Mini Rapport :

Tableau des 10 attaques choisi :

Titre et dates	Cible	Contexte	Avant l'attaque	Dommages	Actions	Bonnes pratiques
MGM Resort : Septembre 2023	L'entreprise MGM Resort	Sans contexte particulier	Aucune attaques permettant de prévoir cette dernière	Gigantesque perte financière, impossibilité d'utiliser les machines à sous, les ascenseurs, et les serrures de chambres	Au lieu de répondre au attaquent ou de payer la rançon ils ont préférer faire la sourde oreille, mais après 2 semaines ils ont payer	S'assurer de ne pas divulguer d'informations confidentiel sans être sur que l'ont s'adresse au bon destinataire
Meduza newspaper: Septembre 2023	Le journal Meduza newspeper	Guerre entre la Russie et l'Ukraine	Multiples piratages russes afin de récolter des données à travers les différent média étranger pour prendre l'ascendant sur l'Ukraine	Récolte de données sensible notamment car la journaliste était présente à une réunion sur le conflit Ukraine Russie	Enquête de différents services de renseignement afin de comprendre et anticiper les futurs attaques	Veiller à ne pas conserver sont téléphone lors de conversation sensible en cas de hacking
Czech banks : Aout 2023	La banque russe Czech banks	Guerre entre la Russie et l'Ukraine	Multiples piratages russes afin de récolter des données à travers les différent média étranger pour prendre l'ascendant sur l'Ukraine	Ralentissement du site de la banque mais pas de pertes monétaires pour les clients	Ils ont limiter le débit sur le réseau pour ralentir les attaques et ont attendu que l'attaque se termine	Disposer d'une installation capable de traiter un grande nombre de donnés et ralentir le débit sur le réseau
Routeur espion : Septembre 2023	Différentes installation sensibles au états unis	Tension entre les Etat Unis et la Chine	Le groupe de hacker chinois « BlackCat » à intercepter des livraisons de routeurs Cisco et les a pirater	Vol de propriétés intellectuel, espionnage	Des équipements corrompu ont était analyser et un correctif de la part de Cisco à permis d'en trouver d'autres qui on par la suite était remplacer par de plus récents et moins vulnérables	Ne pas faire confiances à un produit neuf et vérifier les différentes communication en place sur sont réseaux pour déceler d'éventuel défaillance
Op Aurora : 2009/2010	Différentes entreprises de la tech américaine mais principalement Google	Tension entre les Etat Unis et la Chine	Avant l'attaque, les attaquants ont probablement mené des activités de reconnaissance approfondie pour identifier les vulnérabilités et les points faibles dans les systèmes des cibles. Les techniques d'ingénierie sociale et de spear phishing ont probablement été utilisées pour obtenir un accès initial.	Les dommages de l'opération Aurora ont été significatifs, avec des pertes de propriété intellectuelle, des informations sensibles compromises, et des répercussions sur la confiance en ligne. Les entreprises touchées ont également dû faire face à des coûts importants pour remédier aux vulnérabilités exploitées.	Les entreprises cibler on essayer de poursuivre les différents acteurs de cette attaques mais sans résultats, et on considère que cette opération est un déclencheur du départ de Google du territoire chinois	Veiller à garder sont parc informatique à jour et effectuer de nombreux contrôles et tests de sécurités afin de prévenir d'une éventuelle intrusion
Op Olympic Games : 2006	Les centrales nucléaire Iraniennes notamment celle de Natanz	Préoccupations internationales croissantes concernant le programme nucléaire iranien et les craintes qu'il puisse être utilisé à des fins militaires	Les agences de renseignement américaines, en collaboration avec leurs homologues israéliennes, ont élaboré des stratégies et des armes informatique spécifiques comme Stuxnet pour cibler les infrastructures nucléaires iraniennes.	L'impact précis de l'opération Olympic Games sur le programme nucléaire iranien est difficile à évaluer de manière définitive. Cependant, Stuxnet a été largement considéré comme ayant réussi à ralentir le programme d'enrichissement de l'uranium de l'Iran.	L'opération Olympic Games a été maintenue secrète pendant un certain temps, mais elle a finalement été divulguée dans les médias en 2010. Cela a suscité un débat mondial sur l'utilisation des armes informatique et a conduit à une prise de conscience accrue des implications potentielles de la cyberguerre.	L'opération Olympic Games souligne la nécessité de développer des normes et des règles internationales concernant la conduite dans le cyberespace. Elle souligne également l'importance de la sécurité informatique pour protéger les infrastructures critiques contre de telles attaques.
Le hack de Adobe : Octobre 2013	L'entreprise Adobe System	Cette attaque a eu lieu en Octobre 2013, peu après la transition d'Adobe sur Cloud. Le groupe ayant commis cette attaque se fait connaître sous le nom de 'Syndicat'.	Malgré que les méthode utiliser par les pirates n'ont pas était rendu totalement publique on sait que plusieurs hacker ont infiltré les systèmes informatiques d'Adobe grâce à du phishing pour ainsi tromper les systèmes internes et accéder au différentes donnés utilisateur	Acquisition des informations de 38 millions d'utilisateurs y compris des identifiants et des mots de passe, des informations sur les partenaires commerciaux d'Adobe, des informations financières et de facturations. Cette attaque a également eu d'énormes impacts sur la confiance et la réputation d'Adobe, en plus des millions de dollars qui ont dû être utilisés pour les dédommagements et le renforcement de la sécurité.	Adobe a immédiatement réagi en informant les utilisateurs concernés et en prenant des mesures pour renforcer la sécurité de ses systèmes. De plus, la société a collaboré avec les forces de l'ordre pour retrouver les auteurs de l'attaque.	Ne pas confier de log de connexion n'importe qui et être sur de notre interlocuteur et ne pas ouvrir de liens non sûr. Être également très vigilent, faire des test réguliers et ne pas prendre les attaques informatique à la légère.
Hack de la Bangladesh Bank : 2016	La Bangladesh Bank	Sans contexte particulier	Le groupe nord coréen Lazarus avait déjà implanter des backs doors dans le réseau via du social engineering qui leurs on permis d'avoir accès à une imprimante au centre des transactions monétaire importante de la banque	Perte financière de plus d'1 million de dollars	Les équipes de la banque n'ont pu s'apercevoir de l'attaque que quelques jours plus tard mais on finalement pu annuler la transaction, ils ont ensuite fait analyser leurs réseau par des professionnels qui ont repérer et éliminés la moindre trace des attaquent pour qu'ils ne puissent plus intervenir sur leurs réseau	Ne pas confier de log de connexion n'importe qui et être sur de notre interlocuteur et ne pas ouvrir de liens non sûr
Opération PayBack : 2020	Différentes institutions américaines tel que Recording Industry Association of America (RIAA), Motion Picture Association (MPAA)	Différentes institutions américaines ont mené des actions juridique envers le site de partage de fichier BitTorrent (aussi appeler « The Pirates Bay ») pour les forcer à cesser leurs activité	Après que l'affaire ai était mise publique les cyber hacktiviste Anonymous ont voulu mené des opérations envers ces différentes institutions pour exprimer leur opposition et les frapper dans un domaine ou ils n'ont que très peu d'emprise	Les attaques ont réussi à perturber temporairement les services en ligne de certaines entreprises, entraînant des périodes d'indisponibilité. Cependant, cela a également suscité des critiques en raison de la nature illégale des attaques DDoS.	Les entreprises ciblées par les attaques DDoS ont mis en place des contre-mesures pour atténuer l'impact des attaques. Cela inclut des améliorations de l'infrastructure réseau, des services de sécurité en ligne, et des partenariats avec des fournisseurs spécialisés dans la mitigation des attaques DDoS.	Il faut mettre en place une architecture robuste, utilisés des services spécialiser en attaques DDOS, utiliser des pare-feu capable de détecter des attaques, mettre en place des plans de décence en cas d'attaques, rediriger les utilisateurs légitime vers de services fonctionnels et bloquer les requêtes frauduleuses
Wannacry : Mai 2017	Différents appareils réseaux d'installation sensible à travers plus de 150 pays	Sans contexte particulier	Peut de temps avant une faille de sécurité avait était détecter dans le protocol SMB des OS Windows non mis à jour (on l'a appelé Eternal Blue), par la NSA et les Etats Unis et a était rendu publique grâce au groupe de hackers ShadowBrokers	Il a eu de très nombreux dommages, que ce soit des pertes financière inestimable, des retard et annulation d'intervention médical, dommage de la réputation des entreprise touché	L'ampleur de l'attaque a conduit à une réponse d'urgence à l'échelle mondiale. Les fournisseurs de sécurité, les entreprises technologiques et les gouvernements ont collaboré pour contenir la propagation du ransomware et élaborer des solutions de détection et de prévention.	Les bonnes pratiques à suivre sont la sauvegarde régulière de ses donnés, la sensibilisation, la mise à jour de ses différentes solutions informatique, le contrôle d'accès, la mise en place de plan permettant de faire face à une attaque

Synthèse du déroulement des 5 attaques choisi :

- MGM Resort :

Septembre 2023 sans contexte particulier, attaque par social engineering (vishing, phishing par téléphone) du Casino MGM Resort par le groupe Russe AlphV (BlackCat). L'attaque a était préparer en amont par les attaquent grâce à des recherches sur leurs cibles et le fonctionnement informatique du casino, ils ont par la suite contacté le service informatique du casino en leur demandant de désactiver la double authentification d'un employer choisi à travers LinkedIn, ils ont donc pu infiltrer le réseau et le crypter grâce à un ransomware. Après cela les hackers vont tenter de rentrer en contact le groupe MGM Resort mais ces derniers on préférer ne pas répondre et tout simplement bloquer l'entièreté de leur réseau, ce qui va entrainer la panne d'un grand nombre de machines à sous, l'incapacité d'ouvrir certaine serrure, et le non accès au parking et à l'ascenseur. Le groupe de hacker a donc décider de continuer son attaque et est parvenu à bloquer le reste des machines à sous. A ce stade le groupe MGM reste très silencieux malgré que les hackers aient confirmer avoir fais sortir les données de milliers d'utilisateurs et sont prés à les publier sur des sites de leak. Tout en sachant que MGM Resort aurait déjà perdu plus de 100 millions de dollar depuis le début de l'attaque. L'affaire est encore en cours malgré que des rumeurs affirme que MGM Resort compte payer la rançon demander par le groupe AlphV.

- Meduza news Paper :

Galina Timchenko, propriétaire de l'agence de presse russe Meduza, a été la cible d'une attaque par le logiciel espion Pegasus, marquant le premier cas connu de cet outil puissant utilisé contre une cible russe significative. L'attaque a eu lieu alors que Timchenko était en Allemagne pour une réunion entre différent journaliste russe. L'infection semble avoir été effectuée via une vulnérabilité zero-click de l'application Apple HomeKit et IMessages, mettant en évidence les risques posés par des outils de surveillance sophistiqués. Les chercheurs n'ont pas pu identifier l'auteur de l'infection, mais des suspects incluent la Russie et ses voisins. Cette attaque souligne la nécessité d'actions gouvernementales et de réglementations internationales pour contrer de telles menaces, car la réponse ne peut pas reposer uniquement sur les utilisateurs individuels ou les entreprises comme Apple. Elle met également en lumière les dangers potentiels pour la démocratie, la vie privée et la liberté des journalistes, soulignant l'importance de mesures plus larges pour faire face à ces défis croissants.

- Hack de la Bangladesh Bank :

L'attaque contre la Bangladesh Bank par le groupe Lazarus a débuté par des campagnes de phishing sophistiquées visant les employés de la banque. À l'aide d'informations d'identification obtenues, les pirates ont infiltré le réseau interne, exploitant des vulnérabilités pour échapper aux défenses de sécurité. Une analyse approfondie du système SWIFT a permis aux attaquants de cibler spécifiquement cette infrastructure financière.

Développant un malware sur mesure, Lazarus a orchestré des transactions frauduleuses, altérant subtilement les détails des transferts vers des comptes aux Philippines. Malgré quelques erreurs, une partie des fonds a été transférée avec succès. Les pirates ont mis en place des stratégies pour éviter la détection, manipulant les journaux de sécurité et prolongeant leur présence non détectée.

La fraude a été découverte lorsqu'on a remarqué des erreurs de frappe dans les détails des transactions. Les autorités ont réagi rapidement pour bloquer d'autres transactions et ont lancé des enquêtes. Cette attaque a exposé des lacunes dans la sécurité de la Bangladesh Bank, soulignant la nécessité d'améliorer les protocoles de protection contre les intrusions et de renforcer la résilience face à de telles attaques sophistiquées

- Wannacry :

L'attaque Wannacry a été lancée en mai 2017 et s'est propagée rapidement dans le monde entier. Elle a exploité une vulnérabilité dans le système d'exploitation Windows appelée Eternal Blue, qui était initialement une faille de la NSA. Une fois qu'un système était infecté, le ransomware chiffrait les fichiers de l'utilisateur et demandait le paiement d'une rançon en bitcoin pour la clé de déchiffrement.

Wannacry a utilisé une technique d'auto-propagation, se propageant de manière virale à travers les réseaux en exploitant la vulnérabilité Windows sans aucune intervention de l'utilisateur. Cette caractéristique a contribué à la rapide diffusion de l'infection.

L'attaque a ciblé principalement les organisations utilisant des versions non mises à jour de Windows, soulignant l'importance de maintenir les systèmes à jour pour prévenir de telles attaques. Les secteurs de la santé et des services publics ont été particulièrement touchés, mettant en lumière les risques liés aux infrastructures critiques.

Les dommages causés par Wannacry ont été substantiels, avec des pertes financières importantes pour les organisations touchées. L'attaque a également mis en évidence la nécessité d'une collaboration mondiale pour contrer les cybermenaces, car de nombreuses organisations et gouvernements ont dû travailler ensemble pour atténuer les effets de l'attaque et identifier les coupables.

- Opération Olympic Games :

L'opération Olympic Games a utilisé une approche multifacette, avec le développement du ver informatique Stuxnet comme point central. Pour infecter le réseau iranien, des techniques de cyber espionnage ont été employées pour recueillir des renseignements sur les installations nucléaires. Stuxnet, une fois introduit via un périphérique infecté, exploitait des vulnérabilités zero-day dans les logiciels et systèmes d'exploitation, permettant une propagation rapide. Le ver ciblait spécifiquement les systèmes de contrôle industriel (ICS), en particulier les centrifugeuses d'enrichissement de l'uranium, en utilisant des mécanismes sophistiqués pour manipuler les paramètres des machines. L'utilisation de vulnérabilités zero-day souligne la complexité de l'attaque, car ces failles étaient alors inconnues et non corrigées. L'objectif était de perturber le programme nucléaire iranien en provoquant des défaillances matérielles via des attaques informatiques.

Sources et autres :

https://www.techtarget.com/searchsecu...

https://www.mandiant.com/resources/bl...

https://www.404media.co/inside-mgms-h...

https://sec.okta.com/articles/2023/08...

https://twitter.com/MGMResortsIntl/st...

https://twitter.com/MGMResortsIntl/st...

https://twitter.com/MGMResortsIntl/st...

https://twitter.com/VitalVegas/status...

https://www.reviewjournal.com/busines...

https://fr.pokernews.com/news/2023/09...

https://investor.caesars.com/static-f...

https://cybernews.com/news/mgm-caesar...

https://explore.avertium.com/resource...

https://www.theregister.com/2023/09/1...

https://www.wired.com/story/mgm-ceasa...

https://www.vox.com/technology/2023/9...

https://www.numerama.com/cyberguerre/...

https://www.intrinsec.com/alphv-ranso...

https://www.ic3.gov/Media/News/2022/2...

https://nypost.com/2023/09/14/caesars...

https://apt.etda.or.th/cgi-bin/showca...

https://twitter.com/JacobsVegasLife/s...

https://twitter.com/JacobsVegasLife/s...

https://twitter.com/joetidy/status/17...

https://twitter.com/JacobsVegasLife/s...

https://twitter.com/CBSEveningNews/st...

https://twitter.com/rawsalerts/status...

https://twitter.com/anthonyoren/statu...

https://twitter.com/BretBev19/status/...

https://twitter.com/DiRealDan/status/...

https://twitter.com/aejleslie/status/...

https://twitter.com/Matrixwave/status...

https://twitter.com/LasVegasLocally/s...

https://twitter.com/vxunderground/sta...

https://www.washingtonpost.com/technology/2023/09/13/pegasus-infection-meduza-founder/

https://www.bbc.com/news/technology-66784894

https://www.securityweek.com/chinese-gov-hackers-caught-hiding-in-cisco-router-firmware/

https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-10/231004_Significant_Cyber_Events_List.pdf?VersionId=4b6vWQnhIXGDIZ0mc0MEZtqszjj2qCcF

https://www.youtube.com/watch?v=mH5fXUZyfpE&ab_channel=Sylvqin

https://securite.developpez.com/actu/348688/MGM-Resorts-est-de-nouveau-en-ligne-apres-une-enorme-cyberattaque-l-attaque-pourrait-avoir-coute-80-millions-de-dollars-a-l-exploitant-du-casino-de-Vegas/

https://www.lesechos.fr/idees-debats/cercle/wannacry-la-cyber-securite-le-talon-dachille-de-lentreprise-1010592

https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html

https://en.wikipedia.org/wiki/Operation_Olympic_Games

https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

https://www.bbc.com/news/stories-57520169

https://www.youtube.com/@Sylvqin

https://www.youtube.com/@Underscore_