Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Service de renseignement de la Confédération SRC

Espionnage économique

Pourquoi un film sur l'espionnage économique ?

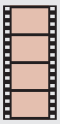
Le court-métrage « En ligne de mire » s'inscrit dans le programme de prévention et de sensibilisation Prophylax conduit par le Service de renseignement de la Confédération (SRC) depuis 2004. Il a été produit pour sensibiliser et informer les entreprises et institutions à l'espionnage économique.

Les techniques présentées dans le film pour accéder à des informations confidentielles ou secrètes sont emblématiques des méthodes employées par les services de renseignement étrangers ou des agents privés, même si la mise en œuvre peut parfois varier. Les explications suivantes sont destinées à sensibiliser le public aux subtilités de telles opérations d'espionnage en décortiquant les procédures et techniques à l'œuvre. Enfin, ce document propose des mesures de protection qui peuvent être prises pour réduire le risque d'espionnage.

Du targeting au recrutement : Les phases d'une tentative de recrutement

Les phases commentées ci-après ne sont pas clairement dissociables les unes des autres et peuvent se chevaucher. Elles dépendent de l'objectif de l'opération et de la personne cible, des méthodes employées et du temps à disposition ainsi que de l'environnement opérationnel. Certaines phases peuvent être très brèves, tandis que d'autres prennent beaucoup plus de temps. En fonction de l'opération, il peut s'écouler quelques semaines à quelques mois, voire plusieurs années entre le targeting et le recrutement d'une personne cible.

Targeting : recherche de la personne cible adéquate et définition des angles d'attaque



OSINT et acquisition clandestine d'informations

L'agent du service de renseignement étranger Frank Salov repère en la personne de Stefan Jeger, responsable de la division recherche et développement chez Grinder SA, une cible prometteuse lors de ses recherches sur Internet et dans les brochures de l'entreprise. Stefan Jeger a publié un profil personnel détaillé sur les réseaux sociaux, où il relate son activité d'écriture et ses séances de lecture publique. Frank Salov réunit du matériel visuel et des informations sur l'environnement et les habitudes de Stefan Jeger par des observations cachées. Il exploite ces informations pour dégager les angles d'attaque et les points faibles de Stefan Jeger.

L'agent glane des indices pouvant le mener sur la piste d'une personne cible intéressante, susceptible de fournir les informations recherchées ou un accès à ces informations. L'acquisition de données sur la personne cible intervient par la collecte ouverte ou clandestine d'informations :

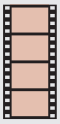
- **Open Source Intelligence (Osint)** désigne l'acquisition et l'analyse légales d'informations de sources publiques (sites Internet, journaux et revues, salons et manifestations publics, bases de données gratuites ou payantes, réseaux sociaux, etc.). Les réseaux sociaux comme Facebook et Linkedin livrent souvent une multitude d'informations sur une personne : profession, photos, relations, loisirs, contributions sur des forums en ligne, voyages, etc. Ces indications permettent d'établir le profil d'une personne cible avec ses habitudes, centres d'intérêt, contacts, passions et frustrations.

- Des moyens propres aux services de renseignement sont employés pour l'**acquisition clandestine d'informations** (surveillance technique ou observation physique de la personne cible par ex.). Il s'agit de repérer les déplacements habituels d'une personne, ainsi que ses contacts et activités.

Mesures de protection possibles :

Les personnes qui publient des informations (documents, photos, commentaires, etc.) décident de leur étendue et des détails qu'elles souhaitent livrer sur un projet, un produit, une institution ou une entreprise et ses collaborateurs.

Approche : établissement du contact avec la personne cible

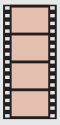


Le premier contact

Frank Salov exploite la passion de Stefan Jeger pour l'écriture et son désir d'être publié. En se faisant passer pour un agent littéraire, il éveille sa curiosité et gagne sa confiance afin de faciliter les contacts suivants.

Le premier contact avec la personne cible fait l'objet d'une préparation minutieuse. L'agent du service de renseignement ou l'agent privé exploitent les informations récoltées dans la phase de targeting au sujet des habitudes et des points faibles de la personne cible. Ces informations lui permettent de trouver le bon angle d'approche, sans risquer d'éveiller les soupçons de la personne cible. Pour y parvenir, l'agent du service de renseignement ou l'agent privé endossent souvent une identité d'emprunt.

« Cultiver » : mise en place d'une relation de confiance et de dépendance



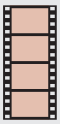
Exploitation du point faible comme un levier, une motivation ou une incitation

Frank Salov se sert de la passion de Stefan Jeger pour l'écriture pour arriver à ses fins. Il le complimente sur sa lecture et feint des intérêts communs. Lorsque Frank Salov lui fait miroiter une parution dans le magazine littéraire « Europe », Stefan Jeger y voit une opportunité unique de réaliser le rêve de sa vie. Frank Salov établit ainsi une relation de dépendance : Stefan Jeger a besoin de son aide et se sent redevable envers lui. Cette dépendance est encore renforcée lorsque Frank Salov propose à Stefan Jeger de devenir son agent littéraire au restaurant « Seesicht ».

Dès que la personne cible est identifiée comme une source d'informations potentielle et que le contact a été établi, l'agent cherche à développer une relation de confiance. Pour y parvenir, il se sert de centres d'intérêt ou de passions « communs ». Il utilise les points faibles de la personne cible comme des leviers. Ces leviers peuvent prendre la forme de services rendus, comme des cadeaux qui flattent l'ego ou encore la perspective d'un nouvel emploi. L'agent peut aussi essayer de collecter du matériel compromettant (moyens de pression ou de chantage) sur la personne cible (enregistrements vidéo ou photos de la personne cible en train de consommer de la drogue, d'avoir des relations extraconjugales ou d'accepter de l'argent). Cette exploitation des points faibles permet d'instaurer une relation de dépendance envers l'agent et d'exercer une pression croissante sur la personne cible.

Acquisition d'informations

L'art de la discussion



Technique éprouvée de conduite d'entretien

Frank Salov sait comment s'y prendre pour soutirer à Stefan Jeger des informations confidentielles sur son activité professionnelle et les projets de recherche de son entreprise Grinder SA.

- Il l'invite dans un restaurant haut de gamme, le « Seesicht », pour l'impressionner et lui faire croire qu'il a reconnu son talent littéraire et qu'il l'apprécie, qu'il dispose de moyens considérables ainsi que d'une certaine influence.
- Frank Salov félicite Stefan Jeger pour son premier jet pour la revue « Europe ». Il l'incite à continuer d'écrire.
- Quand Stefan Jeger explique à Frank Salov qu'il développe des rectifieuses cylindriques, ce dernier fait mine de ne rien y connaître pour faire parler son interlocuteur.

Mesures de protection possibles :

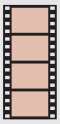
Il est important de définir les informations à protéger et non destinées au partage ou à la transmission à des tiers. Il s'agit notamment de données dont la divulgation ou la publication pourrait nuire à l'entreprise ou l'institution. Une certaine méfiance est donc de mise quand une personne s'intéresse à ce type d'informations.

Dès que l'agent a établi une relation de dépendance positive (invitation) ou négative (moyens de pression), il peut commencer à collecter les informations recherchées. Grâce à sa maîtrise des techniques d'entretien, il soutire à la personne cible toujours plus d'informations sensibles sans que cette dernière ne se doute qu'elle lui livre des indications clés.

Cyberespionnage

La numérisation galopante et l'imbrication entre économie et société augmentent la vulnérabilité des entreprises, institutions et particuliers aux cyberattaques. La protection des données électroniques ainsi que des réseaux et supports de communication revêt une importance capitale. A cet égard, le comportement de l'individu représente toujours le principal facteur de risque.

Ingénierie sociale (social engineering / subversion psychologique)



Hameçonnage ciblé (Spear phishing)

Frank Salov envoie un lien à Stefan Jeger pour qu'il remplisse un CV en ligne à l'attention de Monsieur Simon, l'éditeur du magazine littéraire « Europe ». En cliquant sur ce lien, Stefan Jeger installe sans s'en rendre compte un maliciel sur son ordinateur professionnel. Grâce à ce maliciel, Frank Salov accède au réseau de l'entreprise Grinder SA. Cette dernière exploite toutefois deux réseaux séparés. Les données sensibles en lien avec des projets de recherche et technologies de pointe sont sauvegardées sur un réseau séparé non connecté à Internet. Frank Salov n'a donc pas accès à ces données.

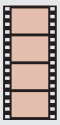
Mesures de protection possibles :

- Ne publier que les informations requises, notamment en ce qui concerne les noms, fonctions et photos des collaborateurs.
- Se méfier des e-mails dont l'expéditeur est inconnu, surtout quand ils contiennent des liens ou une pièce jointe.
- Il convient de définir des règles de sécurité et une culture de sécurité au sein de l'entreprise impliquant tous les collaborateurs.

La notion d'ingénierie sociale désigne la manipulation psychique de personnes dans le but de leur soutirer des informations confidentielles ou de les inciter à réaliser des actions précises. L'ingénierie sociale est souvent utilisée dans le domaine de la sécurité de l'information pour obtenir des noms d'utilisateur et des mots de passe, ainsi que pour infiltrer des virus et des chevaux de Troie. Les collaborateurs d'une entreprise sont abordés sur les réseaux sociaux

ou par e-mail sous de faux prétextes (offre d'emploi par ex.). Les attaques reposent sur les techniques d'hameçonnage (« phishing ») et d'hameçonnage ciblé (« spear phishing »). L'hameçonnage vise des adresses e-mail au hasard, tandis que l'hameçonnage ciblé vise des collaborateurs précis.

Smartphone



Infection d'un smartphone

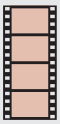
Pendant qu'ils mangent ensemble au restaurant « Seesicht », Frank Salov observe Stefan Jeger quand il saisit son code d'accès sur son portable. Grâce à une manœuvre de diversion, il accède au smartphone de Stefan Jeger et y installe un maliciel qui lui procure un accès total au contenu de l'appareil et le contrôle de toutes les fonctions. Il peut par exemple activer le microphone pour écouter toutes les discussions de Stefan Jeger avec son équipe de recherche.

Les capteurs et fonctions des smartphones (GPS, microphone, appareil photo, applications installées, répertoire, accès WiFi, signal Bluetooth, etc.) transmettent très souvent des données ou métadonnées sur l'utilisation de l'appareil et son détenteur - des données qui sont très facile d'exploiter. Une connexion physique au smartphone n'est pas impérativement nécessaire pour l'infecter. Il est aussi possible de le faire à distance.

Mesures de protection possibles :

- Verrouiller les appareils électroniques et ne pas les laisser sans surveillance.
- N'emmener en voyage d'affaires à l'étranger que les appareils électroniques et les documents absolument nécessaires.
- Ne jamais parler de sujets confidentiels sur son téléphone portable.
- Faire preuve de prudence en cas d'installation d'applications de sources inconnues.

Clés USB



Infection des appareils électroniques ou vol de données par clé USB

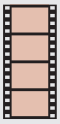
Linda connecte une clé USB à l'ordinateur portable du PDG de Grinder SA.

L'utilisation de clés USB est un autre moyen pour infiltrer des ordinateurs et d'autres appareils électroniques ou pour copier les données qui y sont sauvegardées. Une infection par un maliciel (virus, chevaux de Troie, etc.) sur clé USB ne prend que quelques secondes.

Mesures de protection possibles :

Ne pas utiliser d'appareils périphériques externes inconnus ou reçus en cadeau (clés USB, souris, disques durs externes, etc.). Ces cadeaux publicitaires peuvent être infectés par des maliciels.

La ruse du pot de miel (« honeypot »)



Séduction

Après l'échec des tentatives du service de renseignement étranger pour accéder aux informations secrètes convoitées par l'intermédiaire de Stefan Jeger, Linda séduit le PDG de Grinder SA pour accéder à son ordinateur portable.

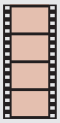
La ruse du pot de miel désigne une technique d'espionnage classique qui consiste à manipuler ou recruter une personne cible au moyen de faveurs sexuelles. La personne cible dévoile les informations souhaitées d'elle-même, ou elle fait l'objet de chantage sur la base de matériel compromettant.

(Le principe du « pot de miel » est aussi utilisée dans le domaine cyber et désigne un programme informatique ou un serveur utilisé pour attirer un attaquant potentiel et obtenir des informations sur ses techniques d'attaque, sans mettre en danger le réseau informatique à protéger.)

Mesures de protection possibles :

- Comportement personnel : faire attention à ce que l'on dit et à qui.
- Respecter les règles de sécurité de l'entreprise ou de l'institution.
- Protéger les appareils électroniques des accès non autorisés.

(Tentative de) Recrutement



Contrecarrer une tentative de recrutement

Stefan Jeger s'est rendu compte à temps de l'espionnage dont il était victime par un service de renseignement étranger. L'objectif de Frank Salov et Linda, à savoir accéder à la technologie secrète de Grinder SA, reste toutefois d'actualité. Avec la manœuvre de séduction du PDG par Linda, l'espionnage économique contre Grinder SA entre dans une nouvelle phase.

Le but d'un service de renseignement étranger ou d'un agent privé est d'exploiter une personne cible à long terme pour se procurer des informations confidentielles ou secrètes. Dans la plupart des cas, la personne cible se rend compte au bout d'un certain temps qu'elle est manipulée par un service de renseignement ou un agent privé. Si elle ne se montre pas coopérative, l'agent peut à nouveau exploiter ses points faibles (moyens de pression) ou décider de se retirer.

… et en cas de tentative avérée d'espionnage ou de recrutement

Si une tentative d'espionnage ou de recrutement est repérée contre une entreprise, une institution ou soi-même, il est important d'en informer sans délai les services de sécurité de l'entreprise, qui préviendront les autorités (SRC ou police cantonale). Le SRC collecte des indices et les analyse en toute discrétion afin d'éviter de nouvelles fuites de données ainsi que d'autres dommages. Les informations réunies sur les cas d'espionnage et les techniques des auteurs contribuent à améliorer la protection des autres entreprises et institutions en les sensibilisant en temps utile aux tentatives d'espionnage. Elles permettent aussi au SRC d'adapter ses mesures de prévention à la menace actuelle.

Rédaction

Service de renseignement de la Confédération SRC

Clôture de rédaction

Juin 2016

Adresse de contact

Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne
E-mail : info@ndb.admin.ch

Vidéo « En ligne de mire »

www.src.admin.ch