Syd
DIGITAL CARE

#9

Note de

PROSPECTIVE

MALWARE

L'ÈRE DE LA PROFESSIONNALISATION

2021

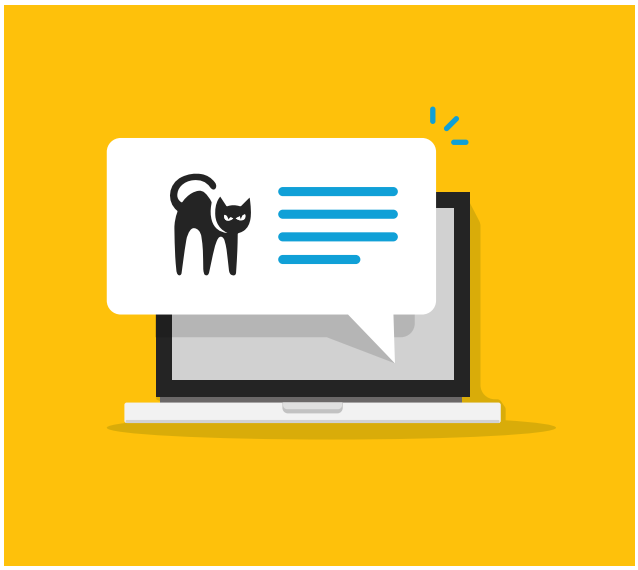
MIAOU.

Nous avons hésité à rédiger un cahier de la prospective sur la cybersécurité. Tous les jours, les journaux spécialisés se font en effet l'écho de nouvelles attaques, de nouvelles fragilités ou de nouvelles actions des autorités.

Mais ça, c'était avant ***BlackCat.***

Ce chat noir est d'un genre nouveau. Plus connu sur les forums russes sous le nom de « ALPHV » : Ransomware as a Service, il inaugure, selon nous, une nouvelle ère de professionnalisation dans les extorsions de fonds.

Le mécanisme du ransomware est désormais très connu. Un groupe malveillant parvient à implanter un logiciel malin au sein d'une entreprise (malware). Tous ses fichiers sont alors cryptés et une rançon est demandée pour l'obtention du code permettant de revenir sur ce cryptage. Depuis quelques années, les métiers s'étaient spécialisés. Vous aviez d'un côté les « éditeurs » de malware (ReVil, BlackMatter, ...) et les exploitants qui les utilisaient pour s'attaquer aux entreprises et demander des rançons. Un pourcentage de chaque somme versée par les entreprises va à l'éditeur et l'exploitant en engrange la plus grande part. Simplement, ces derniers se focalisaient sur les stratagèmes à employer pour pénétrer les systèmes de protection des entreprises. Le logiciel malware avait sa propre logique qu'ils étaient obligés de suivre. C'est même parfois à cause de ça qu'ils se faisaient repérés par le FBI.



BlackCat, quant à lui, offre, cette fois, de nombreuses caractéristiques vraiment professionnelles :

- *Il passe déjà pour le ransomeware le plus sophistiqué de l'année d'après la communauté des consultants en cybersécurité.*

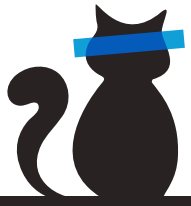
- *Il est écrit en Rust, langage promu par l'ANSS[1] pour sa fiabilité dans les applications de cybersécurité. Pour rentrer dans les détails, ils le qualifient de « langage multiparadigmes dont un des objectifs principaux est de concilier une ergonomie de haut-niveau avec une gestion fine de la mémoire ». En clair, Rust permet l'exploit de développer rapidement et graphiquement des fonctionnalités de haut niveau tout en sécurisant son code en couche basse.*

- *Il offre un très haut niveau de personnalisation. BlackCat peut être configuré selon 4 moyens de chiffrement différents (total, rapide, DotPattern et automatique). Ses concepteurs indiquent sur le darknet qu'ils utilisent, s'il existe, le support matériel AES pour crypter les données. L'Advanced Encryption Standard équipe aujourd'hui l'ensemble des machines. Il avait été mis en place, en 1997, en remplacement du DES, Data Encryption Standard qui était vieillissant et qui ne tenait plus ses promesses notamment vis-à-vis d'attaques par force brute. En clair, BlackCat utilise, pour crypter, le système interne de nos serveurs... qui avait été mis en place pour renforcer la résistance face aux cyberattaques.*

1 *Source : www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-dapplications-securisees-en-rust/*

• *Il est, ensuite, entièrement piloté par ligne de commande, et hautement configurable, avec la possibilité d'utiliser différentes routines de chiffrement et une fonction de propagation entre systèmes, d'arrêter des machines virtuelles et les VM ESXi, et d'effacer automatiquement les snapshots ESXi pour empêcher toute restauration. « Chaque exécutable du ransomware ALPHV comprend une configuration JSON qui permet la personnalisation des extensions, les notes de rançon, la façon dont les données seront cryptées, les dossiers/fichiers/extensions exclus, et les services et processus à terminer automatiquement », complète le site d'assistance informatique Bleeping Computer .*

• *Enfin, et c'est peut-être sa fonctionnalité la plus moderne, BlackCat propose un jeton de connexion (token) entre les victimes et la plateforme de négociation et de paiement des cyberhackers sur le darkweb. Ces conversations ne pourront donc être elle-même piratées.*



POUR CONCLURE

Avec BlackCat, un nouveau stade dans la « professionnalisation » de la cybermenace. Imaginez les dégâts qui ont été causés par ReVil ou BlackMatter et multipliez les nouveaux candidats aux cyberattaques rendus confiants par la simplicité de mise en œuvre d'une telle solution et par la protection contre les autorités qu'elle leur propose.

BlackCat est apparu pour la première fois le 21 novembre 2021. Les rançons demandées dans plusieurs pays varient entre 400 000 et 3 millions de dollars.

vous avez des questions ?
Envoyez-nous un mail à

contact@syd.fr

Syd
DIGITAL CARE