OSINT- open source intelligence

ABI Associazione Bancaria Italiana

Come un criminale prepara un attacco e come una azienda può fare prevenzione

Paolo Giardini
Direttore Osservatorio Privacy e Sicurezza Informatica

Milano, 26-27 maggio 2016

Il relatore

ABI Associazione Bancaria Italiana

- Analista e docente OSINT
- Partner Security Brokers
- Membro Roster of Experts presso ITU (International Telecommunication Union, agenzia delle Nazioni Unite)
- Direttore Osservatorio Privacy Sicurezza Informatica
- Privacy Officer Associazione Informatici Professionisti
- Consulente normativa privacy e sicurezza delle informazioni
- Membro del Centro di Competenza Open Source Regione Umbria
- Consulente tecnico in computer forensics x Procure, FFOO, Avvocati e Privati
- Socio Fondatore Accordance, GNU/LUG Perugia, ...
- Collaboro/ho collaborato con varie Associazioni e Community: Techeconomy, Shanzin Tech, Sikurezza.org, Italian Linux Society, CLUSIT, Information Systems Security Association, Associazione Italiana Professionisti Sicurezza Informatica, Giuristi Telematici, Hacker's Corner, BackTrack Italia,...
- Ideatore ed organizzatore dell'hacker game *“Cracca al Tesoro” (CAT)*

Argomenti

- Spear Phishing. Un problema reale
- Un esempio di attacco Spear Phishing. Il virus *Carbanak*
- Come è possibile trovare le informazioni necessarie per un attacco?
- OSINT. Open Source Intelligence per tutti, buoni e cattivi
- Cosa fare per prevenire i rischi

Cosa è lo Spear Phishing

- Lo spear phishing è truffa via e-mail diretta ad un gruppo specifico o un'organizzazione. Ad esempio una banca
- A differenza del phishing, che è un invio massivo ed indiscriminato di mail fasulle, la mail viene inviata ad un bersaglio preventivamente identificato
- Lo scopo dello Spear Phishing è ottenere l'accesso non autorizzato ai dati sensibili a disposizione della vittima o l'accesso ad un computer all'interno dell'organizzazione dal quale lanciare l'attacco vero e proprio

Il caso del virus Carbanak

- Kaspersky ha pubblicato lo scorso anno l'analisi dell'infezione da parte di un gruppo criminale di circa 100 Istituti Bancari tramite il virus Carbanak
- L'attacco è stato mirato specificatamente sulle banche, perché è *il posto dove si trova il denaro*
- L'infezione è partita tramite la ricezione di e-mail Spear Phishing contenenti un link ad un sito infetto o documenti contenenti macro che sfruttano vulnerabilità Office per installare il virus

Come funziona il modello Carbanak

- Carbanak è un sistema APT *(Advanced Persistent Threat)* che permette di prendere il controllo di un computer ed osservare le attività dell'operatore legittimo
- In questo modo i criminali hanno appreso, direttamente dai dipendenti della banca vittima, le modalità operative per effettuare operazioni di trasferimento fondi e gestione di ATM
- Questo modello ha fruttato ai criminali oltre 1 Mld di dollari
- Secondo Proofpoint sono tutt'ora in corso attacchi a istituzioni finanziarie in USA, Medio Oriente ed Europa con il modello Carbanak

Il report di Kaspersky

Come funziona lo Spear Phishing

- La prima fase è la ricerca di informazioni sull'organizzazione target
  - Dipendenti, struttura, sistemi informatici, procedure, modalità operative, e-mail, server, documenti, informazioni personali, ...
- Una volta individuati uno o più soggetti "interessanti" vengono create ed inviate e-mail appositamente costruite:
  - per apparire inviate da indirizzi "trusted"
  - contenenti riferimenti ed informazioni reali per non creare sospetti e guadagnare la fiducia della vittima
  - contenenti link o allegati malevoli e l'invito a cliccare od aprire l'allegato

Come vengono trovate le informazioni

- La ricerca di informazioni è “facilitata” da:
  - Evoluzione dei mezzi di comunicazione (internet)
  - Esplosione dei social networks
  - Pubblicazione indiscriminata di informazioni ***personali ed aziendali*** da parte di utenti (per voglia di protagonismo, condivisione, necessità di evasione, ricerca di contatti, rivalsa, sfogo, ...) ed organizzazioni (siti web, profili istituzionali, comunicati stampa, comunicazioni interne, documenti pubblici,...)
  - Mancanza di consapevolezza da parte degli utenti
  - Procedure non adeguate delle aziende per la pubblicazione di documenti ecc.

OSINT Open Source Intelligence

- “Open Source” è relativo alle fonti aperte, cioè alle informazioni liberamente disponibili su internet (e non solo)
- E’ in questa infinita quantità di informazioni che opera l’esperto di OSINT
- Ricercare, esaminare, correlare le informazioni pubblicamente disponibili permette di ottenere informazioni sull’organizzazione, sui progetti, sui processi aziendali, sulle persone
- Su queste informazioni si basano gli attacchi dei criminali *(e le attività dei competitor)*

Come contrastare?

- Formare *dipendenti* e *dirigenti* per un utilizzo consapevole degli strumenti (computer, apparati mobile, mail, social networks,...)
- Definire e applicare policy e best practice
- Verificare periodicamente il grado di consapevolezza degli utenti e l'applicazione delle policy
- Utilizzare strumenti di prevenzione (blocco di servizi e di siti, analisi e filtraggio dei contenuti, crittografia, firma elettronica,...)

Una metodologia per la prevenzione

- Effettuare o fare effettuare analisi OSINT sulla propria organizzazione e sulle figure chiave *(ed agire di conseguenza)* per:
  - Verificare quali informazioni rilascia/ha rilasciato la propria organizzazione
  - Valutare quali informazioni sono pubblicamente disponibili da altre fonti (compresi i dipendenti) sulla propria organizzazione o su figure chiave
  - Valutare / sanitizzare i documenti pubblicati / da pubblicare

Conclusioni

- Lo Spear Phishing funziona perché fa leva sulla curiosità innata degli utenti, sulla "moda" dei social network, sulle informazioni impropriamente pubblicate per creare mail credibili ed "appetibili"
- OSINT può aiutare a trovare i problemi ma:
  - La formazione e la consapevolezza sono le chiavi per ridurre i rischi
- Ricordate l'acronimo PEBKAC:

  "Problem Exist Between Keyboard And Chair"

Contatti

ABI Associazione Bancaria Italiana

Grazie
per la vostra attenzione

paolo.giardini@aipnet.it
http://blog.solution.it

Link

- Carbanak

http://www.kaspersky.com/internet-security-center/threats/carbanak-apt
https://www.proofpoint.com/sites/default/files/proofpoint-threat-insight-carbanak-group-en.pdf
https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
http://www.corriere.it/tecnologia/economia-digitale/15_febbraio_18/carnabak-cyberfurto-secolo-banche-italiane-8250af8a-b787-11e4-bef5-103489912308.shtml
http://www.corriere.it/esteri/15_febbraio_17/furto-hacker-1-mld-dollari-che-nessuno-riesce-ancora-fermare-a9c880e2-b679-11e4-a17f-176fb2d476c2.shtml
http://www.bitmat.it/blog/news/41649/allarme-carbanak-100-istituti-finanziari-colpiti-oltre-1-miliardo-di-dollari-il-bottino

- OSINT

http://www.festivaldelgiornalismo.com/programme/2016/analysis-of-open-sources-for-journalists