Ameloot Yoan
Folliet Martin

Rapport d'info 002

La faille de sécurité Amazon Ring

SOMMAIRE :

1)Présentation de Ring

Ring est une entreprise fondée en 2013 par Jamie Siminoff, un jeune entrepreneur.
Cette compagnie a fait un financement participatif pour un produit appelé Doorbot, un objet remplaçant la sonnette classique des foyers par un objet connecté au wifi de la maison, permettant aux utilisateurs de monitorer les visiteurs sonnant chez eux, sur leur téléphone à l'aide d'une application. Ce produit inclut une caméra et un micro, rendant les interactions entre l'invité et le propriétaire plus fluide.

En 2015, Ring met en vente un nouveau produit, la "stick-Up Cam", une caméra IP, reprenant les mêmes principes que Doorbot, mais avec une recharge solaire et une détection de mouvement.

C'est avec ces produits qu'Amazon décide d'acquérir Ring en 2018, en estimant cette entreprise entre 1.2 et 1.8 milliards de dollars. Offrant maintenant une variété de produits axé dans la sécurité intérieure et extérieure des propriétés, à l'aide de caméras, de micros et de services aidant les utilisateurs à mieux surveiller leurs foyers, à distance, en utilisant la wifi des maisons.

Cependant, ces produits, accédant à la vie privée des particuliers, ont été la cible des hackers qui voyaient une opportunité de s'introduire facilement chez ces personnes, pour des raisons diverses et variées.
Ces personnes ont fini par trouver des failles dans les produits d'Amazon Ring, créant ainsi de nombreux problèmes.

2) Les failles de sécurité d'Amazon Ring

C'est pendant l'année 2019 que Amazon Ring a été sujet à de nombreux problèmes de sécurité. Ces problèmes, au nombre de trois, ont été découverts au courant de l'année, et ont soulevé beaucoup de questionnements sur la capacité de Ring à gérer la sécurité de ses clients.
Ces problèmes ont touché la vie privée des utilisateurs, attaqués par une grande variété de personnes mal intentionnées : pédophiles, maîtres chanteurs, etc...

2.1) Première faille découverte : Janvier 2019

C'est en Janvier 2019 que la première faille fut découverte. Elle concerne l'entièreté des produits Ring. En effet, il a été trouvé que depuis 2016, une équipe de recherche et développement de Ring, située en Ukraine, avait un accès illimité à un dossier d'Amazon S3 cloud storage, permettant de visualiser toutes les vidéos créées par les produits de Ring, autour du monde, vidéos qui n'étaient même pas encryptées.
Cette même équipe avait aussi l'accès à une autre base de données permettant de récupérer les données de comptes (nom / email, etc...) et de les lier sur les vidéos, permettant aux employés d'espionner les clients de Ring, 24h/24, en cherchant une simple adresse mail.
Ce problème a aussi été accentué par le simple fait que personne ne savait qui avait exactement accès à ces dossiers, rendant cette faille plus importante.

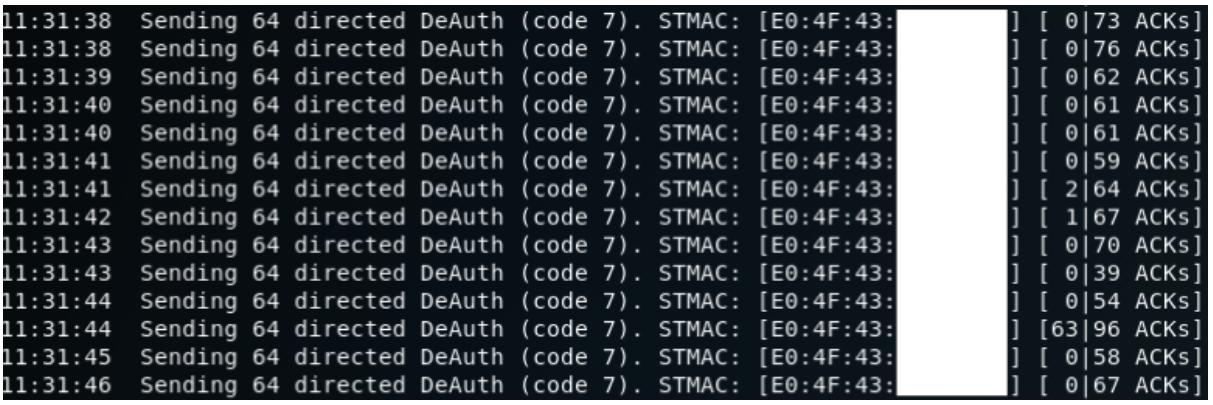
La raison d'un tel problème a été découverte sur le fait qu'un ingénieur avait demandé l'accès à ces vidéos, pour faciliter le travail de recherche sur les logiciels de Ring. Demande qui a ensuite été acceptée par M.Siminoff Sminignov.

Aujourd'hui, ce bureau en Ukraine a été fermé, rendant cette faille obsolète. Cependant, nous n'avons aucune certitude si ce problème a été répliqué autre part.

2.2) Deuxième faille découverte: juillet 2019

Peu de temps après la première faille, PCMag un journal en ligne, avait demandé à BitDefender, une entreprise de cybersécurité d'examiner des objets IoT en incluant les sonnettes vidéos de Ring.
Il a été découvert que ces objets pouvaient mettre à découvert le mot de passe wifi d'un utilisateur, ouvrant la porte au routeur et autres appareils sensibles du foyer aux attaques de hackers.

En effet, Doorbell est un objet relié à une application mobile, ces derniers communiquent entre eux en utilisant des API. Cette communication pouvait alors être falsifiée en envoyant en boucle le processus de désactivation de l'appareil sur l'application. Après un certain temps, l'appareil va se déconnecter, obligeant alors à l'utilisateur légitime de prendre action.



On peut voir ici un exemple ou l'attaquant envoie en boucle des demandes de désauthentification

Ce processus n'était accepté que par une adresse MAC spécifique, celle de l'utilisateur légitime. Mais ce genre de ressource est simple à trouver et à imiter avec les bons outils.
Une fois que l'utilisateur remarque que la sonnette est déconnectée, il entrait à nouveau le mot de passe pour la sonnette via une communication HTTP (et non https), exposant ainsi le mot de passe, facilement récupérable grâce à des logiciels comme wireshark.

Exemple de paquet récupéré, contenant les informations confidentielles du Wi-Fi

Fort heureusement, Amazon a très vite réglé ce problème, en cryptant les données communiquées entre l'utilisateur légitime et l'objet.

Une fois que cette faille a été réglée, Amazon l'a révélée publiquement en Novembre 2019. Cette faille, une fois avoir été dévoilée, a amené une nouvelle vague de cyberattaques sur Ring, créant la troisième faille qui a été rapidement découverte.

2.3) Troisième faille découverte: décembre 2019

La faille principale des produits Ring, qui a été découverte en Décembre 2019, a été celle qui a mis Ring dans un grand scandale au niveau de la sécurisation privée. Cette faille a grandement surpris les clients d'Amazon, en particulier aux États Unis. En effet, Amazon étant une des entreprises les plus importantes en Amérique en termes de développement de produits de gamme d'objets vendus comme sécurisés et sécurisant, ils avaient la confiance de nombreux utilisateurs.
Cette faille à permis à un nombre incalculable de personnes de se rendre compte à quel point leur vie privée est extrêmement fragile bien que l'on essaie de la protéger. Elle a aussi permis au gens de se rendre compte à quel

point il ne faut pas lésiner sur sa protection virtuelle afin que les personnes mal intentionnées ne puissent pas nous nuire.
Cette faille a été celle qui à fait le plus polémique du fait qu'un nombre assez conséquent de familles victimes des attaques s'en sont sorties terrorisées, leur intimité ayant été atteinte et leur sentiment de sécurité réduit à néant par un inconnu, alors qu'il se trouvaient dans le lieu où ils se trouvaient le plus en sécurité : leur maison.

Certains hackers malintentionnés ont réussi, en Décembre 2019, ayant appris à propos de la faille dévoilée en Novembre 2019, à avoir accès à plusieurs caméras de sécurité Ring, et on ainsi pu utiliser les enceintes intégrées aux caméras afin de parler directement aux habitants ayant installé ce dispositif de sécurité. Même si la plupart des hackers ont juste fait cela afin de surprendre leurs victimes, notamment en les insultant, ou simplement en leur demandant ce qu'ils regardaient à la télé, certains cas ont étés plus loin, notamment dans le cas où le hacker (qui, selon certaines rumeurs, serait un pédophile) s'en est pris à une jeune fille de seulement 8 ans, en lui disant qu'il était son meilleur ami, ainsi que le père noël. Ce dernier lui a même demandé de saccager sa maison.
Dans d'autres cas, les hackers s'en sont pris à des personnes âgées, leur faisant des menaces de mort, leur demandant des rançons afin d'éviter la mort.

Après investigation, des forums criminels ont été démasqués, ces derniers proposaient des logiciels pouvant exploiter les appareils Ring, logiciels qui ont été utilisés lors de certaines cyberattaques, et qui étaient disponibles pour des sommes très abordables, avoisinant 5 dollars.
Un podcast sur Discord, nommé NulledCast, à même été trouvé, podcast sur lequel était diffusé en direct certains des incidents.
Cependant, pour des raisons de sécurité, l'origine, l'utilisation, leurs moyens d'exploiter une faille et le nom de ces logiciels ont été cachés afin d'éviter que d'autres personnes malintentionnées n'essayent de trouver d'autres failles afin de les exploiter.

Suite à cette polémique, Ring a conseillé à tous les utilisateurs de changer leurs mots de passe (Wi-Fi & Application Ring) pour des mots de passe plus forts, et surtout d'activer la double authentification afin de renforcer la sécurité des appareils, sachant que dans la grande majorité des cas, la double authentification n'avait pas été activée, les utilisateurs jugeant qu'il n'était pas nécessaire de l'activer.
Afin d'éviter que des problèmes ne puissent ressurgir, Ring à imposé aux utilisateurs d'activer la double authentification afin de pouvoir utiliser leur matériel de vidéosurveillance.

Les cybercriminels ont réussi à avoir accès aux caméras en se connectant au compte Ring ou alors au Wi-Fi des victimes, données qu'il pouvaient facilement récupérer lors de brèches de données.

Afin d'éviter cela, en plus d'activer la double authentification, il a été conseillé à tous les utilisateurs de changer leurs mots de passe, pour des mots de passes longs, uniques, et à forte sécurité, c'est à dire en augmentant l'aspect aléatoire du mot de passe, en utilisant des caractères spéciaux, des chiffres, en évitant d'utiliser des mots de passe lisibles, etc...

Un test, réalisé en Décembre 2019 aurait alors révélé que les logiciels de Ring ne contenaient pas les caractéristiques de sécurité basiques, notamment en autorisant d'accéder à un compte Ring depuis n'importe quelle adresse IP, quelle que soit sa provenance, sans même en notifier l'utilisateur légitime.

Aussi, les métadonnées fuitent facilement du réseau "Nextdoor" (service de réseautage social orienté sur le voisinage), et ces données combinées avec les données publiques concernant les villes, sont fréquemment suffisantes pour découvrir la location d'une caméra Ring "outdoor", ce qui simplifie encore plus l'exploitation de cette faille.

Pour donner un exemple, pendant une expérience de ce type, un homme, qui se fait appeler "Gizmodo" a réussi à localiser 20 000 appareils Ring grâce à cette technique, en utilisant les données qu'il avait pu scrapper depuis l'application de "Nextdoor" sur une période d'un mois.
Des chercheurs ont quant à eux réussi à localiser 440 000 appareils en utilisant des données datées au minimum de 2016.

Suite à cette polémique, l'affaire à vite été prise en charge par Ring, afin de mettre un terme aux exploitations de cette faille.

Ils se sont bien évidemment exprimés, au travers de porte-paroles, publiquement, afin de rassurer la population :

" Récemment, nous avons été mis au courant d'un incident lors duquel des individus malveillants ont obtenu des informations d'identification de certains utilisateurs de Ring (par exemple nom d'utilisateur et mot de passe), depuis un service externe à Ring. Ces informations ont ensuite été réutilisées pour se connecter à certains comptes Ring. Malheureusement, lorsque le même nom d'utilisateur et le même mot de passe sont réutilisés sur plusieurs services, il est possible que des individus malveillants aient accès à plusieurs comptes. Dès que nous avons eu connaissance de l'incident, nous avons pris les mesures appropriées pour bloquer rapidement les pirates ayant affecté les comptes Ring identifiés et les utilisateurs affectés par cet incident ont été contactés. Nos utilisateurs doivent toujours veiller à leur mot de passe et nous encourageons les clients de Ring à changer leurs mots de passe et à utiliser l'authentification à double facteur. "

Afin d'inciter les utilisateurs d'activer la double authentification, et de montrer aux utilisateurs à quel point ils sont aussi acteurs de leur propre sécurité, les portes-paroles se sont aussi exprimés :

"*La confiance de nos utilisateurs est capitale pour nous et nous prenons la sécurité de nos produits très au sérieux. Notre équipe de sécurité a enquêté sur cet incident et nous n'avons aucune preuve d'une intrusion non autorisée ou d'une faille dans les systèmes ou dans le réseau de Ring*".

Selon Ring, leurs serveurs n'auraient pas été la cible d'une brèche de données, cependant, ce n'est pas rare que des personnes mal intentionnées ne récoltent des données depuis des failles de données d'autres firmes, et qu'elles en créent des listes. Ainsi, ils peuvent essayer de gagner l'accès à d'autres services en réutilisant les données qu'ils ont pu extraire de ces brèches.

3) Les plaintes des victimes de la faille de décembre

Aux États-Unis, quinze familles ont lancé des poursuites contre la filiale d'Amazon en raison d'une faille de sécurité, sous forme d'une action collective.

Voici deux exemples sur l'utilisation de ces attaques:

Le cas LeMay :

Pour donner des exemples des cas d'intrusion des familles ayant déposé plainte, le plus connu est celui de la famille LeMay.

La mère d'Alyssa, Ashley LeMay, a expliqué avoir acheté cette caméra Ring, que fabrique Amazon, pour garder un œil sur sa fille lorsqu'elle travaillait de nuit, puisque sa fille avait des antécédents de convulsions.
Elle avait choisi de s'en procurer pour regarder ses enfants sur son téléphone. ainsi que pour pouvoir leur parler, ce qu'elle trouvait vraiment intéressant.

La jeune Alyssa, âgée de 8 ans, entend de la musique venant de sa chambre. Elle entre dans la pièce pour savoir ce qui se passe. Soudain, la chanson s'arrête.
En entrant dans sa chambre un homme lui parle, alors qu'elle ne comprend pas d'où la voix vient.
L'homme commence alors à insulter la fillette, en lui demandant de répéter.
Afin de l'inciter à l'écouter, il essaye de la faire obéir en lui disant qu'il était le Père Noël, son meilleur ami.
Il dit alors à la fillette qu'elle peut faire ce qu'elle veut, mettre sa chambre en désordre, ou même casser son écran de télé.
La fillette va alors chercher sa mère, terrorisée, mais l'homme ne se re-manifestera plus.

Capture de l'attaque dirigée vers la fillette...

Dans ce cas de figure, on pourrait très bien imaginer que l'homme derrière cette attaque puisse être bien plus malveillant que ça, du fait qu'il n'ait visé qu'une enfant, ce qui aurait pu la mettre réellement en danger...

Le cas de la femme anonyme :

Dans un autre cas, une femme âgée, vivant d'un centre de vie avec assistance s'est aussi fait piraté ses caméras de surveillance Ring.
En rentrant dans son appartement, elle a entendu quelqu'un lui dire : "Ce soir, tu meurs", et aurait été harcelée sexuellement par l'attaquant.
Suite à cela, l'attaquant aurait joué des sons de sirènes au volume maximum, pour terroriser encore plus la pauvre femme.
Au final, cette femme a choisi de déménager avec sa famille, ne se sentant pas en sécurité, craignant même pour sa vie dans le lieu où elle vivait.

4) Pénalités appliquées suite à cette faille

Avec la 3e faille, un grand nombre de hackers se sont mis au risque de faire face à la justice.
En particulier face à la justice américaine, vu que la majorité de ces problèmes sont apparus aux États-Unis.
Voici donc un bref résumé des actes qui ont été possiblement commis pendant ces attaques pour avoir une estimation de ce que ces personnes ont risqué :
L'accès illégal à un appareil électronique ainsi que voler des informations privées peut correspondre une peine de 1 à 5 ans.
Cependant, la justice américaine applique un procédé de pénalité additive.
En partant de ce principe, les attaquants n'ont pas fait qu' accéder à la caméra.

Les cybercriminels peuvent donc faire face à des charges supplémentaires :

- Faire des menaces de mort : 1 an de prison et de $1000 à $10 000 d'amende
- Faire du chantage : 1 an de prison et/ou jusqu'à $100 000 d'amende
- Pratiquer de la pédopornographie : 10 à 20 ans de prison
- Faire du vol : 1 an de prison

Amazon, qui s'était fait attaquer en justice par une vingtaine de ces victimes, s'est vu demander des dédommagements par certains de ses clients, dont une personne demandant 5 millions de dollars.
Cette affaire n'a pour le moment eu aucune réelle fin. Ceci est principalement dû à la complexité de l'affaire, qui doit passer en revue toute les plaintes mais aussi vérifier d'autres paramètres ralentissant la justice.
Il est cependant peu probable que ce cas aille donner des pénalités à Amazon, suite au fait que les conditions d'utilisations de ring soient assez claires sur la gestion de ce genre de problèmes.

Cependant, cette histoire n'a pas été bénéfique pour Ring, perdant la confiance de beaucoup d'utilisateurs, avec des associations et des avocats de consommation boycottant ce produit en avertissant les consommateurs des risques des produits de Ring.
D'autres sites, comme WireCutter, un site de revue pour ce genre d'appareils, ont décidé d'enlever tout ce qui parlait de Ring, ce qui a sérieusement endommagé sa réputation.

Amazon a aussi licencié et averti quelques employés de Ring suite à cette affaire, car ils étaient aussi suspectés d'espionnage envers certains de leurs clients.

Conclusion :

Cette histoire rappelle qu'il ne faut pas prendre à la légère la sécurité des objets connectés que nous utilisons, et surtout celle des appareils que nous utilisons afin de protéger notre vie privée. Si les cyberdélinquants ont pu si facilement s'infiltrer dans les caméras Ring, c'est dû au fait que les utilisateurs n'avaient pas jugé bon d'activer la double authentification.
Cela ajouté au fait que Ring n'avait pas mis en place les caractéristiques de sécurité basiques dans leur matériel de sécurité. Ce qui a permis au pirate de facilement trouver un mot de passe et un identifiant pour accéder au système et prendre le contrôle de la caméra.
En ce qui concerne les attaques de Décembre 2019, les victimes, ainsi que tous ceux qui ont entendu parler de l'affaire ont bien appris que l'utilisation de matériel de sécurité pouvait être totalement contre productif, notamment dans le cas où l'utilisateur n'installe pas les dispositifs correctement, ou encore s'il jugent inutile de protéger correctement leur équipement.

Bien que ces attaques ont été en majorité inoffensives, il nous est impossible de déterminer réellement l'ampleur du problème qui a été généré. Un criminel a très bien pu apprendre des faits importants sur la vie d'une personne pour tenter une action contre cette dernière, notamment en faisant du repérage, et ce d'une façon assez discrète pour éviter d'attirer l'attention.

Ressources :

Article sur la première faille : - -
https://theintercept.com/2019/01/10/amazon-ring-security-camera/

https://www.theinformation.com/articles/at-rings-r-d-team-security-gaps-and-rookie-engineers

Articles sur la deuxième faille :

https://www.pcmag.com/news/exclusive-bitdefender-discovers-ring-doorbell-vulnerability

https://www.bitdefender.com/blog/hotforsecurity/bitdefender-finds-ring-doorbell-vulnerability-exposes-users-wi-fi-password

Rapport de BitDefender concernant la deuxième faille:
https://www.bitdefender.com/files/News/CaseStudies/study/294/Bitdefender-WhitePaper-RDoor-CREA3949-en-EN-GenericUse.pdf

Articles sur l'affaire de la troisième faille amenée en justice
https://cisomag.eccouncil.org/amazons-ring-slammed-with-federal-lawsuit/

https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit

Articles sur les lois américaines et les peines encourues

https://www.findlaw.com/criminal/criminal-charges/hacking-laws-and-punishments.html

https://www.criminaldefenselawyer.com/crime-penalties/federal/petty-theft.htm

https://www.pagepate.com/experience/criminal-defense/federal-crimes/federal-child-pornography/

https://www.justia.com/criminal/offenses/white-collar-crimes/blackmail/

https://www.criminaldefenselawyer.com/crime-penalties/federal/Criminal-Threats.htm

Article concernant le cas de la famille LeMay
https://www.today.com/money/family-whose-ring-camera-was-hacked-now-suing-company-t172787