Furto di dati e crimine informatico: il caso Sony

Igor Nai Fovino (GCSEC) e
Salvatore Di Blasi (GCSEC)

L'evoluzione e la diffusione delle tecnologie informatiche e di Internet costituiscono un'opportunità per la crescita e la convergenza dei servizi online: se da un lato le opportunità di business per le aziende e I service providers sono cresciute, dall'altro è indubbio che le possibilità per gruppi criminali organizzati di commettere attività illecite a scopo di frode ed estorsione sono aumentate drasticamente; furto d'identità e violazione dei dati personali rappresentano uno dei trend maggiormente in crescita negli ultimi anni, e recentemente il caso Sony è salito agli onori della cronaca.

Nei primi giorni di Aprile Sony ha citato in giudizio George "GeoHot" Hotz, un hacker di 21 anni che ha scoperto e successivamente rivelato online la root key della PlayStation 3.

Come risposta **the Anonymous**, una nota comunità online, ha lanciato una serie di attacchi DDoS (Distributed Denial of Service) e LOIC (Low Orbit Ion Cannon) contro la società. I due attacchi sono stati denominati #OpSony e #SonyRecon.

Il primo attacco ha colpito i siti web di Sony, mentre il secondo, utilizzando tecniche di social engineering, ha raccolto e pubblicato i dati personali sui dirigenti Sony, compreso il CEO Howard Stringer.

Dopo questa escalation di attacchi, non è accaduto più nulla fino al 19 Aprile, data in cui Sony ha disconnesso le reti Qriocity (per la vendita di servizi come video on demand, musica ed altri contenuti multimediali) e PSN (PlayStation Network). Per alcuni giorni, nessuna comunicazione viene rilasciata alla community sulla motivazione di questa scelta; poi, il 25 aprile la Sony inizia fornire le prime informazioni sugli attacchi subiti.

Apparentemente, sfruttando alcune vulnerabilità dei sistemi di protezione, sono stati colpiti i data center Sony con conseguente furto di dati personali di oltre 77 milioni di utenti nel mondo.

Più specificatamente, secondo Shinji Hasejima, Chief Information Officer di Sony, l'attacco è stato lanciato sfruttando una vulnerabilità di un server applicativo, oltrepassando un server web e due firewall sull'infrastruttura perimetrale di rete.

Le indagini in corso hanno inoltre rivelato che sono stati rubati altri 25 milioni di record relativi

a clienti di Sony Online Entertainment (SOE) tra il 16 e 17 Aprile, ancora prima dell'attacco al sistema PSN: ancora una volta sotto attacco nomi, indirizzi, email, date di nascita, numeri di telefono e altre informazioni sensibili di utenti facenti parte del network dei videogames.
Nella seconda metà di Maggio altri tre attacchi al sistema Sony vengono rilevati; nello specifico, si è dapprima verificata un'intrusione nel sistema So-Net Entertainment Corp, controllata di Sony, mirata al furto di punti bonus virtuali da destinarsi agli utenti del network dei videogames, per un valore stimabile di poco più di 1.000 dollari.
A distanza di poco tempo, F-Secure rivela di aver individuato un server di phishing operante ed ospitato all'interno dell'infrastruttura di rete Sony, nell'area geografica Asia-Pacifico in Thailandia: incidente, questo, che pare non essere correlato al PSN hack, ma che mette in palese risalto quanto estesa sia la superficie di attacco verso un network così ampio come quello di Sony.
Da ultimo, la Sony BMG Greece è stata attaccata ripetutamente da cracker, con furto di dati personali della community greca (SonyMusic.gr), a quanto pare sfruttando vulnerabilità del sistema applicativo ad attacchi di tipo SQL injection.
Iniziando ad analizzare l'intera vicenda, ci si può chiedere intanto perché I primi attacchi non sono stati rilevati prontamente: secondo **Shinki Hasejima**, il sistema di sicurezza non è stato in grado di rilevarli poichè scambiati per normali transazioni di acquisto.
Il gruppo responsabile della gestione della rete Sony Entertainment International non era a conoscenza delle vulnerabilità applicative, fatto di persè già molto significativo, data l'importanza e la dimensione multinazionale di Sony.
Tornando ai risultati dell'attacco, 25 milioni di record utenti sono stati rubati nel primo attacco, 77 milioni in più nel secondo. I dati rubati nell'ultimo attacco sono stati conservati nel Datacenter AT&T di San Diego, in forma non cifrata.
Tra questi 77 milioni di utenti, almeno 10 milioni hanno registrato i numeri delle proprie carte di credito: tali dati erano archiviati in forma cifrata in un altro repository (all'interno dello stesso Data Center); ciò significa che, anche se in possesso delle credenziali di accesso e dei numeri di carte di credito, c'è una buona possibilità che gli attaccanti non ne abbiano potuto usufruire a scopo fraudolento (anche se tuttavia un'operazione di decifratura batch è un'operazione costosa ma non impossibile).
In questo senso, la cosa più importante è che Sony abbia dichiarato di non aver archiviato, in base a policy di sicurezza interne, il codice di sicurezza (CCV) associato alle carte di credito.
In questo contesto, considerando il danno potenziale alle vittime di un simile attacco (gli utenti finali), è possibile fare una prima distinzione tra gli utenti che abitualmente utilizzavano carte prepagate ed utenti che utilizzavano carte di credito. E' ovvio come, in teoria, entrambe le categorie di utenti siano state danneggiate, ma in termini pratici, vale la pena sottolineare come gli utilizzatori di carte prepagate siano in casi simili maggiormente protetti, in quanto queste ultime non danno accesso all'intero plafond del proprio conto corrente, ma (se utilizzate correttamente) ad una limitata somma di denaro.
Nel frattempo, la società G Data ha pubblicato già alcuni dettagli sul mercato underground già operante con i set di dati rubati.
E' importante notare che in questi attacchi, fino ad ora non vi è prova del coinvolgimento del gruppo Anonymous, né di Georg Hotz, le indagini sono in corso.
L'impatto di questa serie di eventi dovrebbe innalzare l'attenzione a livello nazionale e mondiale: in poco tempo questo attacco è stato in grado di colpire direttamente oltre 77 milioni di utenti,

causando allo stesso tempo, considerato l'impatto sul mercato azionario, danni ad una multinazionale come Sony per milioni di euro, e altri danni a tutti i soggetti coinvolti direttamente o indirettamente con le operazioni di Sony.
Fonti interne di Sony hanno reso noto l'entità dei danni derivanti da questa serie di attacchi: si ipotizza un costo totale di circa 170 milioni di dollari (122 milioni di euro), con costi relativi al downtime dei servizi e dei sistemi attaccati, la fornitura gratuita di un programma di protezione antifrodi, la promessa di investimento di 1 milione di dollari per l'assicurazione contro il furto di identità (solo negli USA), il programma "Welcome Back" per il risarcimento degli utenti colpiti, l'assistenza generale e il supporto, il potenziamento dell'infrastruttura e dei processi di gestione della sicurezza interna e perimetrale, con costi ulteriori per azioni legali ed investigazioni, il tutto con un impatto assolutamente negativo sulle previsioni per l'anno fiscale.
Questo incidente evidenzia come la violazione dei dati (**data breach**) rappresenti una delle maggiori minacce che I fornitori di servizi ed i loro clienti possono sperimentare al giorno d'oggi nell'uso dei sistemi ICT e questo sposta inevitabilmente l'attenzione sulla sicurezza dei servizi 'cloud' sotto due prospettive principali: operativa e policy/normativa.
Da un punto di vista strettamente operativo, i piani di incident response ed information security assurance si sono rivelati inefficaci: troppo tempo trascorso tra la rilevazione delle intrusioni e il riconoscimento del danno. Dopo essere stati offline per diversi giorni, i servizi di PSN e Qriocity hanno cominciato ad essere ripristinati progressivamente, con molte difficoltà.
E' importante notare anche come gli attacchi avvengano spesso mediante tecniche già ampiamente riconosciute: pur esistendo tecniche di protezione da questo tipo di attacchi largamente condivise dalle community per secure coding, l'-SQL injection compare oramai da diversi anni al top dei ranking delle vulnerabilità più rischiose per semplicità d'esecuzione - esistono strumenti per automatizzare l'esecuzione di diverse varianti di questo attacco - ed entità dell'impatto finale. Tuttavia, è ancora una delle tipologie di attacco più frequenti.
La gestione della comunicazione non è stata adeguata, soprattutto nella prima fase convulsa di risposta all'incidente: gli utenti, ed in generale

GLOBAL CYBER SECURITY CENTER

A joint event GCSEC – ICANN

The 2011 workshop on DNS HEALTH & SECURITY (DNS EASY 2011)

October 18-20, 2011 - GCSEC headquarter, Rome, Italy

Scope
Global Cyber Security Center - GCSEC, in cooperation with ICANN, organizes the 2011 workshop on DNS hEAlth and SecuritY (DNS EASY 2011). The DNS EASY workshop aims at bringing together researchers and professionals from academia, industry and governmental Agencies as well as representatives from across DNS ecosystem stakeholder groups (technical development, network operators, enterprise users, and security experts) to discuss all different aspects of the DNS Health and Security and its impact on the modern society.
The Domain Name System (DNS) is the core of the Internet infrastructure. With the increasing dependency on ICT of Critical Infrastructures (CIs) control and governance, DNS started to indirectly play a relevant role also in the daily life of the citizen, and for that reason must be considered by itself a critical infrastructure.
The workshop is organized in two parts. The first, for freely attendance, is devoted to research results, R&D results and industrial experiences presentations. The second part, for invitation only, will be related to the discussion of operational and policy open issues and challenging related to the DNS health and security. Scientific contributions will be a precious input and could be used to drive discussions in the second part of the workshop.
Authors are solicited to contribute to the workshop by submitting research papers, work-in-progress reports, R&D project results, surveying works and industrial experiences describing significant advances in

gran parte degli stakeholder, si sono lamentati della lentezza con cui Sony ha preso la decisione di ammettere e comunicare i dettagli del'incidente, con la conseguente minaccia da parte di alcuni bacini d'utenza di avviare una class action contro Sony.
Tuttavia, un lato positivo che si può riscontrare in questa vicenda consiste nella richiesta di supporto che Sony ha inoltrato ad organismi di forze dell'ordine nazionali come l'FBI: questa cooperazione, unitamente ad una rinnovata attenzione alla gestione della sicurezza, hanno portato ad identificare e rilevare i successivi attacchi con maggiore reattività.
Da un punto di vista di policy e normativo, la security rappresenta ancora una sfida ed evidenzia il problema della responsabilità in caso di problemi di sicurezza: in questo senso, è notizia recente che il governo australiano sta progettando di mettere in atto alcune modifiche legislative, per richiedere ai service provider di intervenire immediatamente nei confronti dei loro clienti ogni volta che sono rilevate intrusioni o attacchi informatici.
E' fondamentale comprendere che, come Sony, tutte le grandi multinazionali con distribuzione dei propri servizi su sistemi cloud e relative customer base sono potenzialmente a rischio e dovrebbero correre ai ripari preventivamente: gli incidenti non possono essere evitati, ma le aziende devono essere pronte ad affrontare l'inevitabile e a gestire i rischi.
Audit di sicurezza interna dovrebbero essere continui e con un raggio d'azione capillare; i piani di incident response dovrebbero essere chiaramente definiti, concordati, comunicati, testati ed applicati. Le lessons learnt devono essere condivise all'interno e all'esterno dei confini della società, migliorando quei meccanismi di condivisione di informazioni e di conoscenza che consentono alle comunità di imparare dagli errori.
La cooperazione con le forze dell'ordine deve essere costante, con la definizione di un chiaro punto di contatto, le procedure di incident reporting, lo scambio di informazioni e le operazioni da svolgere comunemente.
Infine, questi attacchi rivelano ancora una volta le vulnerabilità dei sistemi e servizi ICT: è certamente un problema di inadeguatezza di tecnologia e di processi, ma è anche una questione di cultura, di educazione e di sensibilizzazione alla sicurezza. ■

the following areas:
- DNS Security, Resilience, Stability and Performance metrics (DNS Health).
- DNS Infrastructure Resilience and QoS
- DNS Cyber Threats and Vulnerabilities
- DNS Defense
- DNS and Cybercrime
- Impact of DNS on Critical Infrastructures (Energy Systems, Finance etc.)
- DNSSEC (all aspects)
- DNS Infrastructure Modeling & Simulation
- DNS Operations vs. DNS Health and Security
- DNS Governance vs. DNS Health and Security

Date, Venue and Attendance
- October 18-20, 2011
- The workshop will be hosted in GCSEC headquarter, Viale Europa 175, 00144, Rome, Italy.

Collection of works and workshop publications
All submissions will be subjected to a thorough blind review by at least three reviewers. Papers should be up to 12 pages in English, including bibliography and well-marked appendices. It is planned to publish conference post-proceedings by Springer Verlag in the LNCS Series. Pre-proceedings will appear at the time of the conference. At least one author of each accepted paper is required to register with the Workshop and present the paper. Paper submission will be done via EasyChair.
To submit a paper, please follow the specific instructions available at Easychair website e submitted paper (in PDF or PostScript format), which should follow the template indicated by Springer, must start with a title, a short abstract, and a list of keywords. However, it should be anonymised with no author names, affiliations, acknowledgements, nor obvious references.

Important Dates
- Deadline for submission of papers: **July 15, 2011**
- Notification to authors: **August 15, 2011**
- Camera-ready papers: **September 10, 2011**

For further information, contact us at **dnseasy2011@gcsec.org** or visit **dnseasy.gcsec.org**