

CRYPTO-GRAM
15 ottobre 2007

Scritta da Bruce Schneier
Edizione italiana curata da Communication Valley SpA

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0710.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

** ** ** ** **

In questo numero:

- Il worm Storm
- "Amber Alert" fraudolenti
- La polizia britannica ora può richiedere le chiavi crittografiche
- News
- L'anonimato e la rete Tor
- Giocattoli telecomandati e la TSA
- Le news su Schneier/BT Counterpane
- Un attacco simulato causa l'autodistruzione di un generatore
- Commenti dei lettori

** ** ** ** **

Il worm Storm

Il worm Storm è apparso per la prima volta all'inizio dell'anno, nascosto in allegati di email dal titolo "230 dead as storm batters Europe" [La tempesta colpisce ripetutamente l'Europa, provocando 230 morti]. I computer di coloro che aprivano l'allegato diventavano infetti, e si univano a un botnet in crescita continua.

Pur essendo più comunemente identificato come un worm, in realtà Storm è molto di più: è un worm, un Cavallo di Troia e un bot, riuniti in un'unica entità. È anche l'esempio più riuscito di una nuova specie di worm, e ho visto stime secondo le quali in tutto il mondo sono già stati infettati da 1 milione a 50 milioni di computer.

Worm vecchio stile, come Sasser, Slammer e Nimda, erano realizzati da hacker che cercavano la gloria. Venivano diffusi il più rapidamente possibile (Slammer infettò 75.000 computer in 10 minuti) e per questo acquisirono molta notorietà. Grazie a una tale offensiva, gli esperti di

sicurezza poterono facilmente individuare l'attacco, ma fu necessaria una pronta risposta da parte delle compagnie antivirus, degli amministratori di sistema e degli utenti nella speranza di contenere l'attacco. Si pensi a questo tipo di worm come a una malattia infettiva che manifesta sintomi immediati.

Worm come Storm sono scritti da hacker che cercano di trarne profitto, e sono molto diversi. Si diffondono in maniera più subdola, senza fare rumore. I sintomi non appaiono immediatamente, e un computer infetto può starsene tranquillo per molto tempo. Se fosse una malattia, sarebbe più simile alla sifilide, i cui sintomi possono essere molto lievi o del tutto assenti, ma alla fine si ripresenta a distanza di anni e attacca il cervello.

Storm rappresenta il futuro del malware. Analizziamone il comportamento:

1. Storm è paziente. Un worm che attacca continuamente è molto più semplice da rilevare; un worm che attacca e poi si disattiva per un certo tempo può nascondersi con più facilità.
2. Storm è progettato come una colonia di formiche, ossia presenta una suddivisione dei compiti. Solo una piccola frazione degli host infettati diffonde il worm. Un insieme ancor più piccolo è rappresentato da macchine C2: server di controllo (command and control). Il resto delle macchine rimane in attesa di ordini. Dato che permette soltanto a una piccola percentuale di host di propagare il virus e di agire come server di controllo, Storm è piuttosto resistente agli attacchi. Anche se quegli host vengono scollegati, la rete rimane in gran parte intatta, e altri host possono subentrare, incaricandosi di tali compiti.
3. Storm non provoca danni agli host, né causa rallentamenti o cali prestazionali visibili. Come un parassita, Storm per sopravvivere necessita un ospite intatto e sano. Questo ne rende il rilevamento ancor più difficile, perché la maggior parte del tempo utenti e amministratori di rete non noteranno alcun comportamento anomalo.
4. Invece di far comunicare tutti gli host con un server centrale o con un gruppo di server, Storm utilizza una rete peer-to-peer per il C2. Ciò rende il botnet di Storm molto più arduo da disattivare. Il metodo più comune per disattivare un botnet è chiudere il punto di controllo centralizzato. Ma Storm non presenta tale punto di controllo centralizzato, pertanto non è possibile disabilitarlo in questo modo.

Questa tecnica possiede altri vantaggi. Le aziende che monitorano l'attività di rete possono rilevare anomalie nel traffico stesso in presenza di un punto C2 centralizzato, ma un C2 distribuito non appare come un picco, e le comunicazioni non sono facilmente individuabili.

Un metodo standard per rintracciare server C2 di root è far passare un host infetto attraverso un debugger di memoria e analizzare da dove arrivano gli ordini per quella macchina. Ciò non funzionerà con Storm: un host infetto potrebbe soltanto essere a conoscenza di un numero molto piccolo di altri host infettati (25-30 per volta), e tali host distano dai server C2 primari un numero di hop sconosciuto.

E anche se un nodo C2 venisse disattivato, il sistema non ne soffrirebbe più di tanto. Come una idra dalle molte teste, la struttura C2 di Storm è distribuita.

5. Non soltanto i server C2 sono distribuiti, ma si nascondono persino dietro una tecnica di cambiamento costante dei DNS chiamata "fast flux". Per cui, anche se un host compromesso viene isolato e sottoposto a debugging, e un server C2 viene identificato attraverso la nuvola (cloud), esso potrebbe essersi già reso inattivo.

6. Il payload di Storm (ossia il codice che utilizza per diffondersi) si modifica all'incirca ogni 30 minuti, riducendo l'efficacia delle classiche tecniche AV (antivirus) e IDS.

7. Anche il meccanismo di distribuzione di Storm cambia regolarmente. Storm ha cominciato a propagarsi sotto forma di spam PDF, poi gli autori hanno cominciato a servirsi di e-card e di inviti YouTube: qualsiasi mezzo per spingere gli utenti a fare clic su un link fasullo e malevolo. Storm ha prodotto anche commenti di spam nei blog, sempre con l'obiettivo di ingannare i visitatori e invitarli a fare clic su collegamenti infetti. Questi tipi di tattiche di diffusione di un worm sono piuttosto comuni, ma occorre sottolineare come Storm sia in continua metamorfosi a ogni livello.

8. Anche le email prodotte da Storm mutano continuamente, facendo leva su tecniche di ingegneria sociale. L'oggetto delle email è sempre diverso, così come il corpo del testo, tutto per attirare attenzione: "Killer a undici anni, esce di prigione a 21 e...", "Programma di tracciamento di football americano" inviato nel finesettimana di inizio campionato della NFL, nonché avvisi di tempeste e uragani imminenti. I programmatori di Storm sono molto bravi a far leva sulla natura umana.

9. Il mese scorso Storm ha cominciato ad attaccare siti anti-spam dedicati alla sua identificazione (spamhaus.org, 419eater e altri) e il sito personale di Joe Stewart, che ha pubblicato un'analisi di Storm. Ciò mi ricorda una teoria di base della guerra: fate fuori la ricognizione del nemico. O anche una teoria di base delle bande di quartiere e di alcuni governi: fate in modo che gli altri sappiano che è meglio non ostacolarvi.

Il fatto è che neanche sappiamo come ostacolare Storm. Storm è in circolazione da quasi un anno, e le compagnie antivirus non sono praticamente in grado di fare nulla per fermarlo. Inoculare le macchine infettate una a una non porta da nessuna parte, ed è improponibile obbligare gli Internet Provider a mettere in quarantena gli host infetti. Una quarantena non funzionerebbe comunque: i creatori di Storm potrebbero facilmente progettare un altro worm, e sappiamo che gli utenti non riescono a trattenersi dal fare clic su allegati e link invitanti.

Ridisegnare completamente il sistema operativo di Microsoft potrebbe funzionare, ma è una cosa talmente irrealizzabile che è ridicolo perfino suggerirla. Creare un worm benigno anti-Storm sarebbe una trama fantastica per un libro o un film, ma è una pessima idea nel mondo reale. Molto semplicemente, non sappiamo come fermare Storm, se non trovando le persone che lo controllano e arrestandole.

Purtroppo non abbiamo la più pallida idea di chi siano queste persone, anche se si ipotizza si tratti di russi. I programmatori sono ovviamente molto intelligenti e dotati, e stanno continuando a lavorare alla loro creazione.

Stranamente al momento Storm non sta facendo granché, a parte irrobustirsi sempre più. Oltre a continuare a infettare nuove macchine Windows e a prendere di mira certi siti che lo stanno attaccando, Storm è rimasto implicato solo in alcune truffe azionare pump and dump. Voci di corridoio affermano che Storm venga affittato ad altri gruppi criminali. A parte questo, nulla.

Personalmente mi preoccupa ciò che i creatori di Storm stanno pianificando per la Fase 2.

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/10/securitymatters_1004>

oppure <<http://tinyurl.com/2xevsm>>

<<http://www.informationweek.com/news/showArticle.jhtml?articleID=201804528>>

Ritengo che questa sia soltanto un'altra schermaglia della "guerra alla crittografia" che continua da quindici anni (qualcuno si ricorda del chip Clipper?). La polizia ha da sempre sostenuto che la crittografia è un ostacolo insormontabile per il corso della giustizia:

"Il Ministero dell'Interno ha fermamente dichiarato che la legge ha come obiettivo la cattura di terroristi, pedofili e criminali incalliti, tutte categorie che il governo britannico sostiene siano esperte nell'utilizzo della crittografia per occultare le proprie attività".

Tutte cose che abbiamo già sentito dire nel 1993 dal Direttore dell'FBI Louis Freeh. Li ho definiti 'I Quattro Cavalieri dell'Apocalisse dell'Informazione': terroristi, spacciatori di droga, sequestratori e pedopornografi, e sono stati utilizzati per giustificare ogni nuovo potere assegnato alle forze dell'ordine.

<<http://arstechnica.com/news.ars/post/20071001-uk-can-now-demand-data-decryption-on-penalty-of-jail-time.html>>

oppure <<http://tinyurl.com/3btatf>>

<<http://ct.techrepublic.com.com/clicks?t=40345835-0f1945960a0400a9a01bdf730f084221-bf&s=5&fs=0>>

oppure <<http://tinyurl.com/2o9545>>

<http://www.theregister.co.uk/2007/10/03/ripa-decryption_keys_power/>

** ** ** * * * * *

News

Microsoft aggiorna sia XP sia Vista senza avvertire né chiedere il permesso all'utente. Microsoft lo può fare: è semplicemente l'ennesima di tante stupidaggini dell'azienda. Nulla però impedisce a chiunque altro di sfruttare questa possibilità di installazione remota e nascosta di Microsoft per installare qualsiasi cosa sul computer altrui. Quanto tempo passerà prima che qualche hacker brillante sfrutti tale funzione per poi scrivere un programma che permetterà a tutti gli hacker idioti di fare altrettanto? Quando si inserisce una funzionalità come questa in un sistema se ne riduce la sicurezza generale.

<<http://www.informationweek.com/news/showArticle.jhtml?articleID=201806263>>

oppure <<http://tinyurl.com/ytzz7l>>

<<http://blogs.zdnet.com/hardware/?p=779>>

Un altro scandalo di spionaggio nello sport, stavolta nella Formula 1:

<<http://www.iht.com/articles/2007/09/13/sports/prix.php>>

<http://today.reuters.co.uk/news/newsArticle.aspx?type=motoringMotorSportsNews&storyID=2007-09-14T141001Z_01_L14841488_RTRIDST_0_MOTOR-RACING-PRIX-MCLAREN-EVIDENCE-UPDATE-1.XML>

oppure <<http://tinyurl.com/3xb7l7>>

<<http://sport.guardian.co.uk/motorsport/story/0,,2168805,00.html>>

Il Ministero dei Trasporti norvegese ha richiesto all'Unione Europea di eliminare il divieto dei liquidi sugli aerei.

<<http://nyheter.vg.no/nyheter/artikkel.php?artid=162926>>

<<http://www.aftenposten.no/reise/article1994056.ece>>

E il Parlamento Europeo si è detto d'accordo.

<http://www.europarl.europa.eu/news/expert/infopress_page/062-10003-246-09-36-910-20070823IPR09766-03-09-2007-2007-false/default_en.htm>

oppure <<http://tinyurl.com/37x6yt>>

Purtroppo il Parlamento Europeo non ha potere; le sue decisioni vengono costantemente ignorate. In questo caso è la Commissione Europea ad avere il vero potere decisionale.

MediaDefender è un'azienda di P2P poisoning. La scorsa settimana, la corrispondenza elettronica, le chiamate telefoniche e il codice sorgente dell'azienda sono stati divulgati a seguito di una fuga di notizie.

<http://www.schneier.com/blog/archives/2007/09/leaked_media_de.html>

<<http://arstechnica.com/news.ars/post/20070916-leaked-media-defender-e-mails-reveal-secret-government-project.html>>

oppure <<http://tinyurl.com/ywcf2>>

<<http://torrentfreak.com/mediadefender-emails-leaked-070915/>>

<<http://thepiratebay.org/tor/3809004/MediaDefender.Phonecall-MDD>>

<<http://torrentfreak.com/mediadefender-anti-piracy-tools-leaked-070920/>>

I cinesi sono accusati di aver spiato la nazionale danese dei mondiali di calcio femminile:

<<http://afp.google.com/article/ALeqM5gt5-xvFoitzI191Ynd2iPrjyOm7w>>

<<http://www.nytimes.com/2007/09/14/sports/soccer/14cup.html>>

<<http://canadianpress.google.com/article/ALeqM5iwKeRtUUnGMyKcOHdYyrEqDPfDaA>>

oppure <<http://tinyurl.com/3ad4d6>>

<<http://www.iht.com/articles/2007/09/16/news/soccer.php>>

Multics era un sistema operativo degli anni Sessanta, ed era dotato di una sicurezza migliore di molti sistemi operativi attuali. Questo articolo del 2002 parla della sicurezza di Multics e delle lezioni apprese che sono tuttora importanti.

<<http://www.acsac.org/2002/papers/classic-multics.pdf>>

Un ufficiale dell'esercito pakistano diventa un bombarolo suicida. Probabilmente non esiste nessun metodo concreto di evitare questo genere di attacchi da parte di insider fidati.

<<http://in.rediff.com/news/2007/sep/14raman.htm>>

Le 10.000 telecamere di sicurezza di Londra non servono a ridurre la criminalità:

<<http://www.thisislondon.co.uk/news/article-23412867-details/Tens+of+thousands+of+CCTV+cameras%2C+yet+80%25+of+crime+unsolved/article.do>>

oppure <<http://tinyurl.com/286pab>>

Questo è il seguito di un articolo del 2005:

<<http://www.thisislondon.co.uk/news/article-16856213-details/CCTV+'does+not+stop+crime'/article.do>>

oppure <<http://tinyurl.com/2tfjyf>>

Questo articolo è un resoconto dettagliato dell'indagine che ha portato ai recenti arresti di terroristi in Germania. Pare che le email intercettate abbiano svolto un ruolo chiave in diversi momenti dell'indagine, ma l'articolo non spiega se le informazioni ottenute erano il risultato di alcuni dei programmi di intercettazione all'ingrosso, o se siano state acquisite specificatamente per il caso in questione.

<<http://www.spiegel.de/international/germany/0,1518,504837,00.html>>

Un altro "arresto terroristico" basato sulla paura e sulla reazione eccessiva. Una 19enne chiamata Star Simpson si è recata all'aeroporto di Boston con un badge elettronico ed è stata arrestata con l'accusa di terrorismo:

<<http://www.guardian.co.uk/worldlatest/story/0,-6938913,00.html>>

<http://afp.google.com/article/ALeqM5i_pDxEAYSiWgBNILs8ALAyGID7Lw>

<<http://www.abcnews.go.com/US/wireStory?id=3634458>>
<<http://ap.google.com/article/ALeqM5g2-8Em1L5oDKpru3KXghmCB32tCw>>
<http://www.boston.com/news/globe/city_region/breaking_news/2007/09/mit_student_arr.html?p1=MEWell_Pos3>

oppure <<http://tinyurl.com/2bcka7>>
<http://wbztv.com/topstories/local_story_264104114.html>
<http://wbztv.com/topstories/local_story_264172648.html>
Qui si possono trovare ottime informazioni sull'incidente:
<<http://www.jerrypournelle.com/mail/mail485.html#Shepherd>>
La foto migliore del dispositivo:
<http://machinist.salon.com/blog/2007/09/21/star_simpson/>

Misteriosi frigoriferi appaiono e scompaiono a Toronto. Pensate se fosse accaduto a Boston.
<<http://www.thestar.com/News/GTA/article/259100>>
<<http://www.newswire.ca/en/releases/archive/September2007/21/c3698.html>>

Una coperta "Sicurezza nazionale":
<<http://badbanana.typepad.com/weblog/2007/09/homeland-securi.html>>

Strana storia sulla psicotecnologia e il Dipartimento per la Sicurezza Nazionale:
<http://www.wired.com/politics/security/news/2007/09/mind_reading>

Stupido articolo di crittografia...:
<<http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2007/09/12/cndsei212.xml>>
oppure <<http://tinyurl.com/ysg2a5>>
...Su ciò che pare essere un buon prodotto:
<http://www.schneier.com/blog/archives/2007/09/idiotic_cryptog_1.html>

È facile effettuare un'intercettazione attraverso un cavo di rame; molto più difficile se il cavo è in fibra ottica. Ecco come intercettare su un cavo a fibra ottica. Costo totale dell'hardware: meno di mille dollari.
<<http://blogs.techrepublic.com.com/security/?p=222&tag=nl.e036>>

Cloro e colera in Iraq. Sostanzialmente, stiamo vietando il cloro in Iraq a causa di attacchi contro autocisterne di cloro. Come conseguenza, si sta diffondendo il colera.
<<http://www.ericumansky.com/2007/09/chlorine-and-ch.html>>
<<http://thinkprogress.org/2007/09/22/cholera-iraq/>>
<http://www.usatoday.com/news/world/iraq/2007-02-22-chlorine-iraq_x.htm>

Reuters ha un articolo sulle tecnologie future per la sicurezza. Ho già parlato delle telecamere che leggono automaticamente le targhe dei veicoli e della sorveglianza aerea (aerei telecomandati e satelliti), ma nell'articolo vi è dell'altro. La più impressionante è una tecnologia che si dice possa leggere le impronte digitali a cinque metri di distanza.
<http://news.yahoo.com/s/nm/20070921/tc_nm/homeland_technology_dc_2>

Considerazioni di sicurezza sul cibo che viene somministrato nei penitenziari. Per esempio, i corn dog vengono serviti senza bastoncini.
<<http://www.slatev.com/player.html?id=1182700684>>

Uno studio della NASA degli anni Sessanta che parla dell'utilizzo di tecniche di crittanalisi. Beh, più o meno. "NiCd Space Battery Test Data Analysis Project, Phase 2 Quarterly Report, 1 Jan. - 30 Apr. 1967" [Analisi dei dati della prova di una batteria spaziale al Nichel-Cadmio, Fase 2, Rapporto trimestrale 1 gennaio - 30 aprile 1967] si serve di 'tecniche di crittanalisi' (una sorta di analisi di

frequenza dei trigrammi, credo) per scoprire possibili indizi nascosti sui guasti delle batterie. È difficile immaginare l'esistenza di crittografia non proveniente dalla NSA negli Stati Uniti degli anni Sessanta. In sostanza erano tutte cose alfabetiche. Persino le macchine a rotori erano top secret, e non veniva eseguito assolutamente nulla in binario.

<http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19670029657_1967029657.pdf>
oppure <<http://tinyurl.com/2lwun5>>

Neal Koblitz pubblica un pezzo che, onestamente, altro non è che uno sfogo sul settore della crittografia. Per me la parte interessante è dove parla dello scomodo rapporto fra matematici e crittografi. I crittografi, sostiene Koblitz, abusano un po' troppo spesso del termine "sicurezza provabile", pubblicano studi incoerenti con troppa frequenza, e sono generalmente approssimativi nelle loro ricerche. Non posso dire di trovarmi in disaccordo su questo. I crittografi provengono dalla matematica o dall'informatica. I primi (come Koblitz) sono molto più rigorosi dei secondi, ma questi ultimi tendono a produrre sistemi molto più pratici.

<<http://www.ams.org/notices/200708/tx070800972p.pdf>>

Parecchie confutazioni:

<<http://www.wisdom.weizmann.ac.il/~oded/X/pmc-ltr.txt>>

<<http://www.ee.technion.ac.il/~hugo/ams-letter/koblet.pdf>>

<<http://www.cs.umd.edu/~gasarch/BLOGPAPERS/koblitz.pdf>>

<<http://in-theory.blogspot.com/2007/08/swift-boating-of-modern-cryptography.html>>

oppure <<http://tinyurl.com/393o73>>

<<http://in-theory.blogspot.com/2007/08/swift-boating-of-modern-cryptography.html#c123324347271040959>>

oppure <<http://tinyurl.com/3488ce>>

<<http://www.sigcrap.org/?p=21>>

Rivelato l'algoritmo di password di Oracle 11g. Si basa su SHA-1.

<<http://www.petefinnigan.com/weblog/archives/00001097.htm>>

Gli Stati Uniti presentano un mosaico di leggi sul deposito di bottiglie e lattine di bevande analcoliche. La maggior parte degli stati non hanno depositi, ma alcuni, come il Michigan, sì. Le lattine sono le stesse, per cui è possibile guadagnare dieci centesimi acquistando una lattina in uno stato e lasciandola per il vuoto a rendere nel Michigan. Dieci persone sono state arrestate per aver guadagnato più di 500.000 dollari facendo proprio questo; erano gestori di drogherie nel Michigan, e come tali erano in parte degli insider.

<<http://www.clickondetroit.com/news/14214576/detail.html>>

Quella che segue è un'ottima serie di post di Larry Osterman (Microsoft) sul tema della creazione di modelli di minaccia, servendosi delle API di PlaySound come esempio. Sono interventi lunghi, dettagliati e complessi, ma vale davvero la pena leggere. L'ultimo post è particolarmente buono.

<<http://blogs.msdn.com/larryosterman/archive/2007/08/30/threat-modeling-once-again.aspx>>

oppure <<http://tinyurl.com/3648gc>>

<<http://blogs.msdn.com/larryosterman/archive/2007/08/31/threat-modeling-again-drawing-the-diagram.aspx>>

oppure <<http://tinyurl.com/2wvxb5>>

<<http://blogs.msdn.com/larryosterman/archive/2007/09/04/threat-modeling-again-stride.aspx>>

oppure <<http://tinyurl.com/2jrqmh>>

<<http://blogs.msdn.com/larryosterman/archive/2007/09/05/threat-modeling-again-stride-mitigations.aspx>>

oppure <<http://tinyurl.com/3dc52e>>

<<http://blogs.msdn.com/larryosterman/archive/2007/09/07/threat-modeling-again-what-does-stride-have-to-do-with-threat-modeling.aspx>>

oppure <<http://tinyurl.com/2k9d4y>>

<<http://blogs.msdn.com/larryosterman/archive/2007/09/10/threat-modeling-again-stride-per-element.aspx>>
oppure <<http://tinyurl.com/33sg3s>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/11/threat-modeling-again-threat-modeling-playsound.aspx>>
oppure <<http://tinyurl.com/34olwt>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/13/threat-modeling-again-analyzing-the-threats-to-playsound.aspx>>
oppure <<http://tinyurl.com/3xpcy8>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/14/threat-modeling-again-pulling-the-threat-model-together.aspx>>
oppure <<http://tinyurl.com/3ylhu9>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/17/threat-modeling-again-presenting-the-playsound-threat-model.aspx>>
oppure <<http://tinyurl.com/2pqp3w>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/18/threat-modeling-again-threat-modeling-in-practice.aspx>>
oppure <<http://tinyurl.com/32slsv>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/19/threat-modeling-again-threat-modeling-and-the-firefoxurl-issue.aspx>>
oppure <<http://tinyurl.com/3acmbn>>
<<http://blogs.msdn.com/larryosterman/archive/2007/09/21/threat-modeling-again-threat-modeling-rules-of-thumb.aspx>>
oppure <<http://tinyurl.com/2mr9d8>>

Ricordate l'hack TJX del maggio 2007? Pare che le informazioni della carta di credito furono rubate effettuando intercettazioni del traffico di rete wireless in due negozi Marshalls di Miami. Ulteriori dettagli dal Garante della privacy canadese:

<http://www.boston.com/business/technology/articles/2007/09/25/wireless_systems_faulted_in_tjx_theft/>

oppure <<http://tinyurl.com/2wz82j>>

Ottimo articolo dell' "Economist" sulla raccolta dei dati, sulla privacy, la sorveglianza e il futuro.

<http://economist.com/world/international/displaystory.cfm?story_id=9867324>

oppure <<http://tinyurl.com/2tvacd>>

Una serie di interventi davvero interessanti sugli ordigni esplosivi improvvisati (IED, Improvised Explosive Devices) in Iraq, specialmente sul 'braccio di ferro' fra l'esercito americano e i fabbricanti di IED delle jihad. A volte non è detto che una maggiore presenza di tecnologia rappresenti una soluzione di sicurezza efficace.

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html>>

oppure <<http://tinyurl.com/3ak7ur>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html>>

oppure <<http://tinyurl.com/yp13gv>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/30/AR2007093001675.html>>

oppure <<http://tinyurl.com/yp9phk>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100101760.html>>

oppure <<http://tinyurl.com/2398jo>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366.html>>

oppure <<http://tinyurl.com/2twbxn>>

Il Dipartimento per la Sicurezza Nazionale statunitense assunse la compagnia Unisys per gestire e monitorare la sicurezza di rete del dipartimento. A seguito della scoperta di alcune fughe di dati, il

Dipartimento per la Sicurezza Nazionale ha dato la colpa a Unisys, e già mi aspettavo da parte di tutti il classico atteggiamento di 'pararsi il didietro', e che non si sarebbe mai scoperto che cosa fosse realmente accaduto. ma pare che vi sia stata un'insabbiatura da parte di Unisys, e questo è un bell'affare.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471_pf.html>
oppure <<http://tinyurl.com/yruoa2>>

L'ultimo in fatto di falsi allarmi terroristici: una ciotola di peperoncini rossi:

<http://www.guardian.co.uk/uk_news/story/0,,2182525,00.html>
<<http://www.washingtonpost.com/wp-dyn/content/article/2007/10/03/AR2007100300179.html>>
oppure <<http://tinyurl.com/26ekbc>>

Rara manifestazione di buonsenso: "Il portavoce delle forze dell'ordine ha dichiarato che non sono stati effettuati arresti. 'Per quanto ne so non è un reato cucinare una salsa ai peperoncini molto forte', ha detto".

<http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20071003/spicy_chili_071003/20071003?hub=Health>
oppure <<http://tinyurl.com/2waykw>>

La BBC ha la ricetta, nel caso siate interessati a provocare un allarme chimico.

<http://news.bbc.co.uk/2/hi/uk_news/england/london/7025782.stm>

Una scuola superiore proibisce gli zaini come misura di sicurezza. Questo comprende anche le borsette, ed è una seccatura per le ragazze che hanno bisogno di portare con sé degli assorbenti. Per cui ora alle ragazze che hanno con sé una borsetta, gli agenti di polizia chiedono: "State avendo il ciclo?". Seguono i prevedibili cori di protesta.

<<http://www.recordonline.com/apps/pbcs.dll/article?AID=/20070928/NEWS/709280342>>
oppure <<http://tinyurl.com/yp9j83>>
<<http://pixelfish.livejournal.com/676250.html?nc=1>>

Forse dovrebbero provare a usare degli zaini trasparenti o antiproiettile. (Se soltanto qualcuno inventasse uno zaino antiproiettile trasparente, allora sì che i nostri ragazzi sarebbero finalmente al sicuro!)

<http://www.schneier.com/blog/archives/2007/07/seethrough_back.html>
<http://www.schneier.com/blog/archives/2007/08/bulletproof_bac.html>

Un impiegato del governo utilizza il database del Dipartimento per la Sicurezza Nazionale per rintracciare una ex fidanzata.

<<http://www.techdirt.com/articles/20070924/035849.shtml>>

Quel che vorrei sapere è come hanno scoperto questo tizio. Può essere molto difficile fermare insider come questo; è cruciale avere degli ottimi sistemi di auditing, ma spesso vengono trascurati in fase di progettazione.

Non è più possibile acquistare un'uniforme da poliziotto in California, a meno che non si provi di essere davvero un agente di polizia.

<<http://www.sacbee.com/capolitics/story/401565.html>>

Ho scritto molto in merito al problema di autenticazione delle uniformi. Questa soluzione non risolverà tale problema, ma probabilmente non è nemmeno una cattiva idea.

<http://www.schneier.com/blog/archives/2006/05/people_trusting.html>
<http://www.schneier.com/blog/archives/2006/10/new_hardtocou_1.html>
<http://www.schneier.com/blog/archives/2006/01/forged_credenti.html>
<http://www.schneier.com/blog/archives/2005/08/actors_playing.html>
<http://www.schneier.com/blog/archives/2006/05/thief_disguises.html>

La campagna di pubbliche relazioni della NSA è rivolta ai reporter:

<<http://www.nysun.com/article/63465>>

Casualità nella sicurezza aeroportuale. A me pare un'ottima idea.

<<http://www.msnbc.msn.com/id/21035785/site/newsweek/page/0>>

In un penitenziario dello Sri Lanka è stato scoperto un tunnel di 200 metri, completo di elettricità e luci. Come sono riusciti a sbarazzarsi dei detriti? "Sospettiamo inoltre che si siano imbrattati di terra per poi lavarla via, in modo da evitare che il loro piano clandestino venisse scoperto". Non mi pare che un metodo del genere sia in grado di smaltire 200 metri di terra scavata nel corso di un anno, anche assumendo che si tratti di un tunnel di piccole dimensioni.

<http://lankasun.com:8000/index.php?option=com_content&task=view&id=1468&Itemid=26>
oppure <<http://tinyurl.com/33numx>>

Hack ai danni delle telecamere di sicurezza: si reindirizza l'output video a stazioni di controllo remote:

<http://www.wired.com/politics/security/news/2007/10/camera_hack>

Strana storia di minaccia terroristica dal Raleigh Airport:

<http://www.schneier.com/blog/archives/2007/10/weird_terrorist.html>

Ora le celle a combustibile a metanolo diretto sono permesse sugli aerei. Questo paragrafo ben riassume l'incoerenza di fondo: "Per cui adesso gel/liquidi/shampoo del tutto innocui vengono considerati troppo pericolosi da introdurre a bordo di un aereo, mentre un noto liquido volatile (non importa quanto sicuro possa essere) deve obbligatoriamente essere conservato nel bagaglio a mano? Non sto criticando la tecnologia qui, ma ho l'impressione che questo tipo di logica del Dipartimento dei Trasporti verrà ripetutamente messa in discussione da viaggiatori esasperati".

<http://www.gearlog.com/2007/09/methanol_fuel_cells_cleared_fo.php>

Il governo birmano sta confiscando i dischi rigidi delle Nazioni Unite, alla ricerca di informazioni per identificare i dissidenti. Ciò illustra ancora una volta come le richieste delle forze dell'ordine di tracciabilità delle email siano una pessima idea.

<<http://timesonline.co.uk/tol/news/world/asia/article2609683.ece>>

Intanto, Mesa Airlines distrugge delle prove in un caso giudiziario e dà la colpa alla pornografia per la perdita di quei dati:

<<http://www.bizjournals.com/pacific/stories/2007/09/24/daily33.html>>

<<http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=2007709260410>>

oppure <<http://tinyurl.com/34k3zy>>

Questo jammer di frequenze cellulari costa 166 dollari, ha le stesse dimensioni di un telefonino, ha un raggio di azione di 5-10 metri, e blocca le frequenze GSM a 850, 900, 1800 e 1900 MHz.

<http://gadget.brande.com.hk/prod_detail.php?prod_id=00493>

E qui vi è un modello ancor più piccolo. Mi è stato detto che Deal Extreme invia il dispositivo con un'etichetta che dice che è una torcia a LED (del valore di 45 dollari di Hong Kong), per cui non ha problemi a passare la dogana.

<<http://www.dealxtreme.com/details.dx/sku.4355>>

Ne voglio uno. È un peccato che il loro utilizzo sia illegale negli USA.:

<<http://electronics.howstuffworks.com/cell-phone-jammer5.htm>>

Grafi diretti aciclici (DAG) per analizzare algoritmi crittografici:

<<http://cr.yip.to/cipherdag/cipherdag-20070630.pdf>>

La scorsa settimana ho volato passando per Orlando, e ho notato uno scanner di scarpe

Come dice il nome stesso, gli incontri degli Alcolisti Anonimi sono anonimi. Non occorre firmare nulla, né mostrare un documento d'identità, e nemmeno rivelare il proprio vero nome. Ma gli incontri non sono privati. Chiunque può parteciparvi. E chiunque è libero di riconoscervi: dal viso, dalla voce, dalle storie che raccontate. L'anonimato non vuol dire privacy.

Ciò è ovvio e poco interessante, ma molti sembrano dimenticarsene quando utilizzano un computer. Pensano "è sicuro" e si dimenticano che "sicuro" può voler significare molte cose diverse.

Tor è uno strumento gratuito che permette di usare Internet in modo anonimo. Sostanzialmente, entrando in Tor si entra a far parte di una rete di computer sparsa in tutto il mondo: le macchine appartenenti alla rete si passano il traffico Internet in modo casuale prima di inviarlo alla destinazione prescelta. Immaginatevi una ristretta cerchia di persone che si passano delle lettere. Di tanto in tanto una lettera lascia il gruppo, spedita verso una certa destinazione. Se non potete vedere che cosa avviene all'interno di quella cerchia, non potrete stabilire chi ha inviato una qualsiasi lettera basandovi sull'osservazione delle lettere che lasciano il gruppo.

Ho tralasciato parecchi dettagli, ma questo è in sostanza il principio di funzionamento di Tor. Viene chiamato "routing a cipolla", e fu inizialmente sviluppato al Naval Research Laboratory. Le comunicazioni fra i nodi di Tor sono cifrate in un protocollo a livelli (di qui l'analogia con la cipolla), ma il traffico che lascia la rete Tor è in chiaro. Deve esserlo.

Se volete che il vostro traffico Tor sia privato, dovrete criptarlo. Se volete che sia autenticato, dovrete anche firmarlo. Il sito Web Tor dice persino: "Sì, la persona che gestisce il nodo di uscita può leggere i byte che entrano ed escono da quel nodo. Tor rende anonima l'origine del vostro traffico, e garantisce la cifratura di tutto ciò che si trova all'interno della rete Tor, ma non cripta magicamente tutto il traffico di Internet".

Tor 'anonimizza', niente più.

Dan Egerstad è un ricercatore di sicurezza svedese, che gestiva cinque nodi Tor. Il mese scorso ha pubblicato un elenco di 100 credenziali email (indirizzi IP di server, account email e le rispettive password) di ambasciate e ministeri governativi di tutto il mondo; dati ottenuti effettuando lo sniffing del traffico in uscita alla ricerca di nomi utente e password dei server di posta.

L'elenco contiene soprattutto ambasciate del terzo mondo: Kazakhstan, Uzbekistan, Tajikistan, India, Iran, Mongolia, ma figurano anche un'ambasciata giapponese, l'ufficio di richiesta dei visti britannico nel Nepal, l'ambasciata russa in Svezia, l'Ufficio del Dalai Lama e svariati gruppi di Hong Kong per i Diritti Umani. E questa è solo la punta dell'iceberg: Egerstad ha ottenuto anche un migliaio di conti aziendali con lo stesso metodo di sniffing. Davvero pauroso.

Presumibilmente molte di queste organizzazioni stanno utilizzando Tor per nascondere il proprio traffico di rete dalle spie dei loro paesi. Ma dato che chiunque può aggiungersi alla rete Tor, gli utenti di Tor passano necessariamente il proprio traffico a organizzazioni di cui potrebbero non fidarsi: svariate agenzie d'intelligence, gruppi di hacker, organizzazioni criminali e così via.

È semplicemente inconcepibile che Egerstad sia la prima persona ad aver effettuato questo tipo di intercettazione; Len Sassaman ha pubblicato uno studio su tale attacco qualche mese fa. Il prezzo che si paga per l'anonimato è esporre il proprio traffico a persone infide.

Non sappiamo realmente se gli utenti di Tor esposti fossero i legittimi proprietari degli account o se si sia trattato di hacker introdotti in quegli account con altri mezzi e che si stavano servendo di

Tor per cancellare le proprie tracce. Ma di certo molti di questi utenti non hanno compreso che anonimato non significa privacy. Il fatto che la maggior parte degli account elencati da Egerstad fossero di piccoli paesi non sorprende: proprio da quei paesi c'è da aspettarsi una serie di pratiche di sicurezza più deboli.

È difficile conseguire un anonimato completo. Come possiamo essere riconosciuti in un incontro di Alcolisti Anonimi, così si può essere riconosciuti anche in Internet. Vi sono molte ricerche volte a rompere l'anonimato in generale, e quello di Tor nello specifico, ma in alcuni casi non è neanche necessario fare grossi sforzi. L'anno scorso, AOL ha reso pubbliche 20.000 query di ricerca anonime come strumento di ricerca. Non è stato molto difficile risalire alle persone partendo dai dati.

Un progetto di ricerca chiamato Dark Web, finanziato dalla National Science Fundation, ha persino tentato di identificare scrittori anonimi dal loro stile: "Uno degli strumenti sviluppati da Dark Web è una tecnica chiamata Writeprint, che estrae automaticamente migliaia di caratteristiche multilingue, strutturali e semantiche per determinare chi sta creando contenuti 'anonimi' online. Writeprint può esaminare un post in un forum online, per esempio, e confrontarlo con altri scritti trovati altrove in Internet. Analizzando queste caratteristiche specifiche, può stabilire con più del 95% di accuratezza, se quell'autore ha prodotto altri contenuti in passato".

E se il vostro nome o altre informazioni che possano identificarvi si trovano in solo uno di quegli scritti, è possibile risalire a voi.

Come tutti gli strumenti di sicurezza, Tor viene utilizzato sia da persone oneste che da malintenzionati. Perversamente, proprio il fatto che qualcosa si trovi all'interno della rete Tor significa che qualcuno, per qualche ragione, vuole nascondere o nascondere il proprio operato.

Finché Tor sarà un magnete che attira traffico "interessante", Tor attirerà anche coloro i quali vogliono intercettare quel traffico, specialmente perché più del 90% degli utenti di Tor non lo cripta.

Questo articolo è precedentemente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/09/security_matters_0920>

oppure <<http://tinyurl.com/2ux6ae>>

Tor:

<<https://tor.eff.org/>>

<<http://tor.eff.org/overview.html.en>>

<<http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#ExitEavesdroppers>>

oppure <<http://tinyurl.com/2ozo2b>>

Il routing a cipolla:

<<http://www.onion-router.net/>>

Il lavoro di Egerstad:

<<http://www.derangedsecurity.com/deranged-gives-you-100-passwords-to-governments-embassies/>>

oppure <<http://tinyurl.com/28ya72>>

<<http://www.heise-security.co.uk/news/95778>>

<<http://www.securityfocus.com/news/11486>>

<<http://www.derangedsecurity.com/time-to-reveal%e2%80%a6/>>

<http://www.wired.com/politics/security/news/2007/09/embassy_hacks>

industrie elettriche, raffinerie, industrie chimiche e idriche. Hanno ignorato molto di quel che abbiamo detto ma hanno messo i nostri nomi sulle parti tecniche del rapporto per farlo sembrare credibile. Abbiamo alleggerito o eliminato diverse sezioni che avrebbero potuto avere una certa importanza 20 anni fa, come gli attacchi di war dialing contro i modem.

“Il prodotto finale è un documento di ordine di lavoro del Dipartimento per la Sicurezza Nazionale che richiede cose come background check per quelle persone che hanno accesso ai modem, e tenere la registrazione delle loro visite a siti dotati di attrezzature datacom o sistemi di controllo.

“Fra l’altro, non sono stati in grado di danneggiare il generatore che si vede nel filmato, ma hanno distrutto l’albero che lo manovra e il gruppo elettrogeno. Hanno innescato l’evento da una distanza di 30 miglia! Poi hanno estrapolato la teoria per cui un generatore in avaria può distruggere non soltanto altri generatori alla centrale energetica, ma che le interruzioni di elettricità sulla rete potrebbero distruggere motori distanti parecchie miglia sulla rete elettrica che pompano acqua o gasolio (attraverso i condotti).

“Hanno tenuto tutto sotto segreto (ogni email e rapporto venivano criptati, si facevano riunioni ad alta sicurezza a DC) finché hanno prodotto un filmato e un comunicato stampa per la CNN. Il Dipartimento per la Sicurezza Nazionale era enormemente preoccupato che questa vulnerabilità potesse essere scoperta dai criminali, e adesso la rende di dominio pubblico per questioni politiche tutte loro. Davvero vergognoso.

“Oh, e si sono serviti di un appaltatore per tutto il grosso lavoro di lifting impiegato per scrivere e revisionare il documento sulle attenuazioni necessarie. Non sono nemmeno stati in grado di realizzare loro stessi questo lavoro.

“Fra l’altro, la vulnerabilità che ipotizzano è una sciocchezza completa, ma non entrerà nei dettagli. Per me fa ancora troppo caldo a Gitmo in questo periodo dell’anno”.

<<http://www.cnn.com/2007/US/09/27/power.at.risk/index.html>>
<<http://apnews.myway.com/article/20070927/D8RTODL80.html>>
<<http://it.slashdot.org/it/07/09/27/1229230.shtml>>

Sicurezza SCADA:

<http://www.schneier.com/blog/archives/2007/05/scada_security.html>

** ** ** ** **

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l’argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** ** ** ** **

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all’indirizzo <<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare

l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA

<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

<<http://www.counterpane.com>>

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2007 - Bruce Schneier.