REPORT MCAFEE SULLA CRIMINOLOGIA VIRTUALE

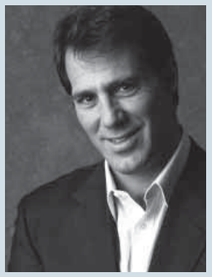
CYBERCRIME: LA PROSSIMA ONDATA

Lo studio annuale di McAfee sui trend mondiali del crimine informatico organizzato e Internet in collaborazione con esperti di sicurezza internazionali

INDICE

PREFAZIONE

CRIMINOLOGIA VIRTUALE. CYBERCRIME. VIOLAZIONI ALLA SICUREZZA INFORMATICA. FURTO ONLINE.



IN QUALUNQUE MODO SI DEFINISCA IL LATO OSCURO DI INTERNET, SI TRATTA DI UNA TRISTE REALTÀ CHE STA CRESCENDO VELOCEMENTE IN MODO ALLARMANTE. IL CRIMINE INFORMATICO MONDIALE È UN PROBLEMA IMPORTANTE, CHE COSTA A AZIENDE E UTENTI FINALI MILIARDI DI DOLLARI ALL'ANNO, E L'UTILIZZO PIÙ ESTESO DELLA TECNOLOGIA NEI PAESI IN VIA DI SVILUPPO NON FA ALTRO CHE APRIRE LA PORTA AD ULTERIORI OPPORTUNITÀ PER I MALFATTORI.

Qual è lo stato del cybercrime oggi? Dove è diretto? In McAfee lavoriamo incessantemente per rispondere a queste domande, ma sappiamo che non siamo da soli in questo arduo compito. Per questo report abbiamo consultato più di una dozzina di specialisti di sicurezza in enti importanti come la NATO, l'FBI, il SOCA, il Centre for Education and Research in Information Assurance and Security (CERIAS), l'Istituto Internazionale Antiterrorismo in Israele e la London School of Economics. Questi esperti sono in prima linea nella lotta contro il crimine online ogni giorno, perciò gli abbiamo il loro punto di vista sullo stato dell'arte di questo pericoloso mondo sommerso, oltre alle loro previsioni su cosa accadrà nel prossimo futuro.

Le conclusioni? Basta leggere quanto segue per tutti i dettagli, ma ai più alti livelli gli esperti concordano sul fatto che il cybercrime si è molto evoluto in termini di complessità e portata. Spionaggio. Trojan. Spyware. Attacchi denial-of-service. Truffe di phishing. Botnet. Exploit zero-day. La triste realtà è che nessuno è immune: singoli individui, aziende e persino i governi. Il mondo si è uniformato e abbiamo rilevato un aumento significativo delle minacce emergenti provenienti da gruppi sempre più sofisticati che attaccano organizzazioni in tutto il mondo. E la situazione può solo peggiorare.

Lo statuto di McAfee prevede lo sviluppo di tecnologia che protegge i dati più preziosi contro questi delinquenti, ma la tecnologia è solo una parte della soluzione. Dall'azione dei singoli, alle aziende che proteggono le loro reti fino ai governi che creano normative esecutive per dissuadere i comportamenti criminali, ci troviamo in una corsa agli armamenti virtuali e dobbiamo collaborare per mantenere il vantaggio.

La battaglia contro il cybercrime è una lotta globale senza tregua, ed è ben lontana dall'essere finita.

Dave DeWalt
Presidente & CEO
McAfee Inc.

“La battaglia contro il cybercrime è una lotta globale senza tregua, ed è ben lontana dall’essere finita”

Dave DeWalt, Presidente & CEO, McAfee Inc.

IL PRIMO REPORT SULLA CRIMINOLOGIA VIRTUALE DI MCAFEE AVEVA EVIDENZIATO COME IL CRIMINE INFORMATICO SI FOSSE EVOLUTO DAI SEMPLICI “SMANETTONI CASALINGHI” A BANDE ORGANIZZATE DI CRIMINALI E SOTTOLINEAVA COME ANCHE LE GANG CRIMINALI ‘VECCHIA MANIERA’ STESSERO INIZIANDO A UTILIZZARE GLI STRUMENTI TECNOLOGICI DISPONIBILI.

Nel 2006, i risultati evidenziavano come i criminali informatici avessero iniziato a adottare tecniche simili a quelle del KGB per reclutare una nuova generazione tra i propri ranghi e a sfruttare le crescenti opportunità di strumentalizzare le nuove tecnologie a fini economici. Sottolineava inoltre la crescente competenza e destrezza del crimine organizzato e come il rischio di cadere vittime di attacchi fosse uguale sia per le aziende che per i singoli.

Quest’anno, McAfee ha collaborato con le forze dell’ordine preposte e esperti di crimini informatici in tutto il mondo per valutare i trend più minacciosi del cybercrime. Il terzo Report McAfee sulla criminologia virtuale mostra come il crimine informatico oggi rappresenta un problema di portata mondiale per tutti noi. Incaricato da McAfee, il Dr. Ian Brown dell’the Oxford Internet Institute e il Professor Lilian Edwards dell’Institute for Law and the Web in Inghilterra, insieme a Eugene Spafford e il suo gruppo del centro CERIAS della Purdue University negli Stati Uniti, hanno condotto ricerche estese e approfondite tra le forze dell’ordine e gli esperti del settore in tutto il mondo per valutare i trend attuali e le minacce emergenti per la sicurezza.

SONO EMERSI TRE PRINCIPALI FATTORI.

Per primo oggi esiste un crescente pericolo per la sicurezza nazionale dal momento che gli attacchi informatici online diventano sempre più complessi, trasformandosi da “attività di ricognizione” a attività ben organizzate e finanziate alla ricerca non solo di un guadagno economico, ma anche politico o tecnico. Ci troviamo nel mezzo di una guerra fredda informatica e in una gara per la supremazia cibernetica?

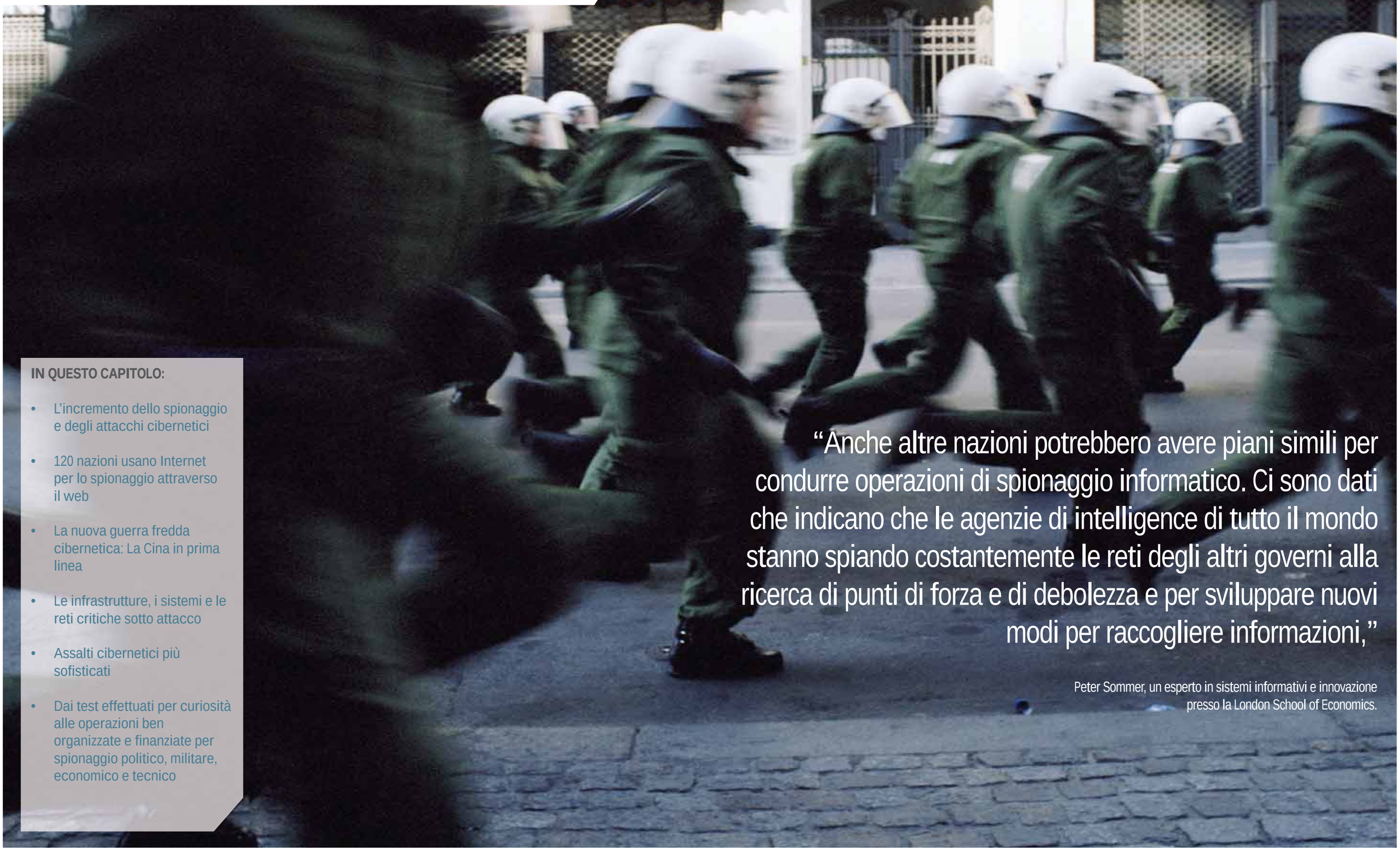
Un secondo trend è la crescente minaccia per i servizi online e la crescente complessità delle tecniche di attacco. Il social engineering, per esempio, ora viene utilizzato insieme alle tecniche di phishing, il che rende la situazione ancor più complessa e minaccia sempre più la fiducia in Internet del pubblico.

Il terzo e ultimo trend è il mercato emergente della commercializzazione delle vulnerabilità dei programmi software che potrebbe essere utilizzato per portare avanti attività di spionaggio e attacchi contro reti di infrastrutture governative vitali. I risultati indicano una vaga linea di demarcazione tra le vendite legali e illegali delle vulnerabilità software.

Il report termina con uno sguardo sui trend futuri e le sfide per il 2008.

CAPITOLO UNO : LA CRESCENTE MINACCIA INFORMATICA PER LA SICUREZZA NAZIONALE

Come Internet è diventata un’arma per lo spionaggio politico, militare e economico



IN QUESTO CAPITOLO:

- L’incremento dello spionaggio e degli attacchi cibernetici
- 120 nazioni usano Internet per lo spionaggio attraverso il web
- La nuova guerra fredda cibernetica: La Cina in prima linea
- Le infrastrutture, i sistemi e le reti critiche sotto attacco
- Assalti cibernetici più sofisticati
- Dai test effettuati per curiosità alle operazioni ben organizzate e finanziate per spionaggio politico, militare, economico e tecnico

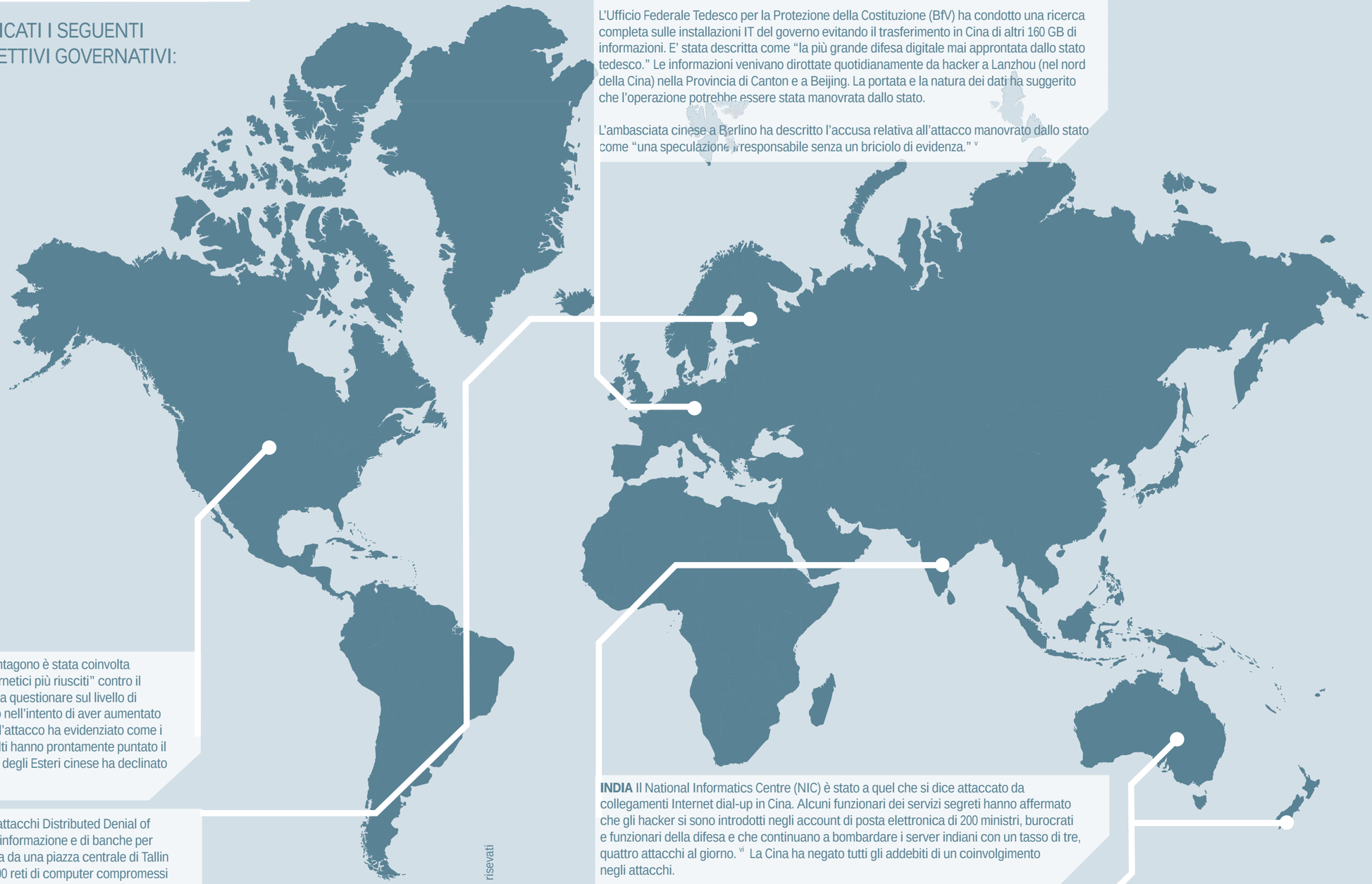
“Anche altre nazioni potrebbero avere piani simili per condurre operazioni di spionaggio informatico. Ci sono dati che indicano che le agenzie di intelligence di tutto il mondo stanno spiando costantemente le reti degli altri governi alla ricerca di punti di forza e di debolezza e per sviluppare nuovi modi per raccogliere informazioni,”

Peter Sommer, un esperto in sistemi informativi e innovazione presso la London School of Economics.

CAPITOLO UNO : LA CRESCENTE MINACCIA INFORMATICA PER LA SICUREZZA NAZIONALE

Come Internet è diventata un'arma per lo spionaggio politico, militare ed economico

NEGLI ULTIMI 12 MESI SI SONO VERIFICATI I SEGUENTI ATTACCHI INFORMATICI CONTRO OBIETTIVI GOVERNATIVI:



GERMANIA Il famoso settimanale tedesco Der Spiegel, ha riportato che si pensava che la Cina si fosse intrufolata nel sistema informatico della Cancelleria tedesca e nei sistemi di tre ministeri, infettando le reti con programmi spia. I presunti attacchi si sono verificati proprio prima che il Cancelliere Angela Merkel si recasse in visita a Beijing. Gli obiettivi erano i computer presenti nella Cancelleria e i Ministeri degli Esteri, dell'Economia e della Ricerca.

L'Ufficio Federale Tedesco per la Protezione della Costituzione (BfV) ha condotto una ricerca completa sulle installazioni IT del governo evitando il trasferimento in Cina di altri 160 GB di informazioni. E' stata descritta come "la più grande difesa digitale mai approntata dallo stato tedesco." Le informazioni venivano dirottate quotidianamente da hacker a Lanzhou (nel nord della Cina) nella Provincia di Canton e a Beijing. La portata e la natura dei dati ha suggerito che l'operazione potrebbe essere stata manovrata dallo stato.

L'ambasciata cinese a Berlino ha descritto l'accusa relativa all'attacco manovrato dallo stato come "una speculazione irresponsabile senza un briciolo di evidenza." [v]

STATI UNITI Nel Giugno 2007, una rete di computer del Pentagono è stata coinvolta da delinquenti con sede in Cina in "uno degli attacchi cibernetici più riusciti" contro il Dipartimento della Difesa degli Stati Uniti. Sebbene si possa questionare sul livello di riservatezza delle informazioni rubate, l'incidente è riuscito nell'intento di aver aumentato enormemente i livelli di preoccupazione dal momento che l'attacco ha evidenziato come i sistemi possono essere danneggiati in momenti critici. Molti hanno prontamente puntato il dito contro l'esercito cinese, ma un portavoce del Ministro degli Esteri cinese ha declinato tutte le accuse come "totalmente infondate." [ii]

ESTONIA Nell'Aprile 2007, l'Estonia ha subito una serie di attacchi Distributed Denial of Service (DDoS) contro i server del governo, degli organi d'informazione e di banche per diverse settimane dopo la rimozione di una statua sovietica da una piazza centrale di Tallin alla periferia della città. Al culmine di questi attacchi, 20.000 reti di computer compromessi erano collegati, e l'analisi del traffico dannoso mostrava il coinvolgimento di computer negli Stati Uniti, Canada, Brasile, Vietnam e altre nazioni.

"Si è trattato di una campagna politica scatenata dai Russi; una campagna politica volta a distruggere la nostra sicurezza e la nostra società. Gli attacchi avevano una struttura gerarchica ed erano coordinati," ha affermato Mikhel Tammet, direttore del dipartimento comunicazioni e informatica estone.[iii] E' stato un attacco minuzioso da cui sia gli aggressori che gli aggrediti hanno avuto molto da imparare.

I funzionari russi hanno smentito la dichiarazione. Il portavoce del Cremlino Dmitri Peskov ha definito "fuori questione" il fatto che il governo Russo fosse coinvolto negli attacchi.[iv]

INDIA Il National Informatics Centre (NIC) è stato a quel che si dice attaccato da collegamenti Internet dial-up in Cina. Alcuni funzionari dei servizi segreti hanno affermato che gli hacker si sono introdotti negli account di posta elettronica di 200 ministri, burocrati e funzionari della difesa e che continuano a bombardare i server indiani con un tasso di tre, quattro attacchi al giorno. [vi] La Cina ha negato tutti gli addebiti di un coinvolgimento negli attacchi.

NUOVA ZELANDA & AUSTRALIA Asia Pacific News ha riportato che gli hacker cinesi hanno presumibilmente cercato di introdursi all'interno di reti di computer governativi estremamente riservate in Australia e Nuova Zelanda come parte di un'operazione internazionale più ampia per appropriarsi di segreti militari delle nazioni occidentali. Secondo il sito news.com.au, Canberra ha rifiutato di confermare o negare che le sue agenzie, incluso il Dipartimento della Difesa, avessero subito un attacco informatico. Il primo ministro neozelandese Helen Clark ha confermato che i servizi segreti stranieri avevano cercato di introdursi sulle reti informatiche governative ma che non avevano compromesso le banche dati top-secret. Il governo cinese ha negato qualsiasi coinvolgimento.

IL CRIMINE TECNOLOGICO NON È PIÙ SOLO UNA MINACCIA PER L'INDUSTRIA E I SINGOLI. GLI ESPERTI RITENGONO CHE LE MINACCE ONLINE PER LA SICUREZZA NAZIONALE A LIVELLO MONDIALE RAPPRESENTERANNO UNA DELLE PRINCIPALI MINACCE PER LA SICUREZZA NEL 2008 E OLTRE.

L'analisi suggerisce che i governi e i gruppi filo-governativi ora utilizzano Internet per attività di spionaggio e attacchi informatici contro le infrastrutture nazionali critiche (mercati finanziari, fornitori di servizi pubblici, controllo del traffico aereo) di altri paesi. Nel 2007 sono stati segnalati più casi rispetto a tutti gli anni precedenti. Questa crescente minaccia è stata riconosciuta dal Dipartimento della Difesa degli Stati Uniti.

"Abbiamo registrato tentativi da parte di varie organizzazioni governative e non di ottenere accesso non autorizzato, o comunque di attaccare il sistema informativo del Dipartimento della Difesa," ha confermato un portavoce del Pentagono.[i]

Gli esperti ritengono che l'attacco in Estonia sia il primo esempio concreto di nazione che mostra le propria capacità di combattere il crimine cibernetico. Di sicuro rappresenta un cambiamento storico nel modo in cui Internet viene utilizzato.

"L'intera sequenza di eventi (in Estonia) è molto simile a quanto un governo farebbe per verificare in che modo se la caverebbe. Il tutto sembra un chiaro esempio di un'operazione 'sotto falsa bandiera' (L'idea è quella di 'firmare' l'operazione attribuendone la responsabilità ad altri). Abbiamo visto terroristi intraprendere tali azioni di 'ricognizione delle difese" prima di condurre attacchi fisici,"

ha affermato Yael Shahar, dell'Istituto Internazionale Antiterrorismo in Israele.

QUANTO SONO SOFISTICATI QUESTI ATTACCHI? DA ATTIVITÀ DI RICOGNIZIONE A ASSALTI BEN PROGETTATI

Gli esperti ritengono che la natura dei recenti attacchi sia molto più sofisticata, poiché sono creati specificamente per eludere il controllo dei sistemi governativi cui mirano. Gli attacchi sono passati da ricognizioni iniziali a operazioni ben organizzate e finanziate per ottenere vantaggi politici o economici.

"Il software utilizzato per perpetrare tali intrusioni (contro il Pentagono statunitense) è stato chiaramente progettato e testato da organizzazioni con molte più risorse dei soliti hacker solitari,"

ha affermato l'esperto Dr. Richard Clayton del Cambridge University Computer Laboratory.

Secondo gli analisti della NATO, molti governi sono ancora inconsapevoli delle minacce da affrontare e alcuni non si proteggono contro possibili attacchi: "Molti uffici governativi non si rendono ancora conto che stanno perdendo informazioni. Il 90% dei casi probabilmente sono ancora sconosciuti. Gli aggressori stanno utilizzando software Trojan (programmi che non si replicano ma che causano danni o compromettono la sicurezza del computer) per colpire uffici governativi specifici. Poiché sono creati in modo personalizzato, questi Trojan non sono soggetti al rilevamento delle firme e possono aggirare le tecnologie anti-virus; si tratta perciò di un grosso problema. Gli hacker dispongono di funzionalità dedicate per garantire la qualità che utilizzano su tutto il loro malware per assicurarsi che non venga rilevato."

Gli analisti della NATO hanno affermato che il 90-95% delle minacce contro i sistemi informativi dei membri della NATO potrebbero essere evitati utilizzando strumenti standard e buone abitudini IT, infatti l'ultima serie di attacchi ha rappresentato un prezioso campanello d'allarme per i governi e le principali industrie di tutto il mondo.

"Gli incidenti in Estonia dovrebbereo essere visti come una sveglia. Che il cybercrime sia rappresentato da una nazione, da un'organizzazione di cyber-criminalità o da un singolo individuo, le informazioni raccolte nelle reti dei governi e delle organizzazioni di importanza nazionale dovrebbero essere considerate come obiettivi di alto valore."

ha affermato Dr. Eugene Spafford, executive director del CERIAS (Center for Education and Research in Information Assurance and Security) alla Purdue University

"Sempre di più la stampa ha riportato numerosi intrusioni informatiche all'interno delle reti governative in tutto il mondo. , Sappiamo inoltre che i consulenti e i fornitori di servizi tecnici e di intelligence ai governi hanno scoperto brecce nei sistemi informativi. Sono stati inoltre riportati esempi di attacchi contro le aziende leader di tecnologia: i brevetti tecnologici dovrebbero essere considerati un obiettivo di altro valore sia per i concorrenti che per le altre nazioni, Non è irragionevole credere che alcuni di questi attacchi possano essere statio diretti – o condotti – da governi di nazioni concorrenti. E' un'opinione diffusa che questi tipi di attività malevoli aumenteranno drasticamente nei prossimi anni."

I GOVERNI E LE AZIENDE DEL SETTORE PUBBLICO QUANTO SONO PREPARATE PER COMBATTERE GLI ATTACCHI INFORMATICI?

Eugene Spafford, professore di informatica presso la Purdue University e executive director del Centre for Education and Research in Information Assurance and Security (CERIAS), ha inoltre affermato che la maggior parte delle agenzie governative e aziende in tutto il mondo utilizzano tecnologie e sistemi informatici comuni, ovvero gli stessi prodotti in cui spesso si infiltrano hacker e malware.

PROGETTATI PER INFILTRARSI NEL CUORE DELL'INFRASTRUTTURA DI UNA NAZIONE

Gli analisti della NATO ritengono che il livello di complessità e gestione dei recenti attacchi suggerisce che l'esperienza dell'Estonia sia solo la punta dell'iceberg della guerra informatica. Ogni fase è stata progettata per infiltrarsi nel cuore dell'infrastruttura della nazione e cercare fino a dove i sistemi e le reti potevano reggere ad assalti cibernetici inesorabili. I punti di inizio e fine, calcolati e improvvisi, della ricognizione indicano che non si è trattato di un attacco su larga scala e gli aggressori probabilmente applicheranno quello che hanno appreso per attacchi futuri.

"Le misure di protezione tradizionali non sono state sufficienti per tutelarsi contro gli attacchi che hanno colpito l'infrastruttura nazionale critica dell'Estonia. Sono state utilizzate delle botnet (rete di pc zombie), ma il livello di complessità e il coordinamento visto durante gli attacchi in Estonia è una novità. Si è trattato di una serie di attacchi attentamente pianificati che hanno utilizzato diverse tecniche ed erano mirati a obiettivi specifici. Gli aggressori si sono fermati volutamente prima di essere bloccati," hanno affermato una fonte anonima della NATO.

Sebbene l'Estonia non fosse preparata, comunque, la stessa fonte della NATO segnala che l'impatto degli attacchi potrebbe essere di più lunga durata e più critico per le altre nazioni:

> "Gli attacchi avrebbero potuto causare seri problemi su alcune reti nazionali in altre nazioni europee con funzionalità di monitoraggio e difesa meno sofisticate di quelle dell'Estonia. Report dettagliati sono stati inviati alle nazioni NATO che ora si stanno muovendo per proteggere meglio le loro reti."

L'Estonia ha dimostrato quanto facilmente può essere compromessa l'infrastruttura di una nazione e gli esperti concordano sul fatto che ogni stato sovrano debba isolare propriamente funzioni così critiche.

COME UN ATTACCO INFORMATICO ININTERROTTO E MIRATO POTREBBE PORTARE A UNA CRISI NAZIONALE

La ricaduta negativa derivante da un attacco informatico sull'infrastruttura nazionale di un paese potrebbe essere devastante.
"Gli hacker potrebbero creare scompiglio manipolando le informazioni e i sistemi elettronici cui si affidano il governo, l'esercito e l'industria privata," ha affermato Joel Brenner dell'Ufficio di Controspionaggio Esecutivo degli Stati Uniti. "Acquedotti e fognature, elettricità, mercati finanziari, ufficio stipendi, sistemi di controllo del traffico aereo e stradale... potrebbero tutti essere oggetto di attacchi sofisticati da parte di terroristi sponsorizzati dallo stato o indipendenti." [vii]

UNA GUERRA FREDDA CIBERNETICA? SIAMO NEL BEL MEZZO DI UNA GUERRA FREDDA CIBERNETICA? GLI ESPERTI PENSANO DI SÌ.

I cinesi hanno affermato pubblicamente che stanno svolgendo attività di spionaggio informatico e nel rapporto governativo e, come interpretato dai McAfee Avert Labs, affermano che la tecnologia rappresenterà una parte significativa della guerra del futuro. Stati Uniti, Regno Unito, Germania e molte altre nazioni sono possibili obiettivi, per spionaggio di tipo politico, militare, economico e tecnico.

> "Anche altre nazioni potrebbero avere piani simili per condurre operazioni di spionaggio informatico. Ci sono dati che indicano che le agenzie di intelligence di tutto il mondo stanno spiando costantemente le reti degli altri governi alla ricerca di punti di forza e di debolezza e per sviluppare nuovi modi per raccogliere informazioni,"
>
> ha spiegato Peter Sommer, un esperto in sistemi informativi e innovazione presso la London School of Economics.

"Tutti spiano tutti," ha affermato Johannes Ullrich, un esperto del SANS Technology Institute, evidenziando le azioni di Israele contro gli Stati Uniti e quelle della Francia contro i membri dell'Unione Europea. Ma sono gli aspetti dell'approccio cinese a preoccuparlo. "La parte di cui ho più paura... è l'organizzazione di "indagini" all'interno di industrie strategiche. E' quasi come avere delle cellule dormienti, disporre di modi per danneggiare i sistemi quando se ne ha bisogno se mai si arriverà a una guerra" [viii]
E con circa 120 nazioni che lavorano per approntare i loro posti di comando per un attacco cibernetico, gli esperti ritengono che entro 10-20 anni potremo assistere a una lotta tra le nazioni per la supremazia cibernetica.

Sommer segnala che le nazioni si stanno indubbiamente preparando a lanciare attacchi cibernetici informatici internazionali. L'ambiente politico esistente è quello in cui le nazioni stanno testando il terreno per stabilire la possibile influenza (e i rischi) di tali attacchiassalti. "Le agenzie governative stanno senza dubbio conducendo ricerche su come le botnet possono essere trasformate in armi offensive, ma prima di utilizzare un'arma bisogna essere sicuri di quale sarà il risultato – infatti non si vuole certo che gli attacchi colpiscano i propri alleati per sbaglio. Gli attacchi DDoS rimarranno un problema per i siti web governativi rivolti al pubblico, ma i siti interni sono solitamente più semplici da proteggere," ha affermato.

"I cinesi sono stati i primi a utilizzare gli attacchi informatici per scopi politici e militari," ha affermato James Mulvenon, un esperto delle forze armate della Cina e direttore del Center for Intelligence and Research di Washington. "Sia che si tratti della preparazione del campo di battaglia o di violare le reti collegate al cancelliere tedesco, sono il primo stato a utilizzare la tecnologia per combattere la guerra cibernetica del 21° secolo. Questo sta diventando un problema in sospeso sempre più serio." [x]

Il crimine tecnologico non è più solo una minaccia per l'industria e i singoli. Gli attacchi e lo spionaggio informatico stanno mettendo sempre più in pericolo la sicurezza nazionale e alcuni governi stanno prendendo molto sul serio la minaccia e rafforzando le loro difese. Il procuratore generale australiano, per esempio, ha annunciato dopo gli attacchi di quest'anno che il governo avrebbe speso 70 milioni di dollari australiani per migliorare la sicurezza informatica. Ma tutte le nazioni sono in grado di affrontare un tale impegno?

Chi sarà in pericolo in futuro? Gli esperti ritengono possibili obiettivi informatici quelle nazioni che hanno un numero elevatissimo di collegamenti di rete e quelle nazioni con un ambiente politico instabile.

CAPITOLO DUE: LA CRESCENTE MINACCIA PER INDIVIDUI E AZIENDE

Come i servizi online stanno diventando degli obiettivi primari per i criminali informatici

IN QUESTO CAPITOLO :

- L'aumento delle minacce per i servizi online
- Le super minacce modificate geneticamente
- Nuova tecnologia, nuove minacce - vishing e phreaking'
- Le minacce per l'industria finanziaria

" Ciò che è necessario è che le banche controllino in modo più accurato i trasferimenti, individuando gli schemi, limitando i trasferimenti a destinatari fidati come le aziende del gas."

Richard Clayton, un famoso esperto di sicurezza della Cambridge University

CAPITOLO DUE: LA CRESCENTE MINACCIA PER INDIVIDUI E AZIENDE

Come i servizi online stanno diventando degli obiettivi primari per i criminali informatici

I CRIMINALI INFORMATICI CONTINUANO A AFFINARE LE LORO ARMI E LE VITTIME CHE VOGLIONO COLPIRE.

Gli utenti di Internet effettuano sempre più operazioni bancarie e acquisti online e visualizzano molte delle loro informazioni personali sui siti di social networking, perciò i criminali online utilizzano mezzi sempre più sofisticati per carpire loro tali informazioni. Anche gli impiegati che caricano online e condividono i dati più riservati tramite software di file sharing sono un obiettivo comune.

Il crimine organizzato sfrutta tutte le opportunità per strumentalizzare queste nuove tecnologie basate sul web per commettere crimini classici come le frodi e le estorsioni.

McAfee Avert Labs ritiene che gli attacchi mirati ai servizi web rappresenteranno una delle dieci maggiori minacce mondiali per la sicurezza nel 2008.

Man mano che il crimine su Internet, i furti d'identità e la violazione della privacy diventano parte della consapevolezza pubblica, i consumatori che si affidano ai servizi online potrebbero essere seriamente danneggiati.

IN BREVE, GLI ESPERTI RITENGONO CHE LE PRINCIPALI MINACCE CHE COLPIRANNO GLI UTENTI NEL 2008 SARANNO:

- Forme di attacco nuove e sofisticate
- Mirati contro le nuove tecnologie, come il peer-to-peer e i servizi VoIP
- Mirati contro i siti di social networking online
- Mirati contro i servizi online, in particolare le operazioni bancarie online

LE 'SUPER' MINACCE GENETICAMENTE MODIFICATE

Il malware presenta un nuovo livello di complessità mai visto prima. Queste minacce 'superdotate' sono più resistenti, vengono costantemente modificate e vantano funzionalità estremamente sofisticate come la cifratura.

Un esempio recente di queste nuove minacce superdotate che hanno colpito gli utenti nel coso del 2007 è Nuwar (conosciuto anche come il Worm Tempesta o Storm Worm). Si è trattata della minaccia più sofisticata che gli esperti hanno mai visto circolare. Storm Worm ha stabilito un preoccupante precedente. McAfee Avert Labs prevede che altri sfrutteranno il successo di Storm Worm, aumentando il numero di PC trasformati in bot. I bot sono programmi informatici che danno ai criminali il pieno controllo dei PC. I programmi bot tipicamente si installano furtivamente sui PC di utenti ignari. David Vaile dell'Australian Legal Information Institute e Università del New South Wales ha segnalato che la sua ricerca in Asia Pacifico ha scoperto un mondo spaventoso dove virus personalizzati vengono compilati nell'Europa dell'Est per colpire aziende e agenzie governative specifiche. Secondo Vaile e il suo gruppo, questi virus si stanno evolvendo molto rapidamente creando un paragone con il DNA ricombinante dove tutti gli elementi di un virus o di un Trojan vengono costantemente ricombinati per formare un nuovo organismo.

Eugene Spafford, professore di computer sciences presso la Purdue University e executive director del Center for Education and Research in Information Assurance and Security (CERIAS) concorda sul fatto che la complessità delle minacce informatiche sta evolvendo rapidamente: "Continueremo ad avere meno attacchi come virus e programmi worm manifesti ma ci sarà un aumento delle minacce che prendono il controllo dei PC tramite bot, trojan e browser web. Un altro trend pericoloso sarà l'arrivo di minacce auto-modificanti e minacce che contrattaccano."

STORM WORM

Nuwar, conosciuto anche come Zhelatin e "Storm Worm", è uno dei ceppi di malware più diffusi al momento con nuove varianti quasi ogni giorno. Nuwar è un Trojan horse distribuito tramite campagna massicce di spam con email che contengono un link a un sito che cerca di installare il malware automaticamente o spingere l'utente a installare il codice se l'installazione automatica fallisce. Tutte le macchine infettate vengono controllate tramite una rete peer-to-peer. La botnet viene utilizzata per inviare spam o lanciare attacchi DDoS. E' una delle botnet più grandi al momento, con milioni di computer infettati in tutto il mondo.

COME I CRIMINALI MIRANO A COLPIRE LE NUOVE TECNOLOGIE

Con la più diffusa adozione delle nuove tecnologie Internet, crescono anche le opportunità per i criminali informatici di estorcere e strumentalizzare i singoli individui e le aziende. Nelle applicazioni Voice over IP (Internet Protocol), per esempio, nel 2007 sono state segnalate oltre il doppio delle vulnerabilità di sicurezza di tutte quelle del 2006. Abbiamo anche visto numerosi attacchi di "Vishing" (phishing tramite VoIP) di altro profilo e azioni di "phreaking" (hacking tramite rete telefonica per effettuare chiamate internazionali o intercontinentali). La tecnologia VoIP è ancora una novità e le strategie difensive sono in ritardo. McAfee Avert Labs prevede un aumento del 50% nelle minacce VoIP nel 2008.

Un altro nuovo obiettivo per i criminali informatici sono i servizi peer-to-peer (p-to-p), in particolare WINNY in Giappone, il più popolare servizio p-to-p in Asia. Sebbene non ancora diffuso in Occidente a causa di limiti nella larghezza di banda, le reti p-to-p come WINNY si diffonderanno senza dubbio man mano che la tecnologia si adeguerà.

Il Professor Keiji Takeda del Carnegie Mellon CyLab Japan ha affermato: "Il virus WINNY ha probabilmente avuto origine da violazioni del copyright piuttosto e non è stato sviluppato a fini dolosi o da parte del crimine organizzato, ma l'effetto è stato catastrofico. "

"Molti impiegati carica il sistema p-to-p WINNY sulle reti dell'ufficio, o collegano latptop personalir con dati dell'ufficio tra casa e ufficio, e, come risultato, i dati aziendali sono stati resi pubblici. Poiché le fuoriuscite di dati non avvengono sempre tramite le reti aziendali ma anche da casa, le violazioni ai dati non vengono bloccate dai firewall aziendali e abbiamo assistito a numerosi casi in cui ex-dipendenti conservano dati aziendali sul loro PC o hard disk personale anche dopo aver lasciato l'azienda, perdendo informazioni riservati in modo accidentale."

MALWARE P-TO-P WINNY: LA MINACCIA CHE ARRIVA DAL GIAPPONE

Nelle aziende giapponesi , circa il 50% di tutte le violazioni che interessano i dati sono state collegate al malware che infetta WINNY. Quando WINNY viene colpito, carica dati fondamentali dagli hard disk degli utenti su altri presenti sulla rete p-to-p. Quando ciò accade a un servizio aziendale, i risultati possono essere catastrofici. In Giappone, sono stati sottratti dati da impianti di energia nucleare e indagini di sorveglianza delicate. Il Giappone pretende che le aziende responsabili segnalino pubblicamente le violazioni subite. Comunque, dal momento che i dati sono disponibili gratuitamente sulla rete WINNY, tali dichiarazioni non fanno altre che avvisare i ladri d'identità su quali dati sono fuoriusciti di recente.

Poiché le minacce p-to-p stanno arrivando in Occidente, gli enti normativi dovranno stare all'erta e non applicare soluzioni obsolete alle nuove minacce. McAfee Avert Labs ha già sottolineato che Nuwar, che utilizza la tecnologia peer-to-peer, potrebbe essere il malware più pericoloso mai visto finora.

CAPITOLO DUE: LA CRESCENTE MINACCIA PER INDIVIDUI E AZIENDE

Come i servizi online stanno diventando degli obiettivi primari per i criminali informatici

SOCIAL NETWORKING: I CRIMINALI INFORMATICI VANNO DOVE C'È GENTE

Gli assalti contro i siti di networking consumer stanno diventando sempre più terrificanti. E' stato segnalato che i criminali informatici l'8 Novembre 2007 si sono appropriati di pagine del sito di social networking di News Corp (NWS) MySpace, inclusa la pagina della cantante americana Alicia Keys. Cliccando in qualunque punto della pagina, gli utenti venivano dirottati su un sito web in Cina che cercava di spingere gli utenti a scaricare software che poi assumeva il controllo dei loro PC.

I siti di social networking come MySpace e Facebook sono diventati un obiettivo allettante per i criminali informatici che cercano di colpire le informazioni personali, ingannare gli utenti con truffe di phishing e mettersi al servizio del malware.

Una nuova opportunità per i criminali informatici è la popolarità delle applicazioni presenti sui siti di social networking, per esempio quelle su Facebook che consentono agli utenti di inviarsi l'uno all'altro "brindisi" e "regali di compleanno" virtuali. Immancabilmente gli autori di malware cercheranno di strumentalizzare questa funzionalità per ingannare gli utenti e garantirsi l'accesso alle informazioni personali. I criminali informatici potrebbero così raccogliere immense quantità di informazioni estremamente preziose e negoziabili.

Il nuovo protocollo Open Social di Google è già stato adottato da MySpace e permette la migrazione di dati personali tra siti di social networking, il che potrebbe essere un'ulteriore minaccia, secondo Lilian Edwards, a uno dei principali esperti in sicurezza informatica presso l'Institute for Law and the Web, Università di Southampton, Regno Unito.

LO SCANDALO "COMPARE ME"

Una delle applicazioni più popolari su Facebook è "Compare Me". Agli utenti viene chiesto quali dei loro amici sono più popolari, i migliori per andare a fare shopping, i più affidabili, etc. I creatori dell'applicazione avevano promesso che potevano essere resi pubblici solo i risultati generali (per esempio "X è il terzo più popolare tra i tuoi amici!"). Poche settimane dopo, invece, si è scoperto che dati non anonimi (per esempio "Il tuo amico X ha detto che Y è un amico migliore di te") erano stati venduti per 9 dollari.

Sebbene il danno potenziale causato da 'Compare Me' sia banale, mostra quanto semplicemente i criminali informatici possono ottenere informazioni personali dagli utenti sui siti di social networking. Mostra anche quanto poco riservati sono gli utenti nel condividere informazioni e opinioni online.

"Data la crescita esponenziale dei siti di social networking, il social engineering potrebbe diventare in poco tempo il mondo più semplice e veloce per commettere furti d'identità. Chi ha bisogno di intrufolarsi o cercare tra la spazzatura quando tutto quello che si deve fare è accendere il proprio PC e collegarsi,"

spiega Lilian Edwards.

LE CRESCENTI MINACCE INFORMATICHE PER L'INDUSTRIA FINANZIARIA

Le frodi online stanno già costando milioni di dollari all'anno agli utenti Internet e alle aziende, ma gli esperti ritengono che un costante attacco contro i clienti da parte dei criminali informatici potrebbe anche danneggiare molto la fiducia del pubblico nei servizi bancari online e credono che per mantenere la fiducia nei servizi bancari online, banche e clienti devono assumersi la responsabilità congiuntamente; per esempio, le banche devono investire in migliori misure di sicurezza e i clienti devono impegnarsi a utilizzare gli strumenti che vengono loro forniti.

"La gente afferma di avere più paura del crimine online che delle aggressioni," ha affermato Lord Broers nel Report on Personal Internet Security della Camera dei Lord. "Ciò deve cambiare, altrimenti la fiducia in Internet potrebbe sgretolarsi. Non si può fare affidamento solo sul fatto che i singoli si prendano la responsabilità della loro sicurezza personale. Saranno sempre raggirati dai malintenzionati. Riteniamo che le aziende che traggono profitto dai servizi Internet ora debbano assumersi la loro parte di responsabilità."

COSA STA FACENDO IL SETTORE FINANZIARIO PER COMBATTERE IL CRIMINE INFORMATICO?

Il settore finanziario non sta con le mani in mano. Molte banche hanno introdotto metodi di sicurezza sofisticati come un secondo livello di autenticazione, sebbene questo tipo di sicurezza avanzata qualche volta è limitato a clienti con conti consistenti e la disponibilità varia in base alla geografia.

Il Brasile, per esempio, dispone di uno dei sistemi bancari online più avanzati al mondo. Circa il 100% dei siti di Internet banking utilizza HTTPS e due PIN (uno per collegarsi al sistema e uno per effettuare una transazione). Alcune banche utilizzano anche un'ulteriore password 'one-time', utilizzabile una sola volta, per fornire un livello di sicurezza aggiuntivo. Molte banche europee fanno lo stesso e le banche in Nord America stanno implementando sistemi di sicurezza aggiuntivi.

Non tutti, comunque, sono convinti che gli sforzi per rendere sicuro il banking online si dimostreranno sufficientemente efficaci e abbastanza veloci. Critiche arrivano dal q dottor Richard Clayton, un famoso esperto di sicurezza della Cambridge University

"Gli stratagemmi dell'interfaccia per migliorare la sicurezza dei clienti non sono promettenti e controllare i clienti sarà molto difficile con i lettori di carte." dichiara. L'autenticazione a due livelli potrebbe portare a un'enorme diminuzione del phishing entro il 2009. Non è ancora chiaro se buona parte delle frodi online sia dovuta a tattiche non di phishing.".

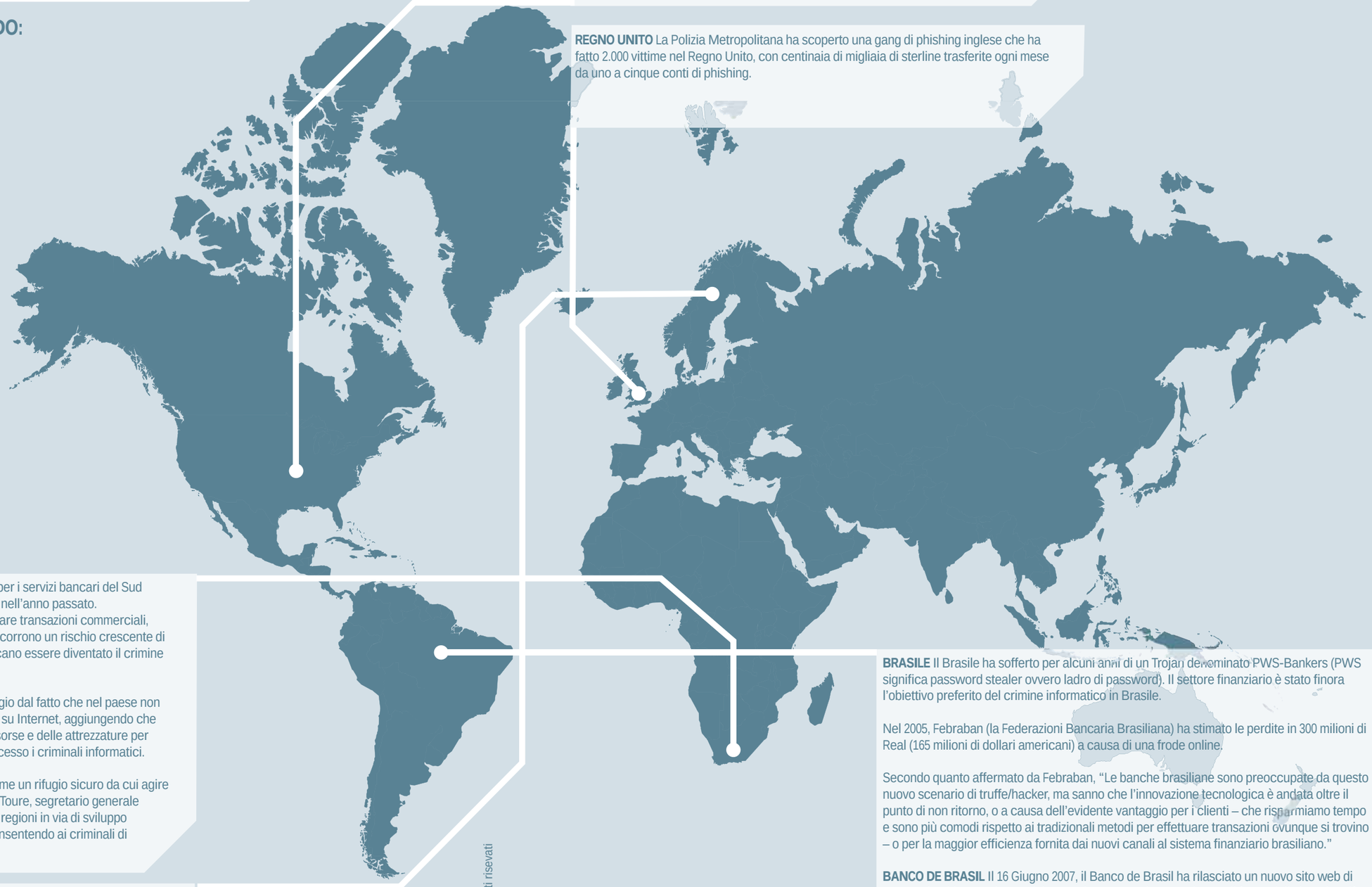
LA FIDUCIA DEL PUBBLICO È IN DECLINO?

Sebbene le perdite dirette per gli utenti di Internet a causa di violazioni della privacy possano essere contenute, recuperabili o addirittura inavvertite, gli esperti hanno paura che l'effetto complessivo possa portare allo sgretolamento della fiducia nelle istituzioni pubbliche come banche e agenzie governative e in particolare nelle operazioni su Internet.

L'impatto del cybercrime sulla fiducia dei consumatori si fa già sentire negli Stati Uniti. Secondo gli analisti di Gartner, la maggior parte dei consumatori non apre email che arrivano da aziende o singoli che non conoscono già. Tre su quattro acquirenti online sono più cauti relativa mente a dove acquistano beni online e un terzo segnala di acquistare meno di quello che farebbero perché non si fidano della sicurezza. Le banche statunitensi stanno già perdendo clienti a causa delle preoccupazioni per la sicurezza . Un recente studio del Ponemon Institute rivela che le violazioni ai dati minano la fiducia dei consumatori e la paura dei furti d'identità ha modificato il loro comportamento d'acquisto. Sommer della London School of Economics afferma che la comunicazione è fondamentale per mantenere la fiducia dei consumatori:

"Per evitare la fuga dalle banche online sarà fondamentale l'efficacia delle loro attività di pubbliche relazioni nelle ore immediatamente successive a quando attacchi significativi e andati a buon fine sono stati resi pubblici. Attività di PR non adeguate unitamente a un evento che non può essere tenuto nascosto con le vittime che parlano con la stampa potrebbero causare seri problemi a una banca online. La banca inglese Northern Rock ha dimostrato che è molto difficile calmare il panico che si crea sul mercato una volta che si è messo in moto."

TRUFFE ONLINE DA TUTTO IL MONDO:



STATI UNITI I singoli individui hanno perso almeno 200 milioni di dollari in frodi online nel 2006 – e si tratta solo di persone che hanno segnalato la loro disavventura all'Internet Crime Complaint Centre dell'FBI. Queste 200.000 vittime delle frodi informatiche hanno affermato di essere state truffate per una media di 724 dollari.

REGNO UNITO La Polizia Metropolitana ha scoperto una gang di phishing inglese che ha fatto 2.000 vittime nel Regno Unito, con centinaia di migliaia di sterline trasferite ogni mese da uno a cinque conti di phishing.

SOUTH AFRICA Secondo Neville Melville, difensore civico per i servizi bancari del Sud Africa, le attività di banking online sono aumentate del 20% nell'anno passato. Poiché l'utilizzo del web da parte dei sudafricani per effettuare transazioni commerciali, inclusi servizi bancari e acquisti online, è in crescita questi corrono un rischio crescente di cadere vittime del crimine informatico, che le ricerche indicano essere diventato il crimine dei colletti bianchi in più rapida crescita nella nazione.

Melville ha affermato che i criminali stanno traendo vantaggio dal fatto che nel paese non esiste una legislazione appropriata per affrontare il crimine su Internet, aggiungendo che la polizia e il sistema giudiziario non dispone inoltre delle risorse e delle attrezzature per indagare in modo efficace sui crimini e perseguire con successo i criminali informatici.

"Al momento, i criminali informatici considerano l'Africa come un rifugio sicuro da cui agire illegalmente senza essere puniti," ha affermato Hamadoun Toure, segretario generale dell'ITU con sede a Ginevra. "Il cybercrime in Africa e altre regioni in via di sviluppo peggiorerà nel momento in cui la banda larga decollerà, consentendo ai criminali di operare in modo più efficace." [xiv]

SVEZIA Durante quella che si ritiene essere la più grande rapina online ad oggi, all'inizio del 2007, truffatori Internet hanno rubato circa 8 milioni di corone (1.1 milioni di dollari; 576.000 sterline) da conti presso la banca svedese Nordea. Circa 250 clienti erano stati ingannati da email di phishing contenenti un Trojan su misura inviato a nome della banca che incoraggiavano le persone a scaricare un'applicazione per 'combattere lo spam'.

Una volta scaricato, il Trojan registrava i tasti digitati che venivano attivati quando gli utenti cercavano di collegarsi al sito di banking online di Nordea. Venivano poi reindirizzati su un'homepage fasulla, dove i loro dettagli di log-in venivano memorizzati e utilizzati dai criminali sul sito reale della banca per rubare denaro dai loro conti.

BRASILE Il Brasile ha sofferto per alcuni anni di un Trojan denominato PWS-Bankers (PWS significa password stealer ovvero ladro di password). Il settore finanziario è stato finora l'obiettivo preferito del crimine informatico in Brasile.

Nel 2005, Febraban (la Federazioni Bancaria Brasiliana) ha stimato le perdite in 300 milioni di Real (165 milioni di dollari americani) a causa di una frode online.

Secondo quanto affermato da Febraban, "Le banche brasiliane sono preoccupate da questo nuovo scenario di truffe/hacker, ma sanno che l'innovazione tecnologica è andata oltre il punto di non ritorno, o a causa dell'evidente vantaggio per i clienti – che risparmiamo tempo e sono più comodi rispetto ai tradizionali metodi per effettuare transazioni ovunque si trovino – o per la maggior efficienza fornita dai nuovi canali al sistema finanziario brasiliano."

BANCO DE BRASIL Il 16 Giugno 2007, il Banco de Brasil ha rilasciato un nuovo sito web di Internet banking, aggiornandolo completamente. Il Banco de Brasil è una delle banche più attaccate del paese e la maggior parte del malware per rubare i dati volto a colpire i clienti della banca era progettato sulla base del vecchio sito.

Dopo pochi giorni, McAfee Avert Labs ha scoperto un repository di codice sorgente di PWS-Bankers pieno di file volti a colpire le banche brasiliane. Un file in particolare aveva attirato la loro attenzione: 'New Banco de Brasil Screen.jpg'. Era datato 21 giugno e aveva la nuova videata di richiesta password del sito web del Banco de Brasil. Presumendo che le date siano precise, in meno di cinque giorni i criminali hanno creato un trojan PWS-Banker funzionante pronto a minacciare il nuovo sito web della banca.

CAPITOLO TRE: IL CRIMINE HI-TECH: UNA SOLIDA ECONOMIA

Il mercato in crescita delle minacce zero-day

IN QUESTO CAPITOLO:

- Servizi per il crimine informatico offresi
- Le leggi per la domanda e l'offerta
- Il mercato legale alimenta il florido mercato nero
- il virtuale arma il mercato

La concorrenza sta diventando così forte che il 'servizio al cliente' è ora diventato un punto specifico

IL TERZO TREND MONDIALE PER LA SICUREZZA IDENTIFICATO DAGLI ESPERTI DEL SETTORE È LA NASCITA DI UN INTERO SISTEMA ECONOMICO EQUIPAGGIATO PER FORNIRE AI DELINQUENTI GLI STRUMENTI PER PERPETRARE CRIMINI INFORMATICI ONLINE .

Questo florido mondo sommerso include siti di aste specializzati, pubblicità di prodotti e anche servizi di supporto. La concorrenza sta diventando così forte che il 'servizio al cliente' è ora diventato un punto specifico quando il crimine organizzato cerca di utilizzare o affittare delle botnet (per inviare spam, bloccare un sito web o anche monitorare i tasti digitati per rilevare le password personali) o farsi creare del malware (per infiltrarsi o danneggiare i sistemi informatici) appositamente. Di seguito una panoramica delle tendenze emergenti in questo settore del crimine informatico:

A BUON MERCATO COME LE BOTNET

Con così tanti PC infetti, la concorrenza per fornire le botnet si è fatta più intensa e il costo per acquistare e affittarle è crollato. Circa il 5% delle macchine esistenti potrebbero essere zombie, e il costo per affittare una piattaforma di spamming oggi si aggira intorno a 0,037 dollari per zombie alla settimana (Fonte: UK House of Lords Report into Personal Internet Security, 2007).

FATTO SU MISURA

Con un budget che va da soli 25 dollari americani fino a un massimo di 1.500 dollari si può acquistare un Trojan creato per rubare e inviare dati delle carte di credito. Il malware viene personalizzato per colpire aziende e enti specifici.

AFFITTARE UNA BOTNET

Per commettere crimini online non è più necessario avere competenze informatiche. Le botnet sono diventati strumenti che possono essere acquistati, venduti e accumulati come le armi o la droga; possono anche essere commercializzate o affittate. Ciò consente ai perpetratori con ridotte competenze tecniche di commettere crimini. [xv]

D'altro canto, gli autori di malware non hanno neanche bisogno di perpetrare crimini loro stessi per avere un ritorno economico; possono semplicemente vendere gli strumenti adatti.


Run PinchBuilder.exe to compile a new version of trojan, always check SMTP server before compilation.
Run Parser.exe to decrypt incoming messages.

Q: Why it's so small?
A: Pinch doesn't actually decrypts passwords, it just retrieves hashes, after they are decrypted using Pinch Parser (Parser.exe).

Q: Bypassing firewalls (zonealarm, outpost, etc)?
A: There's a posibility to bypass firewalls using hidden IE window. In this case Pinch will require an additional HTTP server to send passwords to. You have to build Pinch with 'HTTP protocol' option enabled, take a look at view.php file from 'script' folder for a script example.

Project is written for education purposes only. Author doesn't take any responsibilibies for using Pinch (or parts of it). Using Pinch you see what can hacker potentially steal from your computer, use antiviruses (AVP recommended), and forget about Internet Explorer - it's buggy and insecure, take a look at wonderfull browser Opera 7.

Download Now
Zitat:
Hidden-Text
Sie haben nicht die erforderlichen Rechte, um den Text sehen zu k?Ã¶nnen.

Ci si può abbonare a strumenti che mantengono aggiornati sulle più recenti vulnerabilità, per esempio MPACK o Pinch che includono un servizio di supporto per assicurare che si utilizzino le vulnerabilità più recenti e anche testarli contro soluzioni di sicurezza per validarne l'efficacia. Sebbene molti di questi servizi siano etichettati come venduti a "fini educativi" o puramente per effettuare dei test, è chiaro che potrebbero causare danni se cadono nelle mani sbagliate o vengono venduti da persone con intenti dolosi.
Il ciclo di offerta e domanda è un fattore abilitante per la commercializzazione del crimine informatico.

COME LO SCAMBIO DI ARMI VIRTUALI SEGRETE PREOCCUPA I GOVERNI

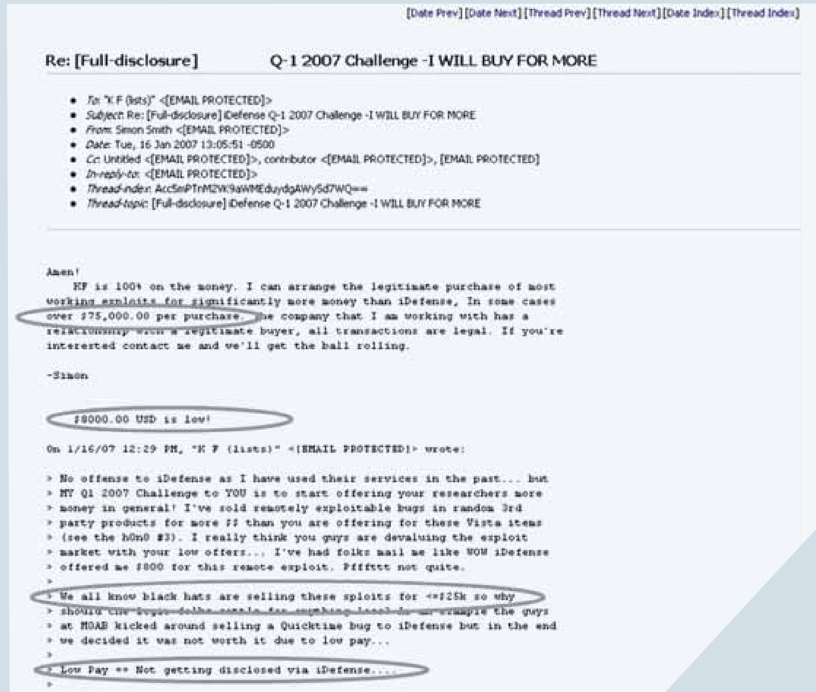
Il mercato nero dei dati rubati (per esempio carte di credito, email, account di Skype, etc.) è oggi ben sviluppato e il costo per ottenere dettagli delle carte di credito potrebbe andare da 0,5 a 5 dollari o più. Però è un altro il mercato nero che sta allarmando i governi e le risorse mondiali: quello degli exploit zero-day.

Gli exploit zero-day: Codice informatico che strumentalizza una vulnerabilità per cui non è ancora disponibile un rimedio (patch).

Gli exploit sono un'arma che può essere utilizzata per danneggiare aziende, concorrenti o governi. Aprono delle 'back door' nei programmi, consentendo il furto di dati personali come i dettagli di conti bancari, e possono anche infliggere danni significativi all'infrastruttura di una nazione o essere utilizzati per attività di spionaggio cibernetico. "Non c'è nessuna magia nello spionaggio informatico online, tutto quello che c'è da fare è sfruttare qualche falla o una vulnerabilità," ha affermato Shawn Carpenter, principal forensic analyst presso Netwitness. Queste vulnerabilità possono anche essere utilizzate per ricattare il fornitore del software colpito.

Nel Gennaio 2006, un exploit Microsoft WMF è stato venduto in un'asta online per 4.000 dollari e si ritiene sia stata venduta a più di un acquirente 'black hat' (una persona che compromette la sicurezza di un computer senza il permesso di una parte autorizzata, tipicamente a fine doloso). Indagini hanno dimostrato che l'exploit è stato poi utilizzato almeno da uno degli acquirenti per prendere il controllo di Pc per diffondere spam di tipo 'pump and dump' (campagne email create per gonfiare i prezzi delle azioni tramite false informazioni).

Ci sono anche elementi che suggeriscono che 4.000 dollari sia un prezzo piuttosto basso che "svaluta il mercato". L'email sopra illustrata [I will buy for more] implica che gli exploit possono raggiungere anche i 75.000 dollari.


[Date Prev] [Date Next] [Thread Prev] [Thread Next] [Date Index] [Thread Index]

Re: [Full-disclosure] Q-1 2007 Challenge -I WILL BUY FOR MORE

- *To*: "K F (lists)" <>
- *Subject*: Re: [Full-disclosure] iDefense Q-1 2007 Challenge -I WILL BUY FOR MORE
- *From*: Simon Smith <>
- *Date*: Tue, 16 Jan 2007 13:05:51 -0500
- *Cc*: Untitled <>, contributor <>,
- *In-reply-to*: <>
- *Thread-index*: Acc5nPTnM2W9aWMEduydgAWy5d7WQ==
- *Thread-topic*: [Full-disclosure] iDefense Q-1 2007 Challenge -I WILL BUY FOR MORE

Amen!
KF is 100% on the money. I can arrange the legitimate purchase of most working exploits for significantly more money than iDefense, In some cases over $75,000.00 per purchase. The company that I am working with has a relationship with a legitimate buyer, all transactions are legal. If you're interested contact me and we'll get the ball rolling.

-Simon

$8000.00 USD is low!

On 1/16/07 12:29 PM, "K F (lists)" <> wrote:

> No offense to iDefense as I have used their services in the past... but
> MY Q1 2007 Challenge to YOU is to start offering your researchers more
> money in general! I've sold remotely exploitable bugs in random 3rd
> party products for more $$ than you are offering for these Vista items
> (see the h0n0 #3). I really think you guys are devaluing the exploit
> market with your low offers... I've had folks mail me like WOW iDefense
> offered me $800 for this remote exploit. Pffttt not quite.
>
> We all know black hats are selling these sploits for <=$25k so why
> should the [illegible] the guys
> at MOAB kicked around selling a Quicktime bug to iDefense but in the end
> we decided it was not worth it due to low pay...
>
> Low Pay == Not getting disclosed via iDefense....
>

QUESTO MERCATO POTRÀ MAI ESSERE LEGALE?

Molte persone potrebbero essere scioccate dall'apprendere che esiste un 'mercato bianco' legale di compravendita di queste vulnerabilità zero-day. Utilizzando contratti e accordi di non divulgazione con organizzazioni legittime, le aziende acquistano apertamente queste imperfezioni software. Tra gli esempi ci sono Tipping Point (di proprietà di 3Com) e iDefense (di proprietà di Verisign). Inoltre i governi impiegano attivamente esperti per dare la caccia a eventuali imperfezioni o falle.

LA VENDITA DI TALI EXPLOIT DOVREBBE ESSERE ILLEGALE?

Gli esperti di sicurezza e gli economisti non concordano sul fatto di rendere legale il 'mercato bianco'. C'è una scuola di pensiero che ritiene che individuare un exploit è un lavoro duro e che i ricercatori dovrebbero essere pagati per farlo, dal momento che la loro attività è per il bene pubblico. Dall'altra parte, gli autori di software affermano che un bug nel loro software non è qualcosa rivendibile a loro stessi, o peggio ancora, a qualcun altro.

Mentre gli esperti concordano sul fatto che le vulnerabilità devono essere scoperte, molti si sentono ancora a disagio relativamente a questo concetto di 'mercato bianco'. Entrambi i principali protagonisti summenzionati sul mercato bianco sono impegnati in una politica di 'divulgazione responsabile, ovvero rendere pubblica la vulnerabilità al vendor di software dopo che l'hanno comunicata ai loro clienti. La vulnerabilità è così già stata risolta o è stata resa disponibile una patch. Comunque, esiste inevitabilmente un intervallo temporale tra il momento in cui viene individuata una vulnerabilità e quando il vendor rende disponibile una patch.

Le prove suggeriscono che dove esiste un 'mercato bianco', c'è sempre il pericolo che gli exploit possano cadere in mani sbagliate. Gli Stati Uniti, per evitare che ciò accada, sta cercando di far approvare una legge per bloccare la vendita di 3Com, proprietaria di Tipping Point, a una grande azienda cinese legata al governo.

In qualità di membro e collaboratore dell'OIS (Organisation for Internet Safety), McAfee ritiene che l'esistenza di un 'mercato bianco' legale non sia nel pubblico interesse e sostiene la divulgazione etica.

"Riteniamo che l'unico modo per proteggere le reti sia divulgare esclusivamente in base all'etica invece che per ottenere notorietà o compensi economici," ha affermato David Coffey, Director of Product Security di McAfee. "Più il mercato degli exploit diventa efficiente, maggiore sarà il potenziale di guadagno per i criminali informatici. L'unica preoccupazione dovrebbe essere quella di assicurare che I vendor siano avvisati della necessità di applicare una patch e che in definitiva tutti siano protetti dal rischio di un attacco. "

Sfortunatamente, esisterà sempre un mercato nero per gli exploit, ma se si acconsente a un 'mercato bianco' è possibile si aumenti il pericolo che le vulnerabilità vadano a finire nelle mani sbagliate.

L'opinione è che nei prossimi anni, i governi perseguiranno con azioni punitive individui e aziende specifiche che perpetrano attacchi contro le nazioni. Diventeranno aggressivi e li inseguiranno, indipendentemente da dove si trovano.

IN QUESTO CAPITOLO:

- Molte nazioni diventano conosciute solo per essere dei rifugi per i cybercriminali
- Vedremo la prima azione internazionale contro le nazioni che ospitano i cybercriminali
- I governi puniranno gli individui e le organizzazioni che attaccano le nazioni, inidpendentemente da dove saranno ubicati
- L'azione porterà un cambiamento dinamico del panorama

DOPO AVER ANALIZZATO L'EVOLUZIONE E LO SVILUPPO ATTUALE DEL CYBERCRIME, MCAFEE E GLI ESPERTI DEL CENTRE FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY (CERIAS) NEGLI STATI UNITI RITENGONO CHE I SEGUENTI TREND INIZIERANNO A MANIFESTARSI NEI PROSSIMI ANNI.

AUMENTANO I RIFUGI SICURI PER I CRIMINALI INFORMATICI: LA NECESSITÀ DI UN ACCORDO INTERNAZIONALE

L'inevitabile realtà è che alcune nazioni si affermeranno come rifugi sicuri per i criminali informatici e la pressione internazionale per l'adozione di provvedimenti severi non funzionerà molto in quelle nazioni dove il governo ha dei ritorni economici o un piano politico che li incoraggia. La prima azione internazionale in quest'ambito sarà intrapresa entro i prossimi cinque anni. "Non credo che i criminali informatici abbiano ancora una reale paura delle forze dell'ordine," ha affermato Sharon Lemon, SOCA (Serious Organised Crime Agency), Regno Unito.

> "Ora gli unici criminali informatici online che sono veramente spaventati sono i pedofili, perché sono state intraprese azioni di vasta portata contro di loro negli ultimi anni, e ora si rendono conto che non possono pensare di inserire i dettagli della loro carta di credito online senza essere catturati. Il nostro compito è quello di creare un clima di paura simile per altri tipi di crimini informatici."
>
> ha affermato Sharon Lemon, SOCA (Serious Organised Crime Agency), Regno Unito.

La buona notizia è che alcune nazioni, fonti conosciute di malware, stanno già agendo per cambiare la situazione. La Russia, per esempio, ha appena formato un'unità per il crimine online. Nel presidiare il cyberspazio, l'Occidente si rende conto che essere internazionali è un requisito piuttosto che una possibilità.

La collaborazione internazionale a questo livello, comunque, non accadrà da un giorno all'altro. Nonostante la Cybercrime Convention e le iniziative della Comunità Europea sugli attacchi informatici, la collaborazione globale per combattere il crimine informatico è ancora difficile e costosa. La NATO e il Comando della Forza Aerea degli Stati Uniti sono stati specificamente coinvolti per supervisionare le minacce contro le nazioni, ma la diffusione del cybercrime deve ottenere una maggior attenzione a livello internazionale.

Sfortunatamente, qualcuno pensa che il cybercrime si radicherà profondamente nella società e prospererà oltre un "rischio gestibile" prima di essere affrontato su larga scala. Quando ciò accadrà, proprio come con la droga e le scommesse, riceverà le risorse e l'attenzione necessarie per iniziare ad affrontarlo in modo appropriato su scala nazionale e mondiale.

L'opinione è che nei prossimi anni, i governi perseguiranno con azioni punitive individui e aziende specifiche che perpetrano attacchi contro le nazioni. Diventeranno aggressivi e li inseguiranno, indipendentemente da dove si trovano.

Quando ciò accadrà, allora si verificherà un drammatico cambiamento della situazione. I criminali informatici non intraprenderanno più azioni criminose utilizzando Internet in certe aree perché presenteranno un rischio maggiore, anche per la loro incolumità personale.

SOLUZIONI LEGALI PER MITIGARE IL PERICOLO CIBERNETICO

I governi faranno pressione sugli enti intermediatori che dispongono delle competenze e delle risorse, come banche, Internet Service Provider e fornitori di software, per proteggere il pubblico dal malware, dagli hacker e dal social engineering. La Federal Trade Commission negli Stati Uniti ne ha già richiesto l'intervento. Probabilmente l'industria opporrà resistenza a queste mosse e i governi dovranno bilanciare l'impatto economico sui settori industriali con le preoccupazioni pubbliche per la sicurezza informatica. Il risultato più probabile sarà una crescita di 'leggi lievi' – codici procedurali per settori industriali che richiedono maggiori misure di sicurezza, forse supportati da marchi di conformità alle norme, garanzie e assicurazioni.

MODIFICARE IL MODO IN CUI CONSIDERIAMO LA SICUREZZA

Assisteremo inoltre a una maggiore connettività, ci saranno più sistemi integrati e i perimetri si faranno meno definiti. Perciò sarà necessario un cambiamento nel modo in cui pensiamo alla sicurezza, ma questo cambiamento sarà lento a venire.

Le regole e le leggi per la conformità porteranno alcuni miglioramenti e cambiamenti significati, ma non tutti saranno appropriati dal momento che la tecnologia evolve. Alcuni requisiti di conformità possono realmente rendere le aziende vulnerabili agli attacchi. In relazione alla conformità, l'applicazione di diritti esterni (per esempio il copyright che utilizza il DRM-Digital Rights Management) porterà a una maggiore complessità nei sistemi e a un numero superiore di dispute legali.

Inizieranno a essere intraprese cause civili individuali per violazioni alla sicurezza, sebbene la loro crescita in Europa probabilmente sarà più lenta per una diversa cultura nei confronti delalle azioni collettive rispetto agli Stati Uniti. Gli standard di sicurezza per una cura ragionevole per l'industria dovranno essere molto più definiti, dal momento che gli enti di vigilanza sono sempre più interessati alla sicurezza delle aziende e dei singoli.

Infine, c'è una crescente consapevolezza del fatto che enormi raccolte di dati, mirroring, RAID, backup, etc. fanno sì che i dati non siano mai definitivamente eliminati. Ciò sarà un vantaggio per alcune attività delle forze dell'ordine, ma sarà anche un onere a carico delle aziende durante le cause legali civili e una costante minaccia per la privacy individuale.

HANNO COLLABORATO:

EMEA:

DR. IAN BROWN – RICERCATORE PRESSO L'OXFORD INTERNET INSTITUTE, UNIVERSITÀ DI OXFORD

Il dottor Ian Brown è un ricercatore dell'Oxford Internet Institute, Università di Oxford, e lettore universitario onorario anziano presso l'University College London. Il suo lavoro è focalizzato sulle problematiche delle policy pubbliche relativamente a informazioni e Internet, in particolare sulle tematiche legate a privacy, copyright e e-democracy. Lavora anche in campi più tecnici come sicurezza informatica, networking e informatica per la sanità.

E' membro della Royal Society of Arts e del British Computer Society, è un consulente di Privacy International, Open Rights Group, Foundation for Information Policy Research e Greenpeace. Ha fornito consulenza per il governo degli Stati Uniti, JP Morgan, Credit Suisse, la Commissione Europea e UK Information Commissioner's Office.

Nel 2004 è stato incluso tra i 100 personaggi più influenti nello sviluppo di Internet nel Regno Unito nel decennio precedente.

LILIAN EDWARDS – INSTITUTE FOR LAW AND THE WEB (ILAWS), UNIVERSITÀ DI SOUTHAMPTON

Lilian Edwards è Professore di Legislazione di Internet a Southampton, e Direttore dell'ILAWS. I suoi interessi di ricercatrice sono generalmente nel campo della giurisprudenza relativamente a Internet, il Web e le nuove tecnologie, con una focalizzazione Europea e comparativa. Le sue attività di ricerca sono attualmente concentrate sui contenuti Internet (pornografia, diffamazione, spam, etc.); responsabilità legale di intermediari/ ISP su Internet; giurisdizione in Internet; privacy e protezione dei dati on-line; cybercrime e sicurezza informatica e protezione dei consumatori on line. Ha pubblicato due famose collezioni su Law and the Internet e una terza collezione di saggi The New Legal Framework for E-Commerce in Europe. Il suo lavoro sulla privacy on-line dei consumatori si è aggiudicato il Barbara Wellbery Memorial Prize nel 2004 quale miglior soluzione al problema della privacy e flussi di dati in tutto il mondo.

E' consulente di BILETA, EURIM, Creative Commons Scotland e dell'Online Rights Group e ha fornito consulenze per la Commissione Europea.

SHARON LEMON – RESPONSABILE DELL'E-CRIME, SERIOUS ORGANISED CRIME AGENCY (SOCA)

Il Serious Organised Crime Agency (SOCA) è un Ente Pubblico Esecutivo Non Dipartimentale sponsorizzato dal Ministero dell'Interno, ma da questi operativamente indipendente.

Il Soprintendente Investigatore Sharon Lemon è a Capo dell'E-Crime del SOCA.

BOB BURLS MSC – DETECTIVE CAPO METROPOLITAN POLICE COMPUTER CRIME UNIT

L'Unità Crimini Informatici è un centro di eccellenza relativamente a crimini informatici perpetrati in base al Computer Misuse Act 1990, ovvero hacking, virus creati e diffusi a fini dolosi e software contraffatto. L'unità offre un ufficiale di servizio dedicato alla computer forensic e fornisce consulenza per il recupero di prove dai computer agli agenti. Biografia personale non disponibile.

YAEL SHAHAR - DIRECTOR, DATABASE PROJECT INSTITUTE FOR COUNTER-TERRORISM, IDC HERZLIYA

Yael Shahar è a capo del progetto OSING e database dell'ICT. Ha creato il database di collegamenti tra terroristi e il database degli incidenti di terrorismo dell'ICT, utilizzati per tracciare i collegamenti tra terroristi singoli, aziende di facciata e organizzazioni.

Shahar è specializzata nello studio dei trend tecnologici applicati al terrorismo e nella condivisione delle informazioni di intelligence. Tiene conferenze sulle tendenze del terrorismo, terrorismo non convenzionale e valutazione delle minacce presso l'International Policy Institute for Counter Terrorism, Interdisciplinary Center Herzliya, oltre a conferenze e seminari sulla sicurezza in tutto il mondo.

La principale responsabilità di Yael Shahar è quella di condurre attività di datamining open-source a supporto dei progetti di ricerca dell'ICT, oltre a valutazioni di minacce in base al luogo per i clienti commerciali dell'ICT.

Ha studiato fisica, progettazione di database, sicurezza e protezione delle installazioni. E' stata riservista dell'unità di recupero ostaggi IDF, e franco tiratore delle unità "Matmid" della Guardia di Frontiera di Israele.

HANNO COLLABORATO:

PETER SOMMER – SENIOR RESEARCH FELLOW DELL'INFORMATION SYSTEMS INTEGRITY GROUP DELLA LONDON SCHOOL OF ECONOMICS.

La principale attività di ricerca di Peter Sommer è nell'ambito dell'affidabilità delle prove digitali, una materia che include l'elaborazione forense e l'e-commerce. Ha contribuito a sviluppare i corsi orientati alle scienze sociali sulla gestione della sicurezza delle informazioni dell'LSE. Nell'ultima legislazione ha ricoperto il ruolo di Specialist Advisor per l'House of Commons Trade e l'Industry Select Committee del Regno Unito durante un'indagine sulle politiche e la legislazione per l'e-commerce nel Regno Unito. Ha fatto parte del Foresight Study, Cyber Trust, Cybercrime dell'Office of Science Technology del Regno Unito. Fa parte di vari Pannelli di Consulenza per il Governo del Regno Unito. Sono stati condotti recenti contratti di ricerca per la Financial Services Authority del Regno Unito e il Safer Internet Action Plan della Comunità Europea. Attualmente fa parte dell'European FIDIS Network of Excellence ed è inoltre membro del Reference Group (meccanismo di revisione) di PRIME, un'altra iniziativa della Commissione Europea.

E' un esaminatore esterno del Royal Military College of Science e consulente di varie forze dell'ordine e altri comitati legati al crimine informatico e alle azioni d'emergenza. Ha fornito consulenza al Centrex, che fornisce formazioni sul crimine tecnologico alle forze dell'ordine del Regno Unito, e a TWED-DE, un'iniziativa finanziata dal Dipartimento di Giustizia statunitense per sviluppare formazione sulle prove digitali. Ha inoltre partecipato come speaker a seminari delle forze di polizia del Regno Unito e degli Stati Uniti sui temi delle prove digitali e intelligence.

Ha fatto parte del comitato programmatico per FIRST 2000 a Chicago.

Peter Sommer è consulente e perito di grandi compagnie di assicurazione di sistemi di elaborazione complessi. Il suo primo incarico come testimone esperto è stato nel 1985 e l'assistenza da lui fornita include il caso relativo all'attacco ai sistemi internazionali di Datastream Cowboy / Rome Labs, la causa di diffamazione Demon contro Godfrey Internet, NCS Operation Cathedral, Operation Ore e molti altri casi relativi a diversi crimini come omicidi multipli, contraffazione, piracy del software, frodi bancarie, clonazione di carte di credito e la vendita di Segreti Ufficiali.

Fa parte dell'Advisory Council della Foundation for Information Policy Research, un centro di ricerca con sede nel Regno Unito.

RICHARD CLAYTON – CAMBRIDGE UNIVERSITY COMPUTER LABORATORY

Il Computer Laboratory di Cambridge è il dipartimento di informatica dell'Università di Cambridge. Il Diploma in Informatica di Cambridge è stato il primo corso di informatica al mondo, ed è iniziato nel 1953.

Richard Clayton è un affermato ricercatore di sicurezza e un collaboratore di lunga data dei gruppi operativi per le politiche di sicurezza del Regno Unito.

STATI UNITI:

EUGENE H SPAFFORD – PROFESSORE DI INFORMATICA, PURDUE UNIVERSITY E EXECUTIVE DIRECTOR DEL CENTRE FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY (CERIAS)

Eugene H. Spafford è uno dei più esperti e riconosciuti leader nel campo dell'informatica. Vanta una costante serie di successi come senior advisor e consulente su problematiche relative a sicurezza, istruzione, crimine informatico e policy informatiche per varie aziende di primaria importanza, forze di polizia, agenzie accademiche e governative, tra cui Microsoft, Intel, Unisys, le Forze Aeree Statunitensi, la National Security Agency, il GAO, l'FBI, la National Science Foundation, il Dipartimento dell'Energia e due Presidenti degli Stati Uniti.

Con circa tre decadi di esperienza come ricercatore e istruttore, il Professor Spafford ha lavorato nel campo dell'ingeneria software, elaborazione distribuita affidabile, sicurezza di sistemi e rete, forensica digitale, policy informatiche e progettazione del programma di studi in informatica. E' responsabile di vari "firsts" in molte di queste aree.

ANDREA M. MATWYSHYN – PROFESSORE UNIVERSITARIO DI STUDI LEGALI E ETICA AZIENDALE, WHARTON, UNIVERSITÀ DELLA PENNSYLVANIA

Andrea M. Matwyshyn professore universitario di Studi legali e Etica Aziendale presso la Wharton School dell'Università della Pennsylvaniaan e affiliato del Centre for Economics & Policy dell'Università di Cambridge.

L'interesse primario delle attività di ricerca e consulenza di Andrea è nell'area della sicurezza delle informazioni aziendali e legislazione e policy in mabito tecnologico. Prima di intraprendere l'insegnamento, ha fatto pratica come procuratore aziendale focalizzata sulle transazioni tecnologiche.

FRED DOYLE - CISSP/GCIH/GREM, DIRECTOR, IDEFENSE RESEARCH LAB, IDEFENSE VERISIGN.

iDefense Labs in provides comprehensive, actionable intelligence regarding cyber security threats and vulnerabilities to the largest financial services firms, government agencies, retailers and other large enterprises. Its multi-lingual network of hundreds of research contributors in over 30 countries offers early and unique insight into the cyber underground and previously unknown software vulnerabilities. This insight provides our customers with intelligence to aid them in making decisions in response to threats on a real-time basis.

HANNO COLLABORATO:

SUD AMERICA:

RENATO OPICE BLUM AND RUBIA MARIA FERRÃO - OPICE BLUM ADVOGADOS ASSOCIADOS

Opice Blum Advogados Associados vanta anni di solida esperienza nelle varie aree della legislazione, in particolare nell'ambito della tecnologia, legislazione elettronica, informatica e sue varianti. Pioniere in queste materie, opera anche in mediazioni, arbitraggi, deposizioni verbali in tribunale, legislazione biologica, tipici contratti tecnologici, crimini informatici, etc. Agisce sul territorio brasiliano e ha corrispondenti internazionali nei principali centri finanziari, come Miami e New York.

In qualità di membro di organizzazione istituzionali, contribuisce all'evoluzione della legge legata allo sviluppo tecnologico. Si distingue come partner fondatore della Brazilian Chamber of Electronic Commerce ed è membro della Computation Brazilian Society, tra le altre istituzioni. Biografie personali non disponibili.

ASIA PACIFICO:

GRAEME EDWARDS - DETECTIVE SENIOR CONSTABLE, COMPUTER CRIME INVESTIGATION UNIT, QUEENSLAND POLICE SERVICE

Il CCIU (Computer Crime Investigation Unit) all'interno del Major Fraud Investigation Group (MFIG) è stato creato nel 2000 e è responsabile delle indagini su tutti i crimini in ambito informatico, infrazioni legate alle frodi commesse contro commercianti online, e-commerce o utenti Internet. L'unità inoltre valuta e fornisce consulenza e assistenza su problematiche che coinvolgono intrusioni da parte di hacker, denial of service o frodi su Internet. Il CCIU attualmente conta su uno staff di cinque ufficiali di polizia e un ufficiale amministrativo. Biografia personale non disponibile.

DAVID VAILE – EXECUTIVE DIRECTOR, CYBER LAW AND POLICY CENTRE, UNIVERSITÀ DELLO STATO DEL NEW SOUTH WALES

David Vaile è diventato il primo direttore esecutivo del Cyberspace Law and Policy Centre nel 2002. Coordina il supporto per i progetti di ricerca ARC del centro come Unlocking IP, Interpreting Privacy Principles e Regulating Online Investing, e insegna Cyberspace Law e Law in the Information Age. La sua formazione in legge, IT e comunicazione include ricerca legale (Legal Aid NSW), protezione dei dati (Privacy Commissioner's Office), difesa pro bono, interesse pubblico e vertenze processuali (Public Interest Advocacy Centre), una comunità virtuale per difensori (con la Law Foundation dell'NSW), governance organizzativa, sviluppo di database e istruzione professionale online.

I suoi interessi nell'ambito della ricerca sulle leggi e policy per il cyberspazio includono privacy e protezione dei dati, sicurezza IT, giurisdizione online, copyright e proprietà intellettuale digitale, salute online, risk management e progettazione focalizzata sugli utenti. E' anche membro dell'Information Security World Advisory Board e del consiglio dell'Australian Privacy Foundation.

GIAPPONE:

PROFESSOR KEIJI TAKEDA – CARNEGIE MELLON CYLAB JAPAN

Il Professor Takeda ha lavorato per l'Agenzia della Difesa del Giappone, la Japan Air Self Defence Force e Accenture. Attualmente ha una cattedra al Carnegie Mellon CyLab Japan e una cattedra aggiunta al Carnegie Mellon Information Network Institute. Ha condotto attività di Ricerca & Sviluppo, direzione, istruzione e consulenza nell'area della sicurezza informatica. Ha conseguito un Dottorato di Ricerca in Media e Governance presso la Keio University.

REFERENZE

[i] http://www.timesonline.co.uk/tol/news/world/asia/article2388375.ece

[ii] http://www.guardian.co.uk/china/story/0,,2162161,00.html

[iii] http://news.zdnet.co.uk/security/0,1000000189,39290289,00.htm

[iv] http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_2.html

[v] http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece

[vi] http://security4all.blogspot.com/2007/10/chinese-hit-india-3-4-times-day.html

[vii] http://www.cnn.com/2007/US/10/19/cyber.threats/

[viii] http://www.csmonitor.com/2007/0914/p01s01-woap.html

[ix] http://www.csmonitor.com/2007/0914/p01s01-woap.htm

[x] http://seattletimes.nwsource.com/html/nationworld/2003886833_chinahack16.html

[xi] http://news.bbc.co.uk/1/hi/technology/7070815.stm

[xii] http://www.finextra.com/fullstory.asp?id=16204

[xiii] http://www.ponemon.org/

[xiv] http://www.spaminspector.org/Internet-Fraud/SouthAfricaInternetBankingFraud_12817.html

[xv] http://news.bbc.co.uk/2/hi/technology/6976308.stm