anche di nove volte in raffronto al precedente), la tipologia di email è la stessa da mesi, tranne, come vedremo, che per il phishing.

Ad oggi, le email di spamming si possono dividere nelle seguenti categorie:

- phishing (tese ad ottenere le credenziali di accesso al proprio conto on line);
- vendita di prodotti (medicinali, orologi, ecc.);
- scommesse;
- suggerimenti (es: investimenti in azioni, interventi per migliorare le "prestazioni", opportunità di lavoro, ecc.);
- richieste di contatto (ragazza russa sola, erede unico di un'ingente fortuna, ecc.);
- vincite alla lotteria;
- saluti (biglietti augurali, messaggi vocali, ecc.).

A volte le email pervengono ad ondate successive. In alcuni casi, inondano con centinaia o migliaia di email i domini di una determinata Azienda o Ente, in modo da provocare un forte rallentamento nella ricezione della posta e riempire le caselle, se non prontamente svuotate dalla email spazzatura.

Anche quelle di phishing, una volta più.discrete, ora arrivano a gruppi e, molto spesso, con il risultato che il ricevente nemmeno le legge, e le cancella tutte in un colpo solo. Infatti, risultano pervenire da quattro o cinque banche diverse, come se tutti avessero più rapporti di conto on line con così tante banche!

Sul fronte della tipologia di messaggi, da pochi giorni si nota qualche novità nella speranza, per il criminale, di riuscire ad ingannare qualche utente.

Possiamo raggruppare le email di phishing in base alla tipologia di messaggio che viene inviato, vuoi positivo (ad esempio, per prevenire atti criminali o per premiare), o negativo (ad esempio, perché l'utente ha sbagliato più di tre volte l'immissione della password).

Vediamo le diverse tipologie:

POSITIVI:

la banca o Ente emittente la carta di credito è attento alla sicurezza; con la email inviata chiede la verifica dei dati per l'accesso online, oppure per attivare un rapporto di conto (in alcuni casi la email dice che il codice dispositivo arriverà via posta, ma per attivarlo bisogna digitare le credenziali, e quindi il codice dispositivo!

Ciò è interessante, in quanto sembra che con queste email i criminali sembrano puntare a clienti con qualche problema di comprensione o fortemente distratti, e tutto ciò fa riflettere sulla reale composizione dell'universo degli utilizzatori di funzionalità offerte dal mondo finanziario e sulla possibile percentuale di utenti con ridotte capacità critiche);

un addebito sul conto è andato a buon fine; se il Cliente ha qualche rimostranza, acceda al conto digitando le note credenziali (è ovvio che, nella mente dell'ignoto criminale, il Cliente sprovveduto accede subito per vedere di che si tratta!);

il Cliente è stato premiato per la sua fedeltà all'accesso online: per ottenere la vincita (da 350 a 500 euro a seconda dell'Azienda) si deve accedere al conto digitando le credenziali, ovviamente!

NEGATIVI:

la banca o Ente è intervenuto bloccando il conto; ciò per una di queste cause: tentativi di accesso che hanno provocato il blocco della password, accesso da un indirizzo del Cliente diverso da quello solitamente utilizzato (in questo caso si nota una incongruenza: l'accesso è bloccato, ma si chiede al Cliente di digitare le credenziali per accedere!)

un accredito è stato bloccato, in quanto vi sono delle irregolarità; il Cliente acceda al conto per correggere tali difformità.

Ciò che fa piacere osservare, è sia come le Aziende - tramite l'Autorità Giudiziaria - intervengano immediatamente per bloccare gli indirizzi Internet forniti dalle email di phishing, sia sulla efficacia dei più recenti software prodotti per difendere i computer (antiphishing, antispamming, personal firewall, ecc.).

In conclusione, ci sembra che, per le ragioni sopradette, la situazione phishing, a tre anni dal suo manifestarsi, appaia oramai avere un lento declino nell'area dell'efficacia.

Una preoccupazione, invece, ci assilla. Come scritto diversi mesi fa, e riportato anche dalla stampa specializzata, non si assiste da tempo ad un attacco virus massiccio. Aumentano invece gli spyware ed i

malware, ossia, programmi atti a catturare le informazioni digitate sul computer ovvero a dirottare su siti criminali gli utenti.

Appare pertanto esserci una stretta correlazione fra i due fenomeni. Infatti, qualora vi fosse un massiccio attacco di virus tesi a boccare le comunicazioni o a distruggere il contenuto dei computer, gli utenti interverrebbero con tempestività e senza tentennamenti nel migliorare le difese dei computer.

Il consiglio, quindi, che ci sentiamo di dare, è chiaramente quello di adottare misure periodiche quali le seguenti:

- sensibilizzare gli utenti ed i Clienti sui possibili rischi nei quali possono incorrere se: non aggiornano il software a protezione del computer utilizzato, evitano di accedere a siti non conosciuti, non scaricano musiche o filmati o foto da siti scono
- intensificare i controlli sui computer, specialmente alla ricerca di spyware; possibilmente, tal fine, eseguire la scansione del pc tramite un antivirus o software diverso da quello dell'antivirus attivo sul computer;
- mettersi in allarme in caso di attività insolita del computer (da non confondere con l'aggiornamento in background del software di sistema).

Fonte: ANSSAIF - www.anssaif.it

Worm Wi-Fi

Non sono solo i PC ad essere suscettibili da tipologie di attacco "tradizionali", se così si può dire.

Hao Hu e Steven Myers ricercatori dell'Indiana University, in collaborazione con Vittoria Colizza e Alessandro Vespignani del Complex Networks Lagrange Laboratory (CNLL), Institute for Scientific Interchange (ISI) di Torino, in una pubblicazione http://arxiv.org/PS_cache/arxiv/pdf/0706/0706.3146v1.pdf illustrano come sia possibile realizzare un worm in grado di sfruttare le debolezze intrinseche in (ahimè) diffuse configurazioni di reti Wi-Fi per attaccare gli stessi router wireless, installando su di essi firmware opportunamente modificati.

Le principali novità introdotte in questo lavoro sono:

- l'ipotesi secondo cui il worm si diffonderebbe esclusivamente attraverso le reti wireless sfruttando la concentrazione di router di questo tipo in grandi contesti urbani: da qui, non è da escludere che evoluzioni di un tale attacco porti a azioni diversificate a seconda del tipo di rete fisica, una caratteristica fino ad oggi non considerata in questo tipo di malware;
- la possibilità che il worm violi la chiave WEP, qualora sia presente almeno questo minimo livello di protezione, con un attacco a forza bruta;
- la possibilità di accedere, sempre basandosi su un dizionario pre-costituito di password, alle interfacce amministrative dei router per installare un firmware modificato, in grado quindi di porre sotto il controllo dell'attaccante il dispositivo.

Per descrivere la potenziale diffusione del worm i ricercatori hanno utilizzato modelli basati sullo studio della diffusione delle malattie infettive negli organismi animali e nell'uomo, poichè la modalità di infezione del

worm è atipica rispetto ai "cugini" che sfruttano Internet (il worm incriminato, infatti, utilizzerebbe il raggio di copertura del segnale, analogamente al "contagio" umano, per individuare altri router da infettare). I risultati: 20.000 potenziali infezioni nella città New York in 2 settimane, la maggior parte delle quali in 24 ore.

Possibili soluzioni? Attenersi alle buone pratiche di sicurezza da tempo consigliate per gli apparati Wi-Fi: abilitare l'autenticazione e la cifratura del canale con WPA o WPE, data l'obsolescenza e la ormai dimostrata debolezza del protocollo WEP, dando per scontato (e ancora oggi non è purtroppo possibile farlo) che almeno questo sia comunque utilizzato... I ricercatori affermano che la complessità dell'attacco è tale da ritenere che non possa essere realizzato un worm del genere di qui a breve, fortunatamente: c'è tutto il tempo per prepararsi a dovere!

Autore: Luca Bechelli - Fonte: ComputerWorld
www.computerworld.com.sg/ShowPage.aspx?pagetype=2&articleid=7276&pubid=3&tab=Home&issueid=122)

In aumento i reati online

E' allarme: Italia sesta al mondo per numero di vittime. Segmaliamo un articolo apparso sul Corriere della Sera dello scorso 19 gennaio, ripreso anche nella versione online.

www.corriere.it/cronache/08_gennaio_19/I_truffatori_della_rete_07666ac8-c665-11dc-9f4d-0003ba99c667.shtml

4. RAPPORTO CLUSIF SUL CYBERCRIME: BILANCIO DEL 2007

Come ogni anno, il CLUSIF ha presentato un rapporto sugli eventi più significativi che hanno caratterizzato l'anno precedente, in materia di cybercrime.

La presentazione è disponibile in francese (prossimamente lo sarà anche in inglese) sul sito del CLUSIF

https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k7-fr.pdf

Il rapporto di quest'anno è particolarmente interessante, ricco di riferimenti e di documentazione.

Tra gli argomenti emergenti:

1. Mondes virtuels : l'appât du gain
2. Perturber, déstabiliser…
   - Attaques en réputation
   - Le hacking pour focaliser l'attention ?
   - Espionnage industriel
   - Réseaux sociaux, opportunités de malveillance/renseignement
3. Sophistication des attaques
4. Enjeux malveillants sur le eCommerce
   - Fraude aux cartes bancaires via Internet
   - Escroqueries via les sites d'enchères
5. Evocation de faits marquants
   - « Cyber-guerre » Estonie

- Cyber-attaques « chinoises »
- Enjeux de sécurité sur les infrastructures SCADA

I rapporti degli anni precedenti sono disponibili in francese ed inglese all'indirizzo

https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER%2DCRIMINALITE

5. BLOG DEL CLUSIT

Dopo qualche mese di "sperimentazione" prende il via il **blog del CLUSIT**, uno spazio in cui i soci possono partecipare con segnalazioni, commenti e riflessioni sul mondo della sicurezza.

E' un modo nuovo di favorire la partecipazione dei soci al dibattito e nel contempo di offrire al mercato spunti e suggerimenti perchè ci sia sempre più informazione e consapevolezza che la protezione dei sistemi informativi è una necessità inderogabile e vitale per le istituzioni, le imprese e per i singoli individui.

La formula del blog offre immediatezza e tempestività nell'informazione e allarga, attraverso i commenti, il dialogo con l'utenza più generale, preparandoci a giocare il ruolo di orientamento che il CLUSIT intende svolgere attivamente con la prossima iniziativa di "Online Sicuro".

La pubblicazione dei messaggi è riservata ai soci a cui è affidata la responsabilità dei contenuti e del rispetto di una "netiquette" che mantenga alto il livello e la qualità dell'iniziativa.

Il sito è già visibile all'indirizzo http://blog.clusit.it (se avete un aggregatore RSS attivate subito il feed!) e ci auguriamo che, dopo qualche mese ancora di "rodaggio", possa diventare un punto di riferimento autorevole e utile per tutti e possa offrire contenuti e spunti che periodicamente saranno riportati sulla newsletter e sul sito ufficiale dell'associazione che continueranno a svolgere la loro funzione.

6. WORKSHOP EUROPEO SUI "GRANDI ATTACCHI"

Lo scorso 17 gennaio si è tenuto a Bruxelles un workshop organizzato dalla DG Information Society and Media per valutare le implicazioni e le "lezioni" che si possono apprendere dai recenti attacchi su larga scala alle infrastrutture informatiche. (Presentazione ed agenda della giornata: http://blog.clusit.it/sicuramente/files/08ws170108.pdf)

Per il Clusit era presente il presidente Tagliapietra che, sempre online anche durante i lavori, ha pubblicato alcuni appunti e spunti di riflessione direttamente sul blog del Clusit.

Live da Bruxelles (1) - La coda lunga
http://blog.clusit.it/sicuramente/2008/01/live-da-bruxell.html

Live da Bruxelles (2) - Silentbanker
http://blog.clusit.it/sicuramente/2008/01/live-da-bruxe-1.html

Live da Bruxelles (3) - Mashups e la verità
http://blog.clusit.it/sicuramente/2008/01/live-da-bruxe-2.html

Live da Bruxelles (4) - Noi siamo internet
http://blog.clusit.it/sicuramente/2008/01/live-da-bruxe-3.html
Live da Bruxelles (5) - Home Router
http://blog.clusit.it/sicuramente/2008/01/live-da-bruxe-4.html.

7. NUOVI OBBLIGHI DI INFORMATION SECURITY PER LE CENTRALI USA

L'autorità per l'energia USA (FERC: Federal Energy regulatory Commission) ha stabilito nuovi obblighi di protezione contro attacchi informatici per proteggere le infrastrutture critiche.

Link: FERC: News Release - FERC approves new reliability standards for cyber security www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp.

"Today we achieve a milestone by adopting the first mandatory and enforceable reliability standards that address cyber security concerns on the bulk power system in the United States," FERC Chairman Joseph T. Kelliher said. "..

The eight CIP reliability standards address the following topics:

- Critical Cyber Asset Identification;
- Security Management Controls;
- Personnel and Training;
- Electronic Security Perimeters;
- Physical Security of Critical Cyber Assets;
- Systems Security Management;
- Incident Reporting and Response Planning; and
- Recovery Plans for Critical Cyber Assets.

Non c'è scienza missilistica in queste cose, giusto buon senso.

Un investimento per la protezione costa e, se funziona, non ne vedi i ritorni (l'investimento ha successo se non succede nulla).

È il paradosso della sicurezza: bisogna investire per non vederne gli effetti.

La cultura USA è molto diversa da quella italiana. Il fatto di non avere un servizio sanitario esteso ed efficiente per tutti educa le persone che "non c'è qualcun altro che pensa per te se qualcosa va storto".

Ricordo un'amica che aveva l'assicurazione auto (non obbligatoria) scaduta e non si sarebbe mai messa per strada. Se in Italia l'RC auto non fosse obbligatoria, ci sarebbero 13-15 assicurati...

La sicurezza è come il fitness, occorre consapevolezza, è una questione di stile di vita e devi dedicartici per evitare i problemi.

Anche in Italia abbiamo definito delle linee guida per la protezione delle infrastrutture critiche www.isticom.it/index.php?option=com_content&task=view&id=16&Itemid=1 (a qualche riunione ho avuto il piacere di partecipare), solo che non le abbiamo rese obbligatorie... sic.

Autore: Stefano Quintarelli

FERC e **NERC** sono attivi in USA per la regolamentazione della Cyber Security nelle centrali elettriche (che in tutti gli States sono 2800!): tutte

potenziali porte di ingresso alla grande Griglia elettrica (National Grid). Ci sono regole e ci sono anche multe salate se non ci si allinea a criteri minimi di protezione. Ci sono però anche i vincoli di bilancio ed altro: alcuni manager elettrici stanno valutando che i "costi della sicurezza" possono a volte essere molto elevati, e forse "conviene" pagare le multe, mettendo a repentaglio la sicurezza di tutti...

La CIA segnala che vulnerabilità esistono, e che intrusioni a scopo di estorsione si sono verificate in "diverse regioni, fuori dagli USA"...

vedi anche:
http://council.smallwarsjournal.com/showthread.php?p=38209

Autore: Enzo Maria Tieghi

8. NOTIZIE E SEGNALAZIONI DAI SOCI

La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese

Gabriele Faggioli, membro del CTS Clusit, ci segnala che terrà un seminario dal titolo "L'utilizzo delle strumentazioni informatiche e telematiche aziendali: limiti normativi, poteri di controllo del datore di lavoro, policy, e strumenti operativi", organizzato dal MIP Politecnico di Milano.

Per maggiori informazioni: www.mip.polimi.it/ictprivacy. Per i soci Clusit è previsto uno sconto del 20%.

Un'Azienda Informatica con sedi a Roma, Genova e Milano ricerca neolaureti con buona competenza in programmazione linguaggi Java e/o C++ da inserire in gruppi di lavoro anche presso clienti. Principali sedi di lavoro sono: Genova, Milano, Parma ed alcune atre città del centro-nord. Si assicurano trattamenti adeguati agli standard di mercato. Chi fosse interessato può scrivere a info@clusit.it

9. EVENTI SICUREZZA

4 febbraio 2008, Milano

1a Conferenza nazionale servizi innovativi e tecnologici

www.conferenzanazionaleservizi.org

5-7 febbraio 2008, Milano

Infosecurity Italia 2008

www.infosecurity.it

5 febbraio 2008, Milano

Seminario Clusit - Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

https://edu.clusit.it/scheda_seminario.php?id=18

7 febbraio 2008, Milano
Seminario Clusit - Sicurezza degli ambienti virtualizzati
https://edu.clusit.it/scheda_seminario.php?id=19

26-27 febbraio 2008, Milano
Cisco Expo 2008
www.ciscoexpo.it

28 febbraio 2008, Roma
Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi
https://edu.clusit.it/scheda_seminario.php?id=22

11 marzo 2008, Roma
Seminario Clusit - Sicurezza degli ambienti virtualizzati
https://edu.clusit.it/scheda_seminario.php?id=21

17-21 marzo 2008, Milano
Seminario CISSP
www.clusit.it/isc2/calendario_isc2.htm

25-28 marzo 2008, Amsterdam
Black Hat Briefing & Training Europe
www.blackhat.com

2 aprile 2008, Milano
Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi
https://edu.clusit.it/scheda_seminario.php?id=20

2-3 aprile 2008, Amsterdam
Forrester's Security Forum EMEA 2008 (Sconto 20% per i soci Clusit)
www.forrester.com/events/eventdetail?eventID=2068

19 aprile 2008, Monza
Esame CISSP
www.clusit.it/isc2/calendario_isc2.htm

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000