RASCAGNERES

William

SIO2 SISR

Les virus, leur diffusion et leur histoire

SOMMAIRE

Termes importants et définitions

Virus: Logiciel réplicatif ayant pour but de se propager sur d'autres ordinateurs, avec ou sans intention malveillante (en analogie avec un virus "médical")

Cheval de Troie (ou trojan): Logiciel ayant pour but de déployer plusieurs logiciels malveillants ou virus sur un hôte (en analogie avec la légende du cheval de Troie)

Rançongiciel (ou Ransomware): Logiciel qui va crypter les documents et fichiers de l'hôte et qui demande une rançon afin de retirer le cryptage

Présentation du sujet:

Ce dossier traitera de l'historique des virus informatiques dans un premier temps, leurs différents buts puis des virus actuels dans un second temps, avant de finir sur les moyens de s'en défendre.

Première Partie

1. Comment sont nés les virus informatiques?

Les premières traces de virus informatiques remontent à 1970, avec un jeu appelé Core War. Ce jeu faisait s'affronter deux logiciels et le logiciel qui réussissait à être le dernier à fonctionner en fermant les instances de l'adversaire était désigné gagnant. A l'origine, il n'y avait pas d'intention malveillante dans ce jeu. Beaucoup des premiers virus de leur catégorie (trojan, vers…) sont des virus de type Proof Of Concept (POC), c'est-à-dire des virus créé dans le but de démontrer la faisabilité d'une thèse.

2. Historique des virus marquants

1970: ébauche des premiers virus informatique avec le jeu Core War

1971: Virus **Creeper**, se duplique d'hôte en hôte et affiche un message sur l'hôte infecté, virus de type POC afin de démontrer la faisabilité de faire transiter un logiciel sur un réseau)

1974: Virus **Rabbit**, a pour but de se répliquer afin de saturer l'espace de stockage, diminue les performances de l'hôte jusqu'à le faire planter. Réelle intention malveillante

1975: premier Trojan, appelé **Animal**. Trojan créé afin de répondre à une demande grandissante d'un jeu, et qui a pour but de se répliquer

dans tous les répertoires dans lequel il n'est pas afin d'assurer sa disponibilité.

1986: Première infection massive, sur des machines IBM par **Brain**, malware qui affiche un texte indiquant à l'hôte qu'il est infecté, et les coordonnées des développeurs du virus afin d'effectuer une "vaccination". Virus créé à des fins de publicités pour la boutique des développeurs, n'avait pas d'intention malveillante à proprement parler.

1988: Vers **Morris**, infectieux massive des machines, très peu de dégâts. Le but était de scanner Internet et d'estimer sa taille. Ce vers à permis de mettre à jour de nombreuses failles informatiques et de revoir les mesures de sécurité.

2000: Première large diffusion d'un virus par mails, écrase les fichiers existants sur l'hôte par des copies du virus et se diffuse en utilisant la boite mail de l'hôte infecté.

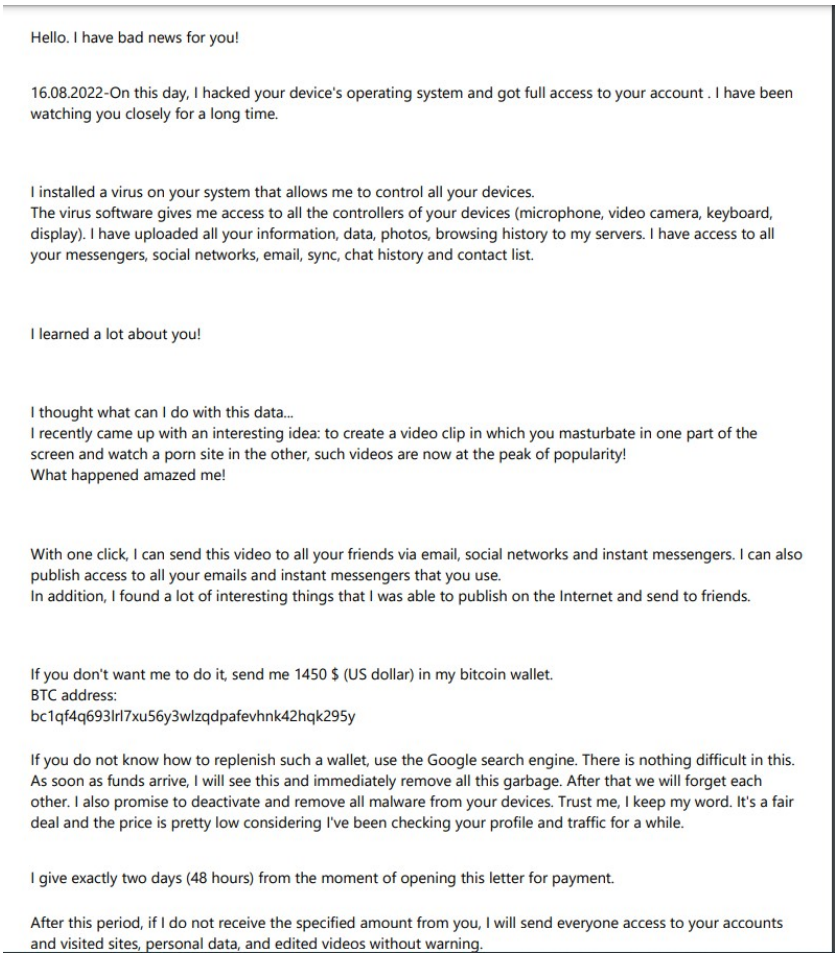
2001: Premier virus de type botnet (**Code Red**), à des fins de DDoS sur la Maison Blanche

2004:**Cabir**, premier virus ciblant la téléphonie avec propagation par le bluetooth (virus de type POC, démontrer que le bluetooth peut permettre la diffusion de logiciel)

Deuxième partie

1. Les virus actuels

Encore aujourd'hui les virus sévissent dans le monde. Il arrive que des attaques soient organisées à des fins d'espionnage en temps de guerre par les gouvernements impliqués, ou par des particuliers ou des groupes indépendants afin de voler des données et de les revendre sur le Dark Net par exemple. Les plus répandus actuellement sont les virus de type ransomware, qui ciblent souvent des entreprises afin de pouvoir espérer récupérer une rançon de la part de celles-ci. D'autres virus auront pour but de récupérer des mots de passe ou des schémas de saisie sur un hôte infecté, et ces données seront revendues ou utilisées comme chantage afin de récupérer de l'argent



Hello. I have bad news for you!

16.08.2022-On this day, I hacked your device's operating system and got full access to your account . I have been watching you closely for a long time.

I installed a virus on your system that allows me to control all your devices.
The virus software gives me access to all the controllers of your devices (microphone, video camera, keyboard, display). I have uploaded all your information, data, photos, browsing history to my servers. I have access to all your messengers, social networks, email, sync, chat history and contact list.

I learned a lot about you!

I thought what can I do with this data...
I recently came up with an interesting idea: to create a video clip in which you masturbate in one part of the screen and watch a porn site in the other, such videos are now at the peak of popularity!
What happened amazed me!

With one click, I can send this video to all your friends via email, social networks and instant messengers. I can also publish access to all your emails and instant messengers that you use.
In addition, I found a lot of interesting things that I was able to publish on the Internet and send to friends.

If you don't want me to do it, send me 1450 $ (US dollar) in my bitcoin wallet.
BTC address:
bc1qf4q693lrl7xu56y3wlzqdpafevhnk42hqk295y

If you do not know how to replenish such a wallet, use the Google search engine. There is nothing difficult in this. As soon as funds arrive, I will see this and immediately remove all this garbage. After that we will forget each other. I also promise to deactivate and remove all malware from your devices. Trust me, I keep my word. It's a fair deal and the price is pretty low considering I've been checking your profile and traffic for a while.

I give exactly two days (48 hours) from the moment of opening this letter for payment.

After this period, if I do not receive the specified amount from you, I will send everyone access to your accounts and visited sites, personal data, and edited videos without warning.

Exemple de mail pouvant être reçu suite à un piratage, contenant des menaces de divulgations de photos privées

D'autres virus peuvent utiliser des failles dans certains réseaux sans-fil, comme le bluetooth ou le WiFi dans certaines voitures possédant ces technologies (possible de modifier les affichages de la voiture et d'afficher des messages d'alertes, ou de prendre indirectement le contrôle du véhicule en activant des mesures de sécurité anti-collisions, récupérer les contacts des téléphones synchronisés) (Source: Quarkslab, Forum International de la Cybersécurité 2023)

2. Quelques attaques récentes

Pour citer quelques attaques récentes en France, il est possible de citer l'attaque de la prison de Draguignan en utilisant un support amovible infecté en janvier 2023, l'hôpital de Neufchâteau en octobre de la même année ou encore le virus Xenomorph, qui cible les matériels sous Android et qui utilise la méthode de superposition des applications afin de récupérer des mots de passe et autres informations de connexion. Xenomorph sévit depuis début 2023 au minimum

3. Comment se défendre

Pour se défendre des virus, il convient d'adopter quelques mesures de base:

-Toujours télécharger un logiciel sur le site d'origine

-Ne pas exécuter un logiciel inconnu reçu par mail, même venant d'une personne de confiance

-Vérifier régulièrement les logiciels installés et se renseigner sur tout logiciel inconnu que vous n'avez pas installé

-Maintenir son antivirus à jour

Conclusion

Les virus informatiques ne datent pas d'hier, et

Sources:

https://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/

https://fr.wikipedia.org/wiki/Creeper_(programme)

https://www.instagram.com/reel/CyY7kDCMowS/?igshid=MzRlODBiNWFlZA%3D%3D

https://fr.wikipedia.org/wiki/Core_War

https://www.ouest-france.fr/high-tech/attention-a-ce-virus-qui-peut-vider-vos-comptes-bancaires-6129b150-c195-11ed-b405-e8b9e5319b6d

https://www.android-mt.com/news/alerte-virus-xenomorph-de-retour-pour-piller-votre-argent/152435/

https://www.welivesecurity.com/fr/2018/11/06/logiciels-malveillants-1980-morris/

https://fr.wikipedia.org/wiki/Code_Red

https://fr.wikipedia.org/wiki/Cabir

https://www.varmatin.com/vie-locale/la-prison-de-draguignan-victime-dun-virus-informatique-822231

https://www.kaspersky.fr/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Expérience personnelle