Historique des ransomwares

"Ransomware: A Growing Menace" (Ransomware : une menace grandissante) a été publié dans le magazine PC World en mai 1989. Il a été écrit par le journaliste américain *John Markoff*.

Cet article décrit les activités d'un programme appelé "AIDS Trojan" (aussi connu sous le nom de "PC Cyborg") qui a été créé par un biologiste américain nommé Joseph Popp. Le programme a été distribué sous la forme de disquettes contenant un questionnaire sur le SIDA, mais il chiffrait ensuite les fichiers de l'ordinateur de la victime et demandait une rançon pour les débloquer.

Bien que l'article de Markoff ne se concentre pas exclusivement sur les ransomwares, il est souvent considéré comme une référence importante dans l'histoire des ransomwares et de leur couverture médiatique.

Au milieu des années 2000, la menace des ransomwares devient vraiment importante pour les entreprises. En 2017 aux états unies, l'internet Crime Complaint Center (IC3) du FBI a reçu plusieurs plaintes concernant les ransomwares (1783 pour être plus précis). Malheureusement ce chiffre ne reflète pas réellement le nombres ransomwares dans qu'il y'a dans le monde. En effet, il y a eu en 2022 plus de 30 millions de ransomwares

2022 CRIME TYPES continued

By Victim Loss

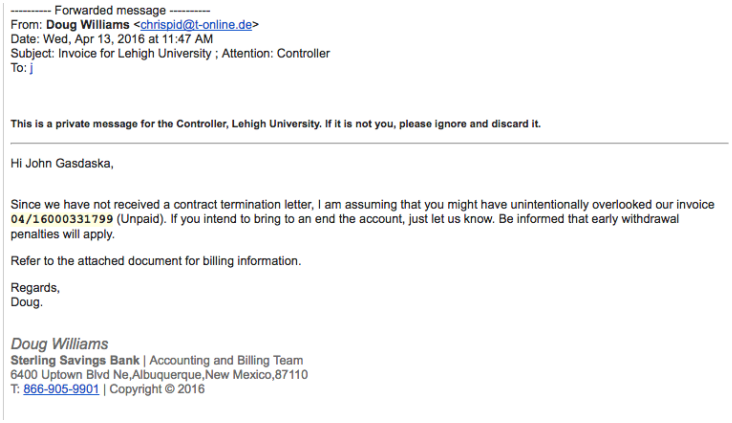
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

*Descriptors***			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

Source :https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Voici des exemples de types de vecteurs :

Pièces jointes aux e-mails



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

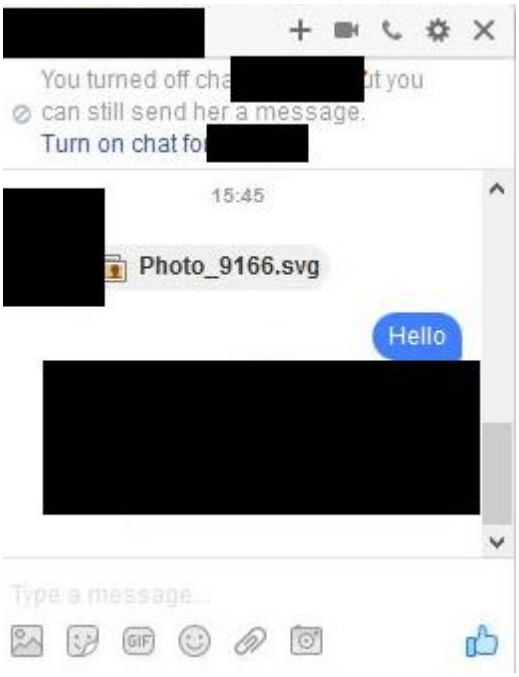
Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

Une méthode de tromperie courante utilisée pour distribuer des rançongiciels est l'envoi d'une raison impérieuse pour les entreprises d'ouvrir des logiciels malveillants déguisés en pièce jointe urgente. Si une facture parvient à un propriétaire d'entreprise ou au service des comptes fournisseurs, elle est susceptible d'être ouverte. Cette tactique, comme beaucoup d'autres dans cette liste, consiste à tromper pour accéder à des fichiers et/ou des systèmes.

Messages :



Les attaquants de ransomwares utilisent les sites de médias sociaux pour tromper les victimes, en particulier Facebook Messenger. Ils créent de faux comptes en prétendant être l'ami de la victime et

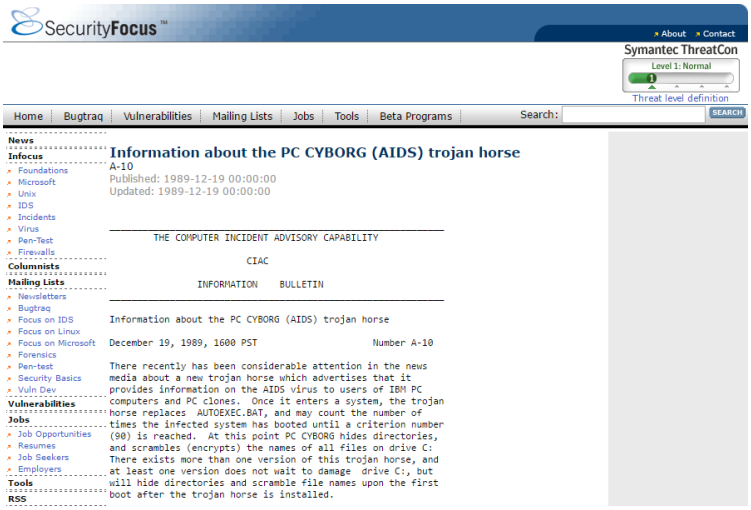
envoient des messages avec des pièces jointes qui, une fois ouvertes, déclenchent le rançongiciel, verrouillant ainsi tous les appareils connectés.

Popups

Les "pop-ups" en ligne sont un vecteur courant et ancien de rançongiciel, conçus pour imiter les logiciels actuellement utilisés et tromper les utilisateurs en suivant des invites qui finalement leur portent préjudice.

La première attaque de ransomware

La première attaque de ransomware visant le secteur de la santé a eu lieu en 1989 comme dit plus haut, faisant de cette attaque la première connue. Depuis lors, le secteur de la santé demeure une cible privilégiée pour les attaques de ransomwares, plus de 28 ans après.



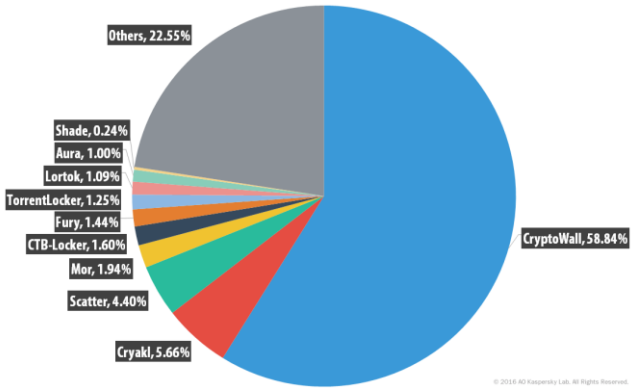
L'évolution des rançongiciels

Au fil des années, les ransomwares ont évolué de manière significative, passant d'attaques rudimentaires à des méthodes sophistiquées utilisées aujourd'hui. Les premiers développeurs de

ransomwares écrivaient leur propre code de cryptage, mais les attaquants actuels utilisent souvent des bibliothèques préexistantes plus difficiles à pirater. De plus, ils ont adopté des techniques de diffusion plus avancées telles que le harponnage, plutôt que les e-mails de phishing traditionnels qui sont facilement filtrés.

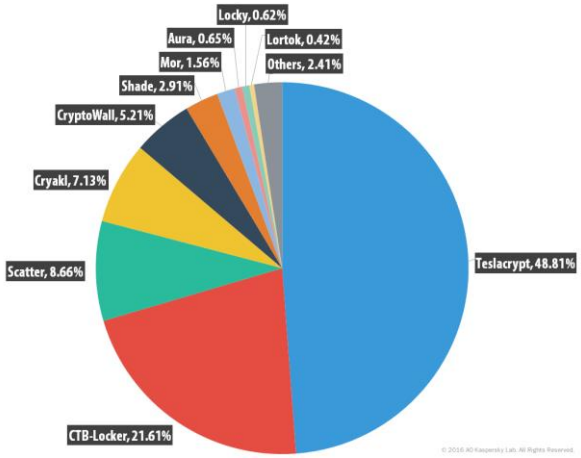
Certains attaquants sophistiqués proposent des kits d'outils accessibles aux cybercriminels moins compétents, tandis que d'autres offrent des programmes de ransomware en tant que service. Cela a conduit à la montée de ransomwares bien connus tels que **CryptoLocker**, **CryptoWal**l, **Locky** et **TeslaCrypt**. Certains de ces ransomwares ont généré des millions de dollars de revenus pour leurs auteurs.

Après la première attaque de ransomware documentée en 1989, ce type de cybercriminalité est resté rare jusqu'au milieu des années 2000, lorsque les attaques ont commencé à utiliser des algorithmes de chiffrement plus sophistiqués et plus difficiles à pirater, tels que le chiffrement RSA. **Gpcode**, **TROJ.RANSOM.A**, **Archiveus**, **Krotten, Cryzip** et **MayArchive** étaient populaire à cette époque. En 2011, un ver rançongiciel est apparu qui imitait l'avis d'activation de produit Windows, ce qui rendait plus difficile pour les utilisateurs de faire la différence entre les notifications authentiques et les menaces



Source: https://securelist.com/pc-ransomware-in-2014-2016/75145/

En 2015, plusieurs variantes de ransomwares ont causé d'importants dommages aux utilisateurs du monde entier. Selon SecureList de Kaspersky, entre avril 2014 et mars 2015, les ransomwares les plus prédominants étaient **CryptoWal**l, **Cryakl**, **Scatter**, **Mor**, **CTB-Locker**, **TorrentLocker**, **Fury**, **Lortok**, **Aura** et **Shade**. Ces ransomwares ont réussi à attaquer 101 568 utilisateurs à travers le monde, représentant ainsi 77,48 % de tous les utilisateurs touchés par des crypto-ransomwares pendant cette période, selon le rapport. En seulement un an, le paysage des ransomwares a considérablement évolué. Selon les recherches de Kaspersky pour l'année 2015-2016, "**TeslaCrypt**, ainsi que **CTB-Locker**, **Scatte**r et **Cryak**l étaient responsables d'attaques contre 79,21 % des utilisateurs confrontés à un crypto-ransomware".



source: https://securelist.com/pc-ransomware-in-2014-2016/75145/

Les plus grandes attaques de ransomware et les variantes les plus importantes

Table 5: Summary of types of charges in 15 ransomware families.

Families	Type of Charge			
	Premium Number	Untraceable Payments	Online Shopping	Bitcoin Transactions
Reveton		✓	✓	
Cryptolocker		✓		✓
CryptoWall				✓
Tobfy		✓		
Seftad	✓			
Winlock				
Loktrom	✓			
Calelk	✓			
Urausy		✓	✓	
Krotten		✓		
BlueScreen		✓		
kovter		✓	✓	
Filecoder		✓		
GPcode		✓		
Weelsof		✓		
Number of Samples	132 (9.71%)	1,199 (88.22%)	14(1.03%)	28 (2.86%)
Number of Variants	18 (19.35%)	75 (80.64%)	4 (4.30%)	4 (4.3%)

Sources: Ransom charges across 15 major ransomware families. Image via Northeastern University.

CryptoLocker était l'une des souches de rançongiciels les plus rentables de son époque. Par la suite, le modèle de chiffrement de CryptoLocker a été analysé, et un outil est maintenant disponible en ligne pour récupérer les fichiers chiffrés compromis par CryptoLocker. Malheureusement, la disparition de CryptoLocker a simplement conduit à l'émergence de plusieurs variantes de ransomwares imitant, notamment les clones bien connus CryptoWall et TorrentLocker. Gameover ZeuS lui-même est réapparu en 2014, "sous la forme d'une campagne évoluée envoyant des messages de spam malveillants." Depuis lors, le nombre de variantes et d'attaques n'a cessé d'augmenter, en ciblant principalement les secteurs bancaire, de la santé et gouvernemental.

Source: Image via *Computer World*

De avril 2014 à début 2016, CryptoWall était l'une des variétés de ransomwares les plus couramment utilisées, avec différentes formes du ransomware ciblant des centaines de milliers de particuliers et d'entreprises. À la mi-2015, CryptoWall avait extorqué plus de 18 millions de dollars à ses victimes, ce qui a incité le FBI à publier un avis sur cette menace.

En 2015, une variante de ransomware connue sous le nom de **TeslaCrypt** ou **Alpha Crypt** a touché 163 victimes, rapportant 76 522 dollars aux attaquants. **TeslaCrypt** demandait généralement des rançons en Bitcoin, bien que dans certains cas, PayPal ou des cartes My Cash aient été utilisés. Les montants des rançons variaient de 150 à 1 000 dollars.

Également en 2015, un groupe connu sous le nom d'Armada Collective a mené une série d'attaques contre des banques grecques. "En ciblant ces trois institutions financières grecques et en cryptant des fichiers importants, ils espèrent persuader les banques de payer la somme de 7 millions d'euros chacune. Il va sans dire que le fait de pouvoir mener trois types d'attaques différents en l'espace de cinq jours est très préoccupant en ce qui concerne la sécurité bancaire", a rapporté Digital Money Times. Les attaquants ont exigé une rançon de 20 000 bitcoins (7 millions d'euros) de chaque banque, mais au lieu de payer, les banques ont renforcé leurs défenses et évité d'autres perturbations de service, malgré les tentatives ultérieures d'Armada.

Pour les attaques contre de grandes entreprises, les rançons ont été signalées pouvant atteindre 50 000 dollars, bien qu'une attaque de ransomware l'année dernière contre un système hospitalier de Los Angeles, le Hollywood Presbyterian Medical Center (HPMC), aurait prétendument exigé une rançon de 3,4 millions de dollars. L'attaque a ramené l'hôpital à l'ère pré-informatique, bloquant l'accès au réseau de l'entreprise, aux e-mails et aux données cruciales des patients pendant dix jours.

En mars 2016, l'hôpital d'Ottawa a été victime d'un ransomware qui a impacté plus de 9 800 machines, mais l'hôpital a répondu en effaçant les disques durs. Grâce à des processus de sauvegarde et de récupération diligents, l'hôpital a réussi à prendre le dessus sur les attaquants et à éviter de payer une rançon.

Le même mois, le ransomware **Locky** a touché l'hôpital méthodiste du Kentucky, le Chino Valley Medical Center et le Desert Valley Hospital en Californie.

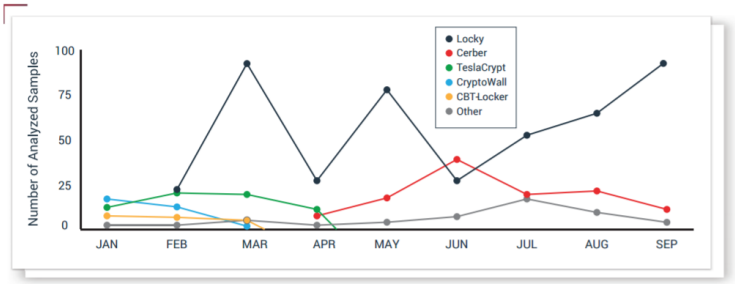


Figure 11: Relative proportions of ransomware varieties analyzed in 2016

Source:
Répartition des variantes de ransomware. Image via *PhishMe*.

L'avenir des ransomwares :

Ces incidents propulsent les ransomwares vers une nouvelle ère, dans laquelle les cybercriminels peuvent facilement reproduire de petites attaques et les diriger contre de grandes entreprises pour demander des rançons plus importantes. Bien que certaines victimes parviennent à atténuer les attaques et à restaurer leurs fichiers ou systèmes sans payer de rançon, il suffit d'un faible pourcentage de réussite des attaques pour générer des revenus substantiels - et une incitation - pour les cybercriminels.