Document
C0 - Public
C1 - Interne
C2 - Restreint
C3 - Confidentiel
C4 - Secret

Forum des compétences
GT Cartographie des points d'entrée

Introduction

Ce book synthétise les **conclusions de l'ensemble des groupes de travail qui se sont tenus autour des scénarios de risques Cyber**. Il n'a pas vocation à être exhaustif mais donne **les bases pour identifier les points** d'entrée des scénarios d'attaques les plus classiques.
Il a été réalisé par le *Forum des Compétences* en partenariat avec la société EGERIE *et* avec la participation d'acteurs du monde des banques/assurances.

Plusieurs axes ont permis d'organiser les groupes de travail autour du sujet :

- *Catégorie de points d'entrée*
- *Liste des points d'entrée*
- ***Illustration d'attaque connues via ces points d'entrée***

La démarche et les finalités 1/2

- La démarche
  - L'objectif de ce groupe de travail est de créer un catalogue, pour la communauté de la banque/assurance, notamment les responsables sécurité ou la direction des risques, permettant de présenter des scénarios de risques cyber. Le groupe s'est concentré sur l'étude des points d'entrée et des impacts, notamment en s'appuyant sur des cas concrets, permettant ainsi de mettre en lumière une typologie d'incidents en face de chacun de ces points.
  - De ce fait, la démarche du groupe est de créer une boite à outil de points d'entrée que chacun pourra transposer dans son système d'information avec des impacts contextualisés, et ainsi d'aider à la présentation de scénarios cyber à des directions métier, à des auditeurs externes ou au COMEX.
  - La liste des points d'entrée a permis de mettre en évidence trois catégories, chaque représentant un niveau d'accès plus ou moins important au système d'information avec une approche en profondeur.

La démarche et les finalités 2/2

- Les exemples
  - Le groupe de travail s'est attaché à associer des exemples réels de cyberattaques auxquelles les entreprises ont été confrontées.
  - Ces exemples ont un rôle pédagogique et ne sont pas nécessairement exhaustifs ou détaillés.
  - Leur objectif est de rendre les scénarios réalistes avec des impacts financiers quantifiés par les entreprises touchées.
  - Ils sont systématiquement associées à une technique attaque issue du MITRE ATT&CK®.

- Choix et limitations
  - Certains systèmes ont été listés et mis de côté, car trop spécifiques et peu impactés. L'approche a été pragmatique et le travail s'est axé sur les scénarios et points d'entrée majeurs des attaques cybersécurité.
  - La cartographie met en évidence des points d'infection secondaires, il est à noter que ces points d'entrée ne sont pas prioritaires par rapport aux points d'entrée de primo infection.

Primo infection	Scénario
[I-11] Service en ligne (Publication du service)	*Un attaquant publie une fausse application mobile pour une banque en ligne du l'entreprise sur un store public. L'application imite la vraie application et permet à l'attaquant de collecter des données sensibles et de réaliser des virements frauduleux*
Illustration	
Brazilian Mobile Malware *Des attaquants ont créé une fausse application bancaire sur Google Play en vue de récupérer des informations sensibles sur les téléphones des personnes infectées.* *https://www.zdnet.com/article/brazilian-mobile-users-hit-with-banking-malware/*	
Impacts suite à l'attaque	
Nombre de personnes impactées : 2000	
Lien avec le MITRE ATT&CK®	
Deliver Malicious App via Authorized App Store *https://attack.mitre.org/techniques/T1475/*	

Explication de la structure

- 3 catégories de points d'entrée : Une approche en profondeur
  - Catégorie Physique/Humain :
    - Elle est afférente à des attaques nécessitant un accès physique (au système d'information) ou une liaison directe (appel téléphonique par exemple) avec une personne en lien avec le système d'information.
  - Catégorie Indirecte (Par rebond) :
    - Elle est afférente à des attaques exploitant la chaîne de sous-traitance (un éditeur logiciel par exemple) ou un utilisateur situé hors des locaux de l'entreprise (par exemple via un keylogger) dans le but d'accéder au système d'information. On considère le point d'entrée initial dans le système d'information, y compris dans le cas où la première infection a lieu chez un tier.
  - Catégorie Internet :
    - Elle est afférente aux attaques depuis Internet, exploitant des failles et des vulnérabilités permettant un accès direct sur le système d'information.

Utilisation des résultats

- *Utiliser les exemples dans les analyses de risques*
  - Les documents produits lors de ce groupe travail permettent d'identifier les modes opératoires des scénarios utilisés dans les analyses de risques.
  - Les exemples permettent également d'identifier le type d'impacts associé à des scénarios de risques.
  - La cartographie des primo infections est très utile pour mettre en évidence le point d'entrée des cyberattaques.

- *Fournir des exemples pédagogiques dans le but d'une présentation*
  - Les exemples illustrés permettent de rendre les scénarios de risques réalistes et compréhensibles par des non experts en cybersécurité.
  - Un article de presse est associé à un exemple.

- *Défier les dispositifs de sécurité existants*
  - S'assurer de la pertinence des dispositifs de sécurité en place au regard des scénarios proposés.
  - Identifier des points d'entrée non pris en compte dans l'analyse de risques.

Volumétrie des résultats

Catégorie	Primo-infection	Id
Internet	Mail avec des liens malveillants	I-01
	Site institutionnel (site vitrine, défacement)	I-02
	Site client (avec un accès client)	I-03
	API (exposées publiquement)	I-04
	Outil de connexion à distance	I-05
	Github	I-06
	Site Internet (intrusion, XSS, ...)	I-07
	Usage d'outils ou d'applications libres ou gratuites sur Internet	I-08
	Poste de travail : PC non-standard avec accès direct à Internet	I-09
	Usurpation de la société envers les clients (tel, mail, site,…)	I-10
	Service en ligne	I-11

Volumétrie des résultats

Catégorie	Primo-infection	Id
Indirecte (Par rebond)	Connexion accès distant utilisateur	R-01
	Connexion accès distant administrateur	R-02
	Connexion partenaire	R-03
	GTB (IOT, Maintenance de l'OT, Clim, …) ou SCADA	R-04
	Réseau wifi d'entreprise	R-05
	Compromission d’un sous-traitant	R-06
	Outils collaboratifs externalisés ou internes	R-07
	Exécutable portable	R-08
	Messagerie interne	R-09
	Usurpation d’un compte collaborateur	R-10
	Téléphones mobiles pro ayant un accès au réseau d'entreprise	R-11

Volumétrie des résultats

		Id
Physique / Humain	Câblage réseau	P-01
	Ménage ou Prestataires sensibles	P-02
	Ingénierie sociale	P-03
	Composant non vérifié (clef USB, …)	P-04
	DAB/GAB	P-05
	Port Ethernet lieu recevant du publique	P-06
	Port Ethernet interne	P-07
	Perte ou vol d'un matériel	P-08
	BIOS / UEFI	P-09
	Abus au niveau de l'accueil d'un bâtiment	P-10
	Menace physique directe sur un employé	P-11
	Chantage sur un employé	P-12
	Imprimantes multifonctions	P-13

Illustration de scénarios : Catégorie internet

Primo infection	Scénario
[I-11] Service en ligne (Publication du service)	*Un attaquant publie une fausse application mobile pour une banque en ligne de l'entreprise sur un store public. L'application faussée imite l'original et permet à l'attaquant de collecter des données sensibles et de réaliser des virements frauduleux*
Illustration	
Brazilian Mobile Malware *Des attaquants ont créé une fausse application bancaire sur Google Play en vue de récupérer des informations sensibles sur les téléphones des personnes infectées.* *https://www.zdnet.com/article/brazilian-mobile-users-hit-with-banking-malware/*	
Impacts suite à l'attaque	
Nombre de personnes impactées : 2000	
Lien avec le MITRE ATT&CK®	
Deliver Malicious App via Authorized App Store *https://attack.mitre.org/techniques/T1475/*	

Illustration de scénarios : Catégorie internet

Primo infection	Scénario
[I-04] API (exposées publiquement)	*Un attaquant exploite une vulnérabilité des API*
Illustration	
N26 Attack *Un attaquant a exploité une mauvaise configuration du trafic entre l'application et les serveurs N26 afin de se placer entre l'utilisateur et le serveur, prendre le contrôle de l'API et modifier les ordres de virement en temps réel.* *https://www.silicon.fr/la-banque-en-ligne-n26-8-mn-pour-inscrire-5-mn-pour-la-pirater-165948.html*	
Impacts suite à l'attaque	
Perte d'image lors d'une conférence publique (8 minutes pour s'inscrire, 5 minutes pour la pirater)	
Lien avec le MITRE ATT&CK®	
Exploit Public-Facing Application *https://attack.mitre.org/techniques/T1190/*	

Illustration de scénarios : Catégorie par rebond

Primo infection	Scénario
[R-06] Compromission d'un sous-traitant	*Le logiciel d'un éditeur a été compromis et des pirates ont installés des backdoor. Ces logiciels sont ensuite installés dans le S.I. de manière légitime par les équipes informatique et les backdoor sont exploités dans un but malveillant.*
Illustration	
Microsoft / Solarwind attack *Un groupe d'attaquants a intégré une backdoor dans une brique logicielle utilisée par Solarwind. Les attaquants ont utilisé cette backdoor pour accéder au code source de Microsoft, et d'autres clients de Solarwind.* *https://www.01net.com/actualites/les-hackers-de-solarwinds-vendent-des-gigaoctets-de-donnees-volees-en-ligne-2028464.html*	
Impacts suite à l'attaque	
Mise en vente du code source de certaines applications Microsoft sur le Dark Web	
Lien avec le MITRE ATT&CK®	
Exploit Public-Facing Application *https://attack.mitre.org/techniques/T1190/*	

Illustration de scénarios : Catégorie par rebond

Primo infection	Scénario
[R-04] Compromission d'un système industriel (GTB, IOT, …)	*Un attaquant compromet le sous-traitant réalisant la maintenance d'un système industriel (système OT) permettant d'accéder au système d'information.*
Illustration	
Target *Un attaquant compromet le système de ventilation (de la société Fazio Mechanical) de Target afin d'accéder au système d'information de Target (Bancaire, …), puis rebondit dans le système afin de voler des informations bancaires et les mettre en vente sur le Dark web.* *https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/*	
Impacts suite à l'attaque	
Nombre de comptes compromis : 110,000,000	
Lien avec le MITRE ATT&CK®	
Supply Chain Compromise *https://attack.mitre.org/techniques/T1195/*	

Illustration de scénarios : Catégorie Physique / Humain

Primo infection	Scénario
[P-01] Câblage réseau	*Des attaquants se connectent au réseau via une prise réseau située à l'intérieur de l' entreprise.*
Illustration	
Banque de l'Europe de l'Est *Des attaquants se sont introduits dans les locaux de la banque et ont branché des outils de hacking (clé USB piégée, Raspberry Pi, …) dans le but de récupérer des informations.* *https://www.zdnet.fr/actualites/plusieurs-banques-d-europe-de-l-est-perdent-des-dizaines-de-millions-de-dollars-dans-un-piratage-hollywoodien-39877811.htm*	
Impacts suite à l'attaque	
Perte de dizaines de millions de dollars en virement frauduleux	
Lien avec le MITRE ATT&CK®	
Hardware additions *https://attack.mitre.org/techniques/T1200/*	

Illustration de scénarios : Catégorie Physique / Humain

Primo infection	Scénario
[P-03] Ingénierie sociale	*Des attaquants envoient des mails frauduleux à des employés en se faisant passer pour la direction du groupe. Les mails demandaient à l'employé visé de réaliser des virements pour le groupe.*
Illustration	
Pathé *Des attaquants envoient des mails frauduleux à des employés en se faisant passer pour la direction. Cette attaque leur a permis de récupérer 19 millions d'euros.* *https://www.leparisien.fr/faits-divers/pathe-victime-d-une-fraude-de-plus-de-19-millions-d-euros-10-11-2018-7939638.php*	
Impacts suite à l'attaque	
Perte de 19 millions d'euros	
Lien avec le MITRE ATT&CK®	
Phishing *https://attack.mitre.org/techniques/T1556/*	

Conclusion

La mise à disposition de cette boite à outils s'inscrit dans un processus d'industrialisation de la cartographie et des analyses de risques cyber. Le catalogue fournit est amené à être enrichi avec le temps et les contributions afin d'apporter une certaine exhaustivité même si ce n'est pas son objectif premier.

Le livrable peut être utilisé dans un but d'identifier un socle de scénarios qu'il faut systématiquement étudier, dans les analyses de risques, dans la construction d'un plan stratégique cyber et/ou dans le cadre du contrôle permanent. De même, cette démarche est utilisable dans les processus d'évaluation des systèmes internes comme dans une démarche d'évaluation des tiers.

Les exemples fournis dans la boite à outils sont illustrés avec des critères quantificatifs des risques cyber, et permettent ainsi d'apprécier les impacts réels.

Il est important de maintenir la cohérence et la véracité de la boite à outils, notamment avec un processus de revue régulière **(par exemple annuelle)**, ainsi qu'avec une mise en application sur son propre système d'information et d'en mesurer les écarts.

Pour aller plus loin, une boite à outils similaire peut être réalisée pour les risques informatiques accidentels (erreur humaine, …). Il est de même pour les technologies d'exploitation et les systèmes IoT de plus en plus répandus dans les systèmes d'informations d'entreprise.

Annexe