

## Indice

1. NUOVI SOCI
2. SICUREZZA DEL VOIP
3. CYBERCRIME
4. NOTIZIE E SEGNALAZIONI DAI SOCI
5. EVENTI SICUREZZA

### 1. NUOVI SOCI

Hanno aderito al Clusit:

- Prolan Network Solutions (Roma)
- RITTAL (Vignate - MI)

### 2. SICUREZZA DEL VOIP

#### **Crackare VoIP: "It's so easy a caveman could do it"**

Fonte: [www.informationweek.com/news/showArticle.jhtml?articleID=202101781&pgno=1&queryText](http://www.informationweek.com/news/showArticle.jhtml?articleID=202101781&pgno=1&queryText)

Edwin Andreas Pena e Robert Moore si sono resi colpevoli nel 2006 di una delle più grandi frodi mai conosciute in merito all'utilizzo del VoIP. Pena, infatti, la mente del "colpo" ha assoldato qualcuno con i necessari skill tecnici, Moore per l'appunto, al fine di diventare il gestore illegittimo del traffico di un network di VoIP provider.

In seguito alle intrusioni, riuscite, Pena ha iniziato a vendere sottocosto ad alcune aziende quel traffico telefonico che poteva gestire. Dopo avere guadagnato diversi milioni di dollari vendendo dieci milioni di minuti di conversazione, Pena avrebbe dovuto rendere conto all'FBI delle proprie azioni, ma è riuscito a fuggire.

Moore è stato invece arrestato; rilasciato recentemente, ha rilasciato una intervista ad InformationWeek, nella quale afferma "è stato così semplice che anche un uomo delle caverne ci sarebbe riuscito".

Parole beffarde, tese a stupire un pubblico spesso ignaro dei rischi che corre con le tanto decantate tecnologie "di moda", se non protegge se stesso nel modo corretto.

Moore infatti punta il dito non tanto contro insicurezze insite nella tecnologia o a problemi di natura tecnica o di design di protocolli, applicazioni o infrastruttura; il problema troppo spesso, sottolinea il cracker, sono le credenziali banali, o addirittura di default, che poco accorti amministratori di sistema lasciano su sistemi di produzione, pubblicati su Internet. L'attività della banda è durata oltre due anni e, sempre secondo le dichiarazioni di Moore, "si sarebbero accorti molto

prima che qualcosa di strano stava accadendo, se solo si fossero degnati di monitorare o controllare i loro apparati".

I problemi evidenziati da Moore sono da tempo fonte di preoccupazione per i professionisti del settore, che da anni cercano di attirare l'attenzione di aziende, utenti, VoIP Service Provider e media al fine di garantire configurazioni quanto meno affidabili ed adeguate per una tecnologia, il VoIP, che plug'n'play non è.

Autore: Alessio L.R. Pennasilico [mayhem@alba.st](mailto:mayhem@alba.st)

Il Clusit, per fornire sia ai soci che al mercato una serie di informazioni corrette, oltre ad avere organizzato seminari che trattano anche questi argomenti, ha in cantiere un quaderno dedicato alla sicurezza del VoIP.

### 3 . CYBERCRIME

#### **Nuovo attacco di phishing: Carta SI**

Alle usuali e oramai stantie email, oggi si aggiunge una "new entry", ovviamente già bloccata:

*Gentile Cliente,*

*la informiamo che e' disponibile on-line (<http://infosistemcartasi.info/login.html>) il suo estratto conto (riferito al codice del rapporto 03500-977608: potra' consultarlo, stamparlo e salvarlo sul suo PC per creare un suo archivio personalizzato.*

*Le ricordiamo che ogni estratto conto rimane in linea fino al terzo mese successivo all'emissione.*

*Grazie ancora per aver scelto i servizi on-line di CartaSi.*

*I migliori saluti.*

*Servizio Clienti CartaSi*

*Per favore, non risponda a questa mail: per eventuali comunicazioni, acceda al Portale Titolari (<http://infosistemcartasi.info/login.html>) e ci scriva attraverso 'Lo sportello del Cliente': e' il modo piu' semplice per ottenere una rapida risposta dai nostri operatori.*

*Grazie della collaborazione.*

**OPPURE**, in una forma più sintetica:

*Gentile Cliente,*

*Una nuova gamma completa di servizi online è adesso disponibile ! Per poter usufruire dei nuovi servizi online di CartaSi.it occorre prima diventare UTENTE VERIFICATO.*

*Accedi ai servizi online di Cartasi.it e diventa UTENTE VERIFICATO »*

*Cordiali Saluti*

con il link che conduce all'indirizzo

<http://66.155.104.123/~contact/www.cartasi.it/33554433&REALMOID/gtw/pages/index.jsp/index.htm>

con una ricostruzione perfetta della Home Page non del sito CARTASI, ma del portale riservato ai Titolari della carta.

Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it)

**La dodicesima indagine CSI (The 12th Annual Computer Crime and Security Survey).**

L'indagine di quest'anno non è stata condotta insieme all'FBI, come negli anni precedenti: ciò probabilmente ha consentito di ricevere un maggior numero di risposte. Su 5000 questionari inviati ad un campione di aziende in tutti i settori economici (il settore Finance ha rappresentato il 20% delle risposte) , sono state ricevute 494 risposte, di cui 194 hanno riportato l'ammontare delle perdite economiche subite. Queste sono state pari a \$ 67.000.000, con una perdita media di \$ 350.000 per attacco.

Le perdite maggiori hanno riguardato: frodi ( 21 milioni); virus (8 milioni); system penetration da parte di esterni (6, 8 milioni); furto di informazioni (5, 7 milioni).

A differenza degli anni passati, quest'anno il 18% dei rispondenti ha asserito di aver subito un attacco mirato via malware. Ciò conferma quanto ANSSAIF aveva già anticipato molto tempo addietro come possibile rischio.

Per quanto riguarda gli attacchi dall'interno, il 36% ha dichiarato di non averne identificati, il 59% di aver subito perdite economiche rappresentanti dal 20 all'80% del totale dei danni incorsi nell'anno, ed il 5% ha dichiarato che la grande maggioranza dei danni sono stati dovuti ad insiders.

Se ci ricordiamo l'indagine "CIO Survey 2007" di Net Consulting, i CIO italiani hanno già segnalato che le minacce alla sicurezza provengono più dall'interno che dall'esterno, e che "la dimensione di queste cresce al crescere della dimensione delle aziende".

Con riferimento ai danni subiti per attacco di virus, oltre il 50% delle aziende ha denunciato che la presenza di virus all'interno dei sistemi dell'azienda è stato causato dall'accesso del personale a siti a contenuto pornografico oppure acceduti ai fini di scaricare software pirata.

A questo proposito, un dato che fa pensare è quello relativo alla sensibilizzazione del personale; infatti, il 48% delle aziende ha dichiarato di spendere meno dell'1% del budget della sicurezza a tale scopo!

In Italia sappiamo che le Aziende hanno a budget investimenti per l'"awareness" del personale, specialmente per aiutarlo ad evitare sanzioni penali. Non abbiamo una quantizzazione degli investimenti previsti, ma - in base a quanto ci risulta - gli investimenti dovrebbero ammontare nel 2008 ad almeno il 3% del budget dedicato alla Sicurezza.

Se si legge il diagramma relativo alla tecnologia utilizzata per proteggere gli asset dell'azienda, è sconcertante osservare che ancora esistono aziende prive di software antivirus o di firewall! I sistemi anti-intrusione (IDS) sono installati nel 69% delle aziende; il 66% delle aziende incrypta i dati in transito e il 47% quelli memorizzati; il 40% utilizza strumenti di analisi forense. Solo il 28% utilizza sistemi di sicurezza per il wireless.

Scarsa risulta attenzione alla protezione dei laptop e delle chiavi USB.

Su quest'ultimo dato, si deve aprire una parentesi.

La chiave USB è un tool - come sappiamo - utile per copiare i dati (e quindi sottrarli), ma può costituire, per un criminale, una via per inserire un virus malevolo all'interno di un computer in LAN e, successivamente, ottenere informazioni utili per portare a termine dei progetti a danno dell'Azienda.

Una domanda. Se viene trovata per terra o su un tavolo una chiave USB, qual' è l'azione più ovvia? Inserirla nel computer per vederne il contenuto?

Questa tecnica è millenaria: si chiama cavallo di Troia!

Non è allora il caso di sensibilizzare il personale anche su eventi di questo tipo?

Per concludere, citiamo le risposte sulla tecnica utilizzata per valutare l'efficacia del sistema di tecnologia di sicurezza: il 63% utilizza l'Audit interno; il 53% usa penetration tests eseguiti da risorse interne od esterne, il 49% applica strumenti automatici.

Il testo originale è scaricabile da [www.anssaif.it/allegati/CSISurvey2007.pdf](http://www.anssaif.it/allegati/CSISurvey2007.pdf)

Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it)

---

I dati di 79.000 utenti finlandesi sono stati resi pubblici sul web.

Si tratta di un ennesimo episodio che riguarda una delle problematiche più inquietanti per la sicurezza ICT: il furto dell'identità digitale.

Il "lavoro" dei criminali è, come spesso accade, ancor più facilitato dal fatto che molti utenti utilizzano password troppo semplici e spesso usano le stesse password per accedere a diversi servizi.

Fonte: [www.f-secure.com/weblog/archives/00001293.html](http://www.f-secure.com/weblog/archives/00001293.html)

#### **4. 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***

---

Si stanno chiudendo le iscrizioni alla **6° edizione del Corso di Alta Formazione ISM - Information Security Management**, organizzato dal Cefriel e dal MIP, Politecnico di Milano. Saranno messe a disposizione dei profili più meritevoli 7 borse di studio a copertura parziale.

Per maggiori informazioni è possibile consultare il sito [www.securman.it](http://www.securman.it) o contattare il Coordinamento [securman@cefriel.it](mailto:securman@cefriel.it)

---

Vi Ricordiamo che ENISA ha organizzato per i giorni 8-9 Novembre un evento in Barcellona incentrato sul tema della **gestione del rischio IT per le PMI**. L'evento intende evidenziare la preparazione e le lacune delle PMI in tema di gestione del rischio informatico. Saranno anche presentati alcuni case studies selezionati da 5 Stati Membri, per discutere diverse strategie per il trasferimento di conoscenza sui metodi di gestione del rischio.

Maggiori dettagli al link: <http://enisa.inteco.es/>

È disponibile anche un programma di sponsorship per 25 PMI o consulenti di PMI per partecipare al convegno ricevendo il rimborso delle spese (form sul sito).

---

L'Istituto Nazionale per il Commercio Estero (ICE) ha promosso, insieme alla Banca Mondiale (WB), uno studio sulla **partecipazione italiana ai bandi di gara finanziati dalla Banca Mondiale**. Lo studio verrà realizzato dal Dipartimento di Studi Economico-Finanziari e Metodi Quantitativi dell'Università di Roma "Tor Vergata".

Lo studio prevede di sottoporre ad un campione di Imprese Italiane un Questionario che consenta di rilevare:

- il livello di conoscenza delle Imprese relativo alle modalità di partecipazione a bandi di gara internazionali, con particolare riferimento ai bandi finanziati dalla Banca Mondiale;
- le motivazioni alla partecipazione;
- le problematiche riscontrate.

Lo studio conta, sulla base delle informazioni collezionate, di orientare interventi e predisporre strumenti istituzionali atti a favorire la partecipazione delle Imprese Italiane ai bandi di gara della Banca Mondiale e ad incrementarne la probabilità di successo.

L'ICE sollecita la partecipazione delle Imprese a compilare il questionario online, disponibile al link [www.economia.uniroma2.it/ICE/benvenuto.asp](http://www.economia.uniroma2.it/ICE/benvenuto.asp). Le imprese che parteciperanno all'iniziativa potranno:

- partecipare alla giornata di presentazione dei risultati dello studio (presumibilmente il 18/12/2007);
- ricevere il rapporto finale;
- essere inserite nelle mailing list di WB e di ICE.

---

Anche quest'anno, il giorno 27 novembre, si terrà a Pisa il convegno **Net&System Security**. Tema specifico del convegno sono le nuove frontiere dell'IT-Security. I lavori occuperanno l'intera giornata durante la quale saranno approfonditi in modo particolare quegli aspetti che, nell'ultimo anno, si sono maggiormente imposti all'attenzione degli addetti ai lavori. Novità di quest'anno è la presenza dell'area espositiva e l'introduzione di due sessioni di tutorial la mattina.

L'ingresso è gratuito, per procedere alla registrazione: [www.atsystemgroup.org/it/convegni/nss07/registrazione](http://www.atsystemgroup.org/it/convegni/nss07/registrazione)

---

Il comitato SP99 di ISA (International Society for Automation & Control), dopo aver reso disponibile la parte 1 dello standard ISA-S99 per la messa in sicurezza di reti e sistemi di controllo e produzione, stà per rilasciare la parte 2 dello standard **Manufacturing & Control Systems Security**.

Il documento, in fase di discussione e di votazione, è consultabile all'indirizzo <http://tinyurl.com/2btlga>

Fonte: Enzo Maria Tieghi, autore del quaderno Clusit **Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.)** [www.clusit.it/download/Q07\\_web.pdf](http://www.clusit.it/download/Q07_web.pdf).

## 5. EVENTI SICUREZZA

6 novembre 2007, Roma - Seminario Clusit

### **VoIP (in)Security**

[https://edu.clusit.it/scheda\\_seminario.php?id=12](https://edu.clusit.it/scheda_seminario.php?id=12)

8-9 novembre 2007, Barcellona - ENISA event on Risk Management

### **Information Risk Management Why Business needs it?**

<http://enisa.inteco.es/>

24 novembre 2007, Roma

### **Esame CISSP**

[www.clusit.it/isc2/calendario\\_isc2.htm](http://www.clusit.it/isc2/calendario_isc2.htm)

27 novembre 2008, Pisa

### **5° convegno Net&System Security**

[www.atsystemgroup.org/convegni/nss07](http://www.atsystemgroup.org/convegni/nss07)

29 novembre 2007, Milano - Seminario Clusit

### **Programmazione Sicura**

[https://edu.clusit.it/scheda\\_seminario.php?id=14](https://edu.clusit.it/scheda_seminario.php?id=14)

**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

**© 2007 Clusit - Vietata la riproduzione**

Clausola di esclusione della responsabilità e informazioni relative al

Copyright: [www.clusit.it/disclaimer.htm](http://www.clusit.it/disclaimer.htm)