



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Servizio delle attività informative della Confederazione SIC

Spionaggio economico



Spiegazioni del cortometraggio
«Nel mirino»

Perché un film sullo spionaggio economico?

«Nel mirino» fa parte del programma di prevenzione e sensibilizzazione Prophylax lanciato nel 2004 dal Servizio delle attività informative della Confederazione (SIC). Il cortometraggio è stato prodotto a fini di formazione per trasmettere alle aziende e alle istituzioni informazioni sullo spionaggio.

Il modo di procedere dei servizi di intelligence stranieri per accedere a informazioni confidenziali o segrete, descritto nel film, è un tipico metodo mirato impiegato dai servizi di intelligence stranieri o da attori privati, anche se nel dettaglio gli approcci possono variare. I commenti seguenti mirano a incrementare la comprensione del pubblico sulle peculiarità di tali azioni di spionaggio. In tale ambito vengono trasmesse ulteriori informazioni sui modi di procedere e sui metodi di spionaggio e illustrate le possibili misure di protezione che possono essere adottate per minimizzare il rischio di spionaggio.

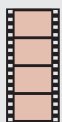


NEL MIRINO

Dal targeting al reclutamento: Le fasi di un tentativo di reclutamento

Le fasi descritte di seguito non sono chiaramente scindibili, bensì possono sovrapporsi. Esse dipendono dallo scopo dell'operazione, dalla persona obiettivo, dai mezzi impiegati, dal tempo a disposizione e dal contesto operativo. Determinate fasi possono essere molto brevi, mentre altre richiedono tempi più lunghi. Tra il targeting e il reclutamento di una persona obiettivo possono trascorrere, a seconda dei casi, da alcune settimane a vari mesi e, in determinati casi, persino diversi anni.

Targeting: ricerca della persona obiettivo adeguata e accertamento delle vulnerabilità



OSINT e acquisizione clandestina di informazioni

Tramite ricerche online e consultazione di opuscoli pubblici della ditta Grinder SA, l'agente straniero Frank Salov identifica Stefan Jeger, responsabile del settore ricerca e sviluppo, quale persona obiettivo molto promettente. Jeger è presente con un profilo dettagliato su vari social network dove fornisce altresì informazioni sulla sua attività di scrittore e sulle sue prossime letture pubbliche. Tramite l'osservazione segreta di Jeger, Salov raccoglie immagini e informazioni sul suo entourage e sui luoghi che frequenta abitualmente. Tali informazioni consentono a Salov di individuare le vulnerabilità e i punti deboli di Jeger.

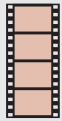
L'autore cerca informazioni che possono condurre a una persona obiettivo adeguata in grado di fornire le informazioni richieste o di favorire l'accesso a tali informazioni. L'acquisizione di informazioni e dati sulla persona obiettivo può avvenire tramite una raccolta di informazioni pubblica o clandestina:

- È definita **Open Source Intelligence (Osint)** l'acquisizione e l'analisi legale di informazioni da fonti accessibili al pubblico quali pagine web, giornali e periodici, visite a esposizioni e manifestazioni pubbliche, banche dati gratuite o a pagamento, social media ecc. Le reti sociali (Facebook, LinkedIn ecc.), in particolare, offrono spesso una grande varietà di informazioni su una persona. Attività professionale, fotografie, relazioni, hobby, contributi a forum online, viaggi ecc. consentono di tracciare un profilo di una persona provvisto di abitudini, interessi, contatti, passioni e frustrazioni.
- Nell'ambito dell'**acquisizione clandestina di informazioni** vengono impiegati mezzi di intelligence quali per esempio la sorveglianza tecnica o fisica della persona obiettivo. In questo caso si tratta di identificare i movimenti nonché ulteriori contatti personali e attività della persona obiettivo.

Possibili misure di protezione:

Chi pubblica informazioni (documenti, immagini, commenti ecc.), ha la possibilità di decidere fino a che punto informare su sé stesso/a o su un progetto, un prodotto, un istituto o una ditta e i suoi collaboratori.

Presenza di contatto: inizio dei contatti con la persona obiettivo

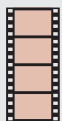


Il primo contatto

Salov sfrutta il fatto che Jeger scrive volentieri e aspira a essere letto nonché a pubblicare i suoi testi. Pertanto, si fa passare quale agente letterario per stimolare la curiosità e la fiducia di Jeger e facilitare l'ulteriore sviluppo dei contatti.

Il primo contatto con la persona obiettivo viene preparato nei minimi dettagli. Al riguardo l'agente o l'attore privato si serve delle informazioni sulle abitudini e sui punti deboli della persona obiettivo acquisite durante la fase di targeting. Tali informazioni consentono di trovare una corretta base di discussione senza che la persona obiettivo sospetti intenzioni illecite. A tale scopo l'agente o l'attore privato assumono spesso un'identità fittizia appropriata.

«Coltivare»: instaurazione di un rapporto di fiducia e di dipendenza



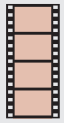
Sfruttamento del punto debole quale leva, motivazione o incentivo

Salov sfrutta in modo mirato la passione di Jeger per la scrittura. Al Caffè letterario lo elogia per la sua lettura e finge di avere interessi comuni. Quando Salov ventila a Jeger la possibilità di una pubblicazione nella rivista letteraria «Europe», quest'ultimo vede l'opportunità di realizzare il sogno della sua vita. In questo modo Salov crea un rapporto di dipendenza: Jeger ha bisogno del suo aiuto, per cui si sente in dovere di ricambiare. Questo rapporto di dipendenza viene ulteriormente consolidato, quando al ristorante «Seesicht», Salov dichiara a Jeger di mettersi a sua disposizione quale agente letterario.

Quando la persona obiettivo è ritenuta una potenziale fonte appropriata e il ghiaccio è rotto, si instaura un rapporto di fiducia. A tale scopo l'autore strumentalizza gli interessi o le passioni «comuni» e sfrutta in modo mirato i punti deboli della persona obiettivo come leva. Quest'ultima può presentarsi sotto forma di favori (p. es. omaggi destinati a stuzzicare la vanità o la prospettiva di un nuovo posto di lavoro). L'agente dei servizi d'intelligence può anche tentare di procurarsi materiale compromettente strumento di pressione/di ricatto) sulla persona obiettivo (riprese video o fotografiche che, per esempio, ritraggono la persona obiettivo mentre consuma droga, commette un'infedeltà sessuale o accetta denaro). Attraverso lo sviluppo dei contatti viene a crearsi una dipendenza della persona obiettivo nei confronti dell'autore, rendendola sempre più ricattabile.

Acquisizione

Colloquio di acquisizione



Un'abile svolgimento del colloquio

Salov carpisce abilmente a Jeger informazioni confidenziali sulla sua attività e sui progetti di ricerca della Grinder SA.

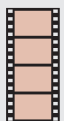
- Salov invita Jeger nel rinomato ristorante «Seesicht» fingendo di intravedere il suo potenziale e di apprezzarlo nonché facendogli credere che dispone di risorse importanti e di grande influsso.
- Salov elogia il progetto di testo per la rivista «Europe» e incoraggia Jeger a continuarne la redazione.
- Quando Jeger racconta a Salov, che sviluppa rettificatrici cilindriche, Salov finge di non avere conoscenze in merito affinché Jeger fornisca ulteriori dettagli.

Non appena l'autore ha coinvolto la sua persona obiettivo in una dipendenza positiva (incentivo) o negativa (materiale compromettente), inizia l'acquisizione delle informazioni cercate. Con uno svolgimento abile et acuto del colloquio carpisce alla persona obiettivo un numero crescente di informazioni, senza che questi abbia il sospetto di fornire informazioni importanti.

Cyberspionaggio

La progressiva digitalizzazione e interconnessione dell'economia e della società aumentano la vulnerabilità di istituzioni e persone private nei confronti dei cyberattacchi. La protezione di dati elettronici, di reti e di mezzi di comunicazione assume pertanto un'importanza fondamentale. Nondimeno, il comportamento della persona continua a rappresentare il maggiore fattore di rischio.

Social engineering (manipolazione sociale)



Spear phishing

Salov invia un link a Jeger, affinché questi compili un curriculum vitae elettronico destinato al Signor Simon, l'editore della rivista di letteratura «Europe». Cliccando sul link Jeger installa inconsapevolmente sul suo computer della ditta un malware tramite il quale Salov ottiene l'accesso alla rete informatica della ditta Grinder SA. Tuttavia, la ditta gestisce due reti separate: i dati sensibili concernenti i progetti di ricerca e le tecnologie sono registrati su una rete separata che non è collegata a Internet. In questo modo l'accesso di Salov a tali dati viene impedito.

Per social engineering si intende l'influsso psichico esercitato su persone allo scopo di indurle a rivelare dati confidenziali o a effettuare determinate azioni. Nel campo della sicurezza delle informazioni il social engineering è spesso utilizzato per ottenere i nomi degli utenti e le password nonché per diffondere virus e cavalli di Troia. Le collaboratrici e i collaboratori di un'azienda vengono avvicinati tramite i social network, false e-mail o offerte di lavoro. Questi attacchi possono avvenire tramite phishing o spear phishing:

Possibili misure di protezione:

È importante sapere quali informazioni sono degne di protezione e non devono essere condivise o trasmesse a terzi. Si tratta in particolare di dati la cui pubblicazione o comunicazione può causare un danno alle aziende o alle istituzioni. Se una persona chiede simili informazioni specifiche è opportuno dare prova di una certa diffidenza.

Possibili misure di protezione:

- Pubblicare solo tante informazioni quanto basta. Ciò vale in particolare per la pubblicazione di nomi, di funzioni e di fotografie di collaboratrici e collaboratori.
- Diffidenza nei confronti delle e-mail provenienti da mittenti sconosciuti, in particolare quando contengono un link o un allegato.
- Prescrizioni di sicurezza e una cultura della sicurezza a livello aziendale che coinvolge tutte le collaboratrici e i collaboratori.

mentre le e-mail di phishing sono inviate in massa a indirizzi e-mail qualsiasi, le e-mail di spear phishing mirano la collaboratrice o il collaboratore che si intende attaccare.

Smartphone



Infezione di uno smartphone

Nel ristorante «Seesicht» Salov osserva come Jeger digita il suo codice di accesso sullo smartphone. Con una manovra diversa Salov ottiene l'accesso allo smartphone di Jeger e installa un malware che gli consente di accedere a tutte le applicazioni e di controllarle. In tal modo è in grado, tra l'altro, di attivare il microfono, per cui può ascoltare tutte le conversazioni di Jeger con il suo team di ricerca.

Molto spesso i sensori e le funzioni disponibili negli smartphone (GPS, microfono, videocamera, applicazioni scaricate, rubrica dei contatti, Wi-Fi, Bluetooth ecc.) trasmettono dati e metadati sull'utilizzazione dello smartphone o sull'utente. Pertanto, l'analisi di questi dati da parte di terzi è un'impresa facile. L'infezione di uno smartphone non necessita un accesso fisico al cellulare poiché esistono metodi che permettono di infettarlo a distanza.

Possibili misure di protezione:

- Cifrare gli apparecchi elettronici e non lasciarli incustoditi.
- In occasione di viaggi di servizio all'estero portare con sé soltanto gli apparecchi elettronici e i documenti strettamente indispensabili.
- Mai discutere di argomenti confidenziali al cellulare.
- Attenzione all'installazione di app da fonti sconosciute.

Chiavi USB



Infezione di apparecchi elettronici o furto di dati mediante chiavi USB

Linda inserisce una chiave USB nel Laptop del CEO della Grinder SA.

L'impiego di una chiave USB è un ulteriore mezzo per infettare i computer e altri apparecchi elettronici o per scaricare i relativi dati da parte di persone non autorizzate. Un'infezione con un malware (virus, cavalli di Troia ecc.) tramite una chiave USB può avvenire in pochi secondi.

Possibili misure di protezione:

Non utilizzare periferiche esterne (chiavi USB, mouse, dischi duri esterni ecc.) estranee o regalate. Tali omaggi promozionali possono essere infettati con un malware.

Honey pot (vaso di miele)



Seduzione

Dopo che i tentativi del servizio di intelligence straniero per ottenere le informazioni segrete cercate attraverso Jeger sono falliti, Linda seduce il CEO della Grinder SA, per accedere al suo laptop.

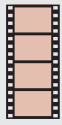
Il termine «Honey pot», riferito a una tecnica di spionaggio classica, designa il tentativo di acquisire o di reclutare una persona obiettivo mediante seduzione a sfondo sessuale. La persona obiettivo fornisce le informazioni desiderate di sua iniziativa o gli vengono estorte mediante materiale compromettente.

(Il termine «Honey pot» è altresì utilizzato in ambito cyber in cui designa un programma informatico o un server che simula i servizi di rete di un altro computer allo scopo di ottenere informazioni su un possibile aggressore e sul suo modello di attacco, senza mettere in pericolo la rete da proteggere.)

Possibili misure di protezione:

- Comportamento personale: prestare attenzione su cosa si racconta e a chi lo si racconta.
- Rispettare le regole di sicurezza dell'azienda o dell'istituzione.
- Protezione degli apparecchi elettronici dall'accesso da parte di persone non autorizzate.

(Tentativo di) Reclutamento



Respingimento di un tentativo di reclutamento

Jeger si è accorto in tempo delle attività di spionaggio del servizio di intelligence straniero. Tuttavia, l'obiettivo di Frank Salov e di Linda di accedere alla tecnologia segreta della Grinder SA permane. Con la seduzione del CEO della Grinder SA da parte di Linda, lo spionaggio economico contro l'azienda prosegue.

Il tentativo di reclutare la persona obiettivo affinché collabori a lungo termine alle attività di intelligence, ossia all'acquisizione di informazioni confidenziali o segrete per il servizio di intelligence straniero o l'attore privato è un ulteriore passo avanti. Nella maggior parte dei casi la persona obiettivo è ora cosciente che un servizio statale d'intelligence o un attore privato sono alla base di tali attività. Se la persona obiettivo non coopera, l'autore tenta di sfruttare nuovamente i suoi punti deboli (soprattutto mediante l'uso di mezzi di pressione) o decide di ritirarsi.



... e nel caso di un autentico tentativo di spionaggio o di reclutamento

Se si constata un tentativo di spionaggio o un tentativo di reclutamento contro un'azienda, un'istituzione o se stessi, è importante che gli organi dell'azienda competenti per la sicurezza e, tramite questi, le autorità (SIC o polizia cantonale) siano immediatamente informati. Il SIC raccoglie e valuta indizi e provvede con discrezione all'esame e al trattamento del caso di spionaggio. In tal modo si possono impedire ulteriori deflussi di dati e danni. I dati raccolti sul caso di spionaggio e sul comportamento dell'autore contribuiscono a proteggere meglio e a sensibilizzare tempestivamente altre aziende e istituzioni sugli eventuali tentativi di spionaggio. Ciò consente al SIC di adeguare le sue misure di prevenzione all'attuale situazione di minaccia.

Redazione

Servizio delle attività informative
della Confederazione SIC

Chiusura redazionale

Giugno 2016

Indirizzo di contatto

Servizio delle attività informative
della Confederazione SIC
Papiermühlestrasse 20
CH-3003 Berna
E-mail: info@ndb.admin.ch

Copyright

Servizio delle attività informative
della Confederazione SIC, 2016

Video «Nel mirino»

www.sic.admin.ch