RAPPORT CYBERATTAQUE CONFORAMA

BUT1 R&T – Sorbonne Paris Nord

IUT DE VILLETANEUSE

ALI EL MGHAIMIMI – REDWANE BAIROUQ – RAYAN SAIDFARAH

R111 – Expression & Culture
S1 2023 - 2024

Table des matières

INTRODUCTION

L'évolution rapide de la technologie et la numérisation croissante des opérations commerciales ont apporté de nombreux avantages aux entreprises, mais elles ont également ouvert la porte à une menace omniprésente : les cyberattaques. Ces attaques, perpétrées par des acteurs malveillants, peuvent causer des dommages considérables aux entreprises, mettant en péril leur sécurité, leur réputation et leurs opérations. Dans ce rapport, nous explorerons de manière approfondie une cyberattaque récente qui a touché l'entreprise Conforama.

Notre problématique centrale se concentre sur les circonstances qui ont permis au groupe de cybercriminels connu sous le nom de BlackCat, alias ALPHV et Noberus, de s'infiltrer dans le système d'information de Conforama. Cette attaque a eu un impact significatif sur l'entreprise, exposant la nécessité cruciale de comprendre les tactiques employées par les cybercriminels et les mesures de sécurité nécessaires pour se protéger contre de telles menaces.

Nous diviserons ce rapport en trois parties clés, chacune avec deux sous-parties. Tout d'abord, nous entreprendrons une analyse du type d'attaque mise en place par BlackCat, en examinant les méthodes et les outils utilisés, tels que les malwares et les ransomwares. Ensuite, nous explorerons le groupe BlackCat lui-même, ses origines, ses modèles d'attaque et son historique d'attaques notables.

La dernière partie du rapport se penchera sur les mesures prises par Conforama pour faire face à cette cyberattaque et renforcer sa sécurité informatique. Nous verrons comment l'entreprise a réagi après l'incident, en mettant en place des mesures spécifiques telles que l'authentification à deux facteurs et la surveillance du trafic réseau. Nous examinerons également les recommandations générales de l'Agence Nationale des Systèmes de Sécurité des Informations (ANSSI) que chaque entreprise devrait suivre pour renforcer sa sécurité informatique.

En fin de compte, ce rapport vise à tirer des leçons de cette cyberattaque contre Conforama et à proposer des orientations précieuses pour aider les entreprises à se préparer et à se protéger contre les menaces croissantes dans le paysage numérique complexe d'aujourd'hui.

ANALYSE DU TYPE D'ATTAQUE MISE EN PLACE

A/ Analyse du type d'attaque subie par CONFORAMA :

1/ Nature de l'attaque L'attaque dont CONFORAMA a été la cible était une attaque par ransomware. Les cybercriminels ont réussi à infiltrer le système d'information de l'entreprise en utilisant une variante de ransomware connue sous le nom de "WannaCry". Une fois à l'intérieur du réseau, les attaquants ont chiffré les fichiers et les données sensibles de l'entreprise, rendant ainsi les systèmes inaccessibles.

Figure 1: Logiciel "Wannacry"

2/ Impact de l'attaque Cette attaque a eu un impact significatif sur CONFORAMA. Les systèmes informatiques de l'entreprise ont été paralysés, entraînant une interruption majeure de ses opérations commerciales. Les données critiques ont été chiffrées, ce qui a entraîné des perturbations dans la chaîne d'approvisionnement, des retards dans les livraisons et des problèmes de gestion des stocks. De plus, les attaquants ont demandé une rançon importante en échange de la clé de déchiffrement nécessaire pour restaurer les données.

B/ Mesures de récupération et de prévention mises en place par CONFORAMA après l'attaque :

1/ Récupération des données CONFORAMA a d'abord décidé de ne pas payer la rançon exigée par les attaquants, conformément aux recommandations de nombreux experts en sécurité. Au lieu de cela, l'entreprise a fait appel à des experts en sécurité informatique et à des professionnels de la récupération de données pour tenter de restaurer les informations chiffrées. Malheureusement, une grande partie des données n'a pas pu être récupérée, ce qui a entraîné des pertes importantes.

2/ Renforcement de la sécurité Suite à cette attaque dévastatrice, CONFORAMA a entrepris une refonte complète de sa stratégie de sécurité informatique. L'entreprise a investi massivement dans des solutions de sécurité avancées, telles que la détection avancée des menaces, l'analyse comportementale, et la surveillance en temps réel de l'activité réseau. De plus, CONFORAMA a renforcé ses politiques de sauvegarde de données et de reprise après sinistre pour minimiser les impacts en cas de nouvelles attaques. Elle a également mis en place des formations de sensibilisation à la sécurité plus fréquentes pour son personnel, afin de réduire les risques liés à l'ingénierie sociale.

En conclusion, CONFORAMA a subi une attaque par ransomware dévastatrice, ce qui a entraîné des perturbations majeures dans ses opérations. Cependant, l'entreprise a choisi de ne pas payer la rançon et a concentré ses efforts sur la récupération des données et le renforcement de ses mesures de sécurité pour prévenir de futures attaques de ce type. Cette expérience a conduit à une amélioration significative de la posture de sécurité de l'entreprise.

Voyons voir maintenant les assaillants, leurs méthodes et leur historique d’attaque.

LE GROUPE APLHV ET LEURS DIFFERENTES ATTAQUES

QUI SONT-IL ?

BlackCat, aussi connu sous le nom d'ALPHV et de Noberus est une famille de rançongiciels écrite en Rust (langage de programmation), qui apparaît en novembre 2021. Par extension, c'est aussi le nom du groupe de hackers qui l'exploite. Blackcat opère suivant un modèle de rançongiciel en tant que service, avec des développeurs proposant leur logiciel a des affiliés en échange d'un pourcentage de la rançon extorquée. Le groupe est également connu pour ses méthodes non conventionnelles et l'utilisation de techniques d'extorsion avancées telles que la triple extorsion. Ses tactiques ont fait de BlackCat une menace cybercriminelle majeure. Le groupe cible des centaines d'organisation à travers le monde, dont Reddit en 2023. Depuis sa création, il s'agit de l'un des rançongiciel les plus actifs.

Le groupe derrière BlackCat utilise principalement la tactique de la double extorsion, mais a aussi recours à la triple extorsion. Cette dernière consiste à crypter le système d'information de la victime, à exposer les données exfiltrées, à menacer de lancer des attaques par déni de service (DDoS) sur l'infrastructure des victimes. Les affiliés de BlackCat demandent généralement des paiements de rançon de plusieurs millions de dollars en Bitcoin et Monero et ont déjà accepté des paiements de rançon inférieurs au montant initial de la demande. Selon le FBI, de nombreux développeurs et blanchisseurs d'argent pour BlackCat/ALPHV sont liés à Darkside/Blackmatter, ce qui indique qu'ils disposent de réseaux étendus et d'expérience dans le fonctionnement des rançongiciels. Le groupe est connu pour être le premier rançongiciel à avoir créé un site web public de fuites de données sur internet. Les cyber-groupes précédents publiaient généralement les données volées sur le dark web. L'innovation de BlackCat a consisté à publier des extraits ou des échantillons des données des victimes sur un site accessible à toute personne disposant d'un navigateur web. Les experts en sécurité pensent que cette tactique vise à donner plus de crédibilité à leurs déclarations de violation des systèmes des victimes et à accroître la pression sur les organisations pour qu'elles paient des rançons afin d'empêcher l'exposition publique complète de leurs données. Le groupe imite également les sites web de ses victimes pour afficher les données volées sur des répliques typo-squattées. Pour ses premières campagnes, Royal ransomware utilise l'outil de cryptage « BlackCat ».

Figure 2: Le groupe BlackCat

HISTORIQUE DE LEURS ATTAQUES ?

- BlackCat est observé pour la première fois par des chercheurs de la MalwareHunterTeam à la mi-novembre 2021.

- En avril 2022, le Fédéral Bureau of Investigation (FBI) publie un avis indiquant que plusieurs développeurs et blanchisseurs d'argent pour BlackCat avaient des liens avec deux anciens groupes de rançongiciels en tant que service (RaaS) DarkSide et BlackMatter. Selon certains experts, ce ransomware pourrait être une nouvelle marque de DarkSide, après son attaque contre le Colonial Pipeline. Il pourrait aussi s'agir d'un successeur du groupe cybercriminel REvil.

- En janvier 2022, le groupe lance une attaque d'ampleur contre des compagnies pétrolières allemandes. En septembre 2022, BlackCat revendique une attaque contre une agence italienne de l'énergie et a affirmé avoir exfiltré environ 700 gigaoctet (Go) de données de l'agence.

- Fin mai 2022, un gouvernement européen est ciblé par BlackCat, qui exige une rançon de 5 millions de dollars américains. Le même mois, un rapport remarque que le ransomware s'appuyait sur le Botnet Emotet.

- En septembre 2022, des chercheurs sur les menaces ont noté l'utilisation par BlackCat d'une version améliorée de l'outil d'exfiltration de données

ExMatter et d'Eamfo, un logiciel malveillant conçu pour voler les informations d'identification stockées par le logiciel de sauvegarde Veeam. Le même mois, un rapport indiquait que BlackCat utilisait le botnet Emotet pour déployer sa charge utile de rançongiciel.

- En décembre 2022, les opérateurs derrière BlackCat annoncent que leur offre RaaS incluait désormais un Log4J Auto Exploiter préemballé.

- Au début de l'année 2023, Blackcat attaque Grupo Estrategas EMM, NextGen Healthcare, Solar Industries India, Instituto Federal Do Pará, Munster Technological University, et Lehigh Valley Health Network.

- En février 2023, une variante appelée « Sphynx » est publiée avec des mises à jour visant à augmenter la vitesse et la furtivité. En mai 2023, on estime que le groupe a ciblé plus de 350 victimes dans le monde depuis son apparition.

- En juin 2023, le groupe revendique une violation des systèmes de Reddit datant de février 2023. Sur leur site de fuite de données, ils ont affirmé avoir volé 80 Go de données compressées et demandé une rançon de 4,5 millions de dollars à Reddit. Cette attaque n'impliquait pas de chiffrement de données comme les campagnes de ransomware habituelles.

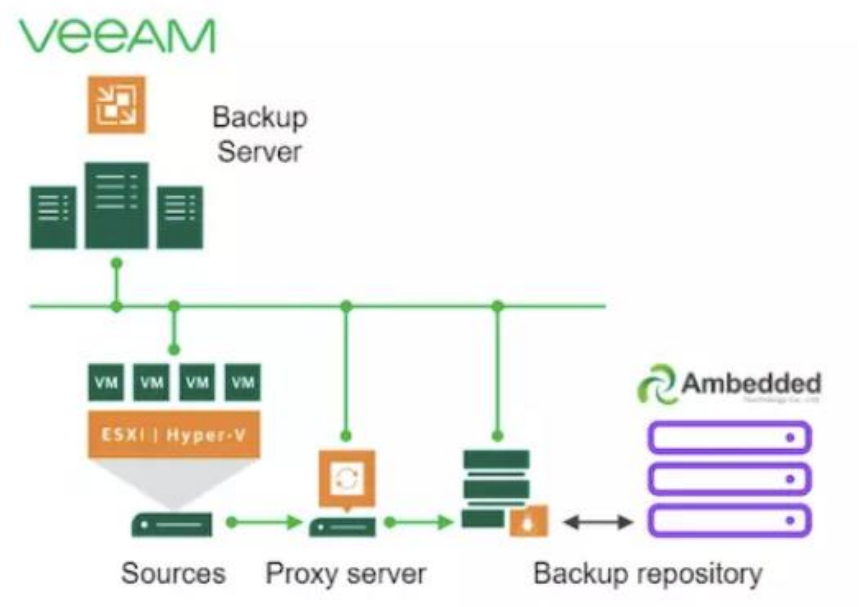

Figure 3: Sauvegarde veeam

Finalement, leur attaque contre l'entreprise française Castorama a également retenu l'attention, suivie par une menace similaire à l'encontre de Conforama. Dans ce dernier cas, le groupe a prétendu avoir volé plus de 1 To de données sensibles et a exigé des mesures spécifiques sous peine de publication des données volées.

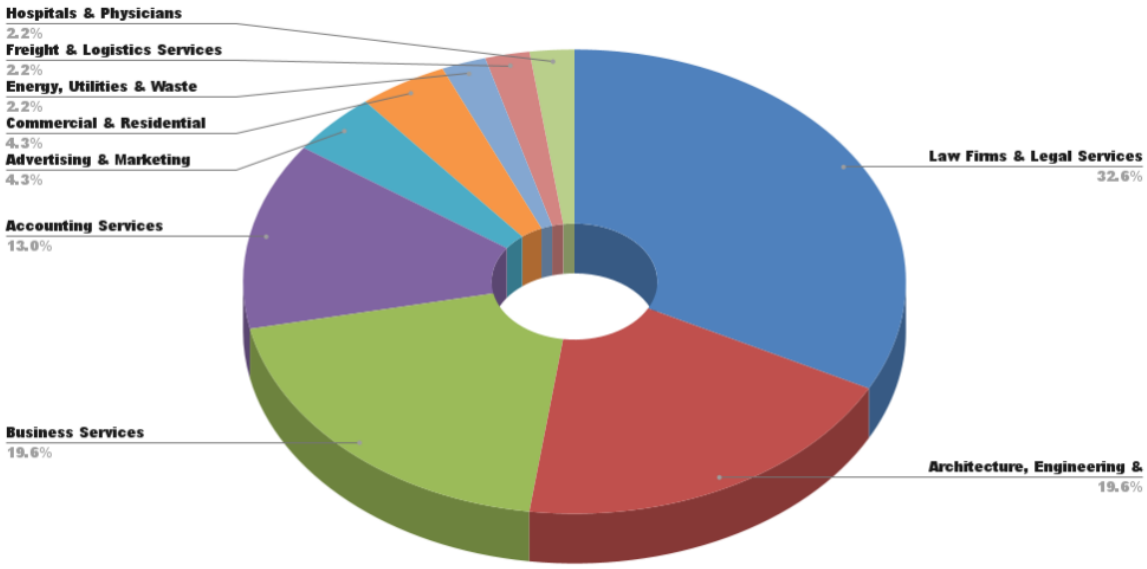

Figure 4: Diagramme circulaire du pourcentage d'organisations et de services touchées par BlackCat

Modes opératoire du groupe ALPHV

A/ attaque de ALPHV envers Bolloré et son entreprise Automatic système

Automatic Systems, une entreprise belge spécialisée dans les portiques de sécurité et filiale du groupe Bolloré, a été victime d'une cyberattaque par ransomware. Revendication du groupe de hackers russophones ALPHV. Le collectif de cybercriminels a confirmé le 12 juin 2023 sur son site darknet être à l'origine d'une cyberattaque par ransomware contre l'entreprise belge Automatic Systems. Cette filiale du groupe Bolloré figure parmi les plus importants fabricants de portiques d'entrée et de sécurité sur le marché mondial. La société a reconnu l'attaque le 3 juin, déclarant sur son site « qu'elle fait appel à des experts externes en cybercriminalité qui épaulent actuellement les équipes informatiques internes 24h/24. Des investigations sont en cours afin d'évaluer la nature des informations qui auraient pu être rendues accessibles à des tiers *».*

Les hackers ont lancé un chrono de 48h dans la nuit du 12 juin en attendant d'être contactés par les responsables de la société. Sinon, de nouvelles données seront publiées. Les cybercriminels exigent généralement une rançon élevée pour débloquer l'ensemble des fichiers chiffrés. Le collectif ALPHV met la pression sur la victime en partageant des informations personnelles de salariés et des contrats avec d'importants clients. Parmi les documents que Numerama a pu consulter, on trouve des échanges avec la RATP, le géant chinois Alibaba, le fournisseur énergétique Engie ou encore le groupe Thalès.

RECOMMANDATIONS ET LES SYSTEMES MIS EN PLACE APRES L'ATTAQUE PAR CONFORAMA

A/ Moyen mise en place par Conforama

Après la tentative d'intrusion du groupe ALPHV dans le système d'information de l'entreprise CONFORAMA, examinons les mesures précises et techniques prises par l'entreprise pour renforcer sa sécurité et la protection des données personnelles :

1/ Mises à jour de la politique de protection des données personnelles CONFORAMA a mis en place plusieurs mesures techniques pour renforcer sa sécurité après la cyberattaque. Parmi celles-ci, l'entreprise a mis en œuvre un système d'authentification à deux facteurs (2FA) pour l'accès à ses systèmes sensibles. Cela signifie que, en plus d'un mot de passe, les utilisateurs doivent fournir une deuxième forme d'authentification, telle qu'un code généré par une application sur leur smartphone, pour accéder aux données sensibles.

De plus, CONFORAMA a déployé un système de détection des intrusions basé sur l'intelligence artificielle (IA) qui analyse le trafic réseau en temps réel pour détecter les comportements suspects. En cas de détection d'une activité anormale, le système déclenche automatiquement des alertes et isole la partie du réseau affectée pour prévenir une éventuelle propagation de l'attaque.

2/ Sanctions pour les cyberattaques CONFORAMA a adopté une approche technique rigoureuse pour dissuader les cybercriminels. L'entreprise a mis en place un système de surveillance des activités sur son réseau qui enregistre chaque action effectuée par les utilisateurs. En cas de tentative de cyberattaque, les preuves techniques sont conservées, ce qui facilite la collecte de preuves à des fins juridiques.

De plus, CONFORAMA a conclu des partenariats avec des entreprises de sécurité informatique pour effectuer des tests de pénétration réguliers sur son réseau. Ces tests simulent des attaques réelles pour identifier les vulnérabilités et les corriger avant qu'elles ne soient exploitées par des attaquant.

Figure 5:Politique de protection sur le site Conforama

B/ Recommandation Général

En plus des mesures spécifiques prises par CONFORAMA, examinons des exemples concrets des recommandations générales de l'ANSSI que chaque entreprise devrait suivre en matière de sécurité informatique :

1/ Suivre les recommandations de l'ANSSI L'ANSSI recommande aux entreprises de mettre en œuvre des pare-feu avancés, tels que des pare-feu d'application Web (WAF), pour protéger leurs applications en ligne contre les attaques. CONFORAMA a suivi cette recommandation en déployant un WAF qui identifie et bloque automatiquement les tentatives d'exploitation de vulnérabilités connues.

De plus, l'ANSSI encourage l'utilisation de chiffrement fort pour protéger les données en transit. CONFORAMA a répondu à cette recommandation en utilisant des certificats SSL/TLS pour sécuriser les communications entre les utilisateurs et ses serveurs, garantissant ainsi la confidentialité des données échangées.

2/La nécessité d'une approche holistique de la sécurité CONFORAMA a adopté une approche holistique de la sécurité en formant régulièrement ses employés aux bonnes pratiques en matière de sécurité informatique. Par exemple, l'entreprise a organisé des séances de sensibilisation pour enseigner aux

employés comment identifier les emails de phishing et éviter de cliquer sur des liens malveillants.

De plus, CONFORAMA a élaboré un plan de réponse aux incidents qui comprend des scénarios spécifiques, tels que la gestion d'une fuite de données, avec des étapes techniques détaillées pour contenir, analyser et résoudre l'incident. Cette approche assure une réaction rapide et efficace en cas de cyberattaque.

En conclusion, les mesures techniques mises en place par CONFORAMA incluent l'utilisation de la 2FA, la surveillance du trafic réseau, les tests de pénétration, les pare-feu avancés et le chiffrement. De plus, en suivant les recommandations de l'ANSSI et en adoptant une approche globale de la sécurité informatique, l'entreprise renforce sa défense contre les cyberattaques et protège efficacement ses données et ses systèmes.

Figure 6 : logo ANSSI

CONCLUSION

La cyberattaque subie par l'entreprise Conforama, orchestrée par le groupe de cybercriminels BlackCat, également connu sous les noms ALPHV et Noberus, a révélé la complexité croissante des menaces en ligne et la nécessité pour les entreprises de renforcer leur sécurité informatique. Cette attaque a soulevé la question fondamentale de savoir comment un groupe comme BlackCat a pu s'infiltrer dans les systèmes de Conforama, mettant en danger la confidentialité des données et la continuité de ses opérations.

L'analyse du type d'attaque a révélé que BlackCat opère principalement en utilisant des rançongiciels, avec une préférence pour la double extorsion et même la triple extorsion. Ils ont été responsables de plusieurs attaques notables, y compris celle contre Conforama, où ils ont menacé de publier des données sensibles volées.

Le groupe BlackCat a été particulièrement audacieux et sophistiqué dans ses attaques, utilisant des outils et des techniques avancés pour atteindre ses objectifs. Les recommandations générales de l'ANSSI en matière de sécurité informatique, telles que l'utilisation de pare-feu avancés, le chiffrement fort et la sensibilisation des employés, ont été adoptées par Conforama pour renforcer sa sécurité.

Conforama a également mis en place des mesures spécifiques pour répondre à l'attaque, notamment l'authentification à deux facteurs, la surveillance du trafic réseau, les tests de pénétration et la conservation de preuves techniques pour d'éventuelles poursuites judiciaires.

En conclusion, la cyberattaque contre Conforama a été un rappel brutal de la nécessité pour toutes les entreprises de prendre au sérieux la sécurité informatique. Les menaces en ligne évoluent rapidement, et il est essentiel de mettre en place des mesures techniques et organisationnelles robustes pour se protéger. En suivant les recommandations de l'ANSSI et en adoptant une approche holistique de la sécurité, les entreprises peuvent renforcer leur défense contre de telles attaques et protéger efficacement leurs données et leurs systèmes.

Table des illustrations