LA LUTTE DU SIÈCLE VIRUS D'INFORMATION VS SÉCURITÉ DE L'INFORMATION

Valentina ASTAFI[1*], Ana Maria VECHIU[1]

[1]*Université Technique de Moldavie, Faculté Ordinateur, Informatique et Microélectronique, Département Génie Logiciel et Automatique, gr.FI-191, Chișinău, Moldova*

*L'auteur correspondant: Astafi Valentina, astafi.valentina@isa.utm.md

Résumé: *Dans le contexte de l'évolution rapide des technologies de l'information, les confrontations provoquées par la cybersécurité ont commencé, au fil du temps elles se sont amplifiées. Cela crée le besoin d'améliorer la prise de conscience et la sensibilisation des gens, en se référant au processus de développement des technologies de l'information et de la communication (TIC). Nous devons accroître notre capacité à répondre aux cyberattaques qui nous touchent tous directement.*
Malheureusement, ces menaces se sont déjà propagées au-delà des frontières personnelles et affectent non seulement la sécurité et la stabilité, mais aussi notre propre prospérité et notre équilibre émotionnel. Chaque utilisateur a besoin d'assistance pour pouvoir utiliser et naviguer en toute sécurité parmi ces technologies.

Mots clés: *technologie de l'information, virus, sécurité, antivirus, informatique, systèmes, programmation, espionnage, protection*

Introduction

Chaque jour, le monde change, les progrès s'accroissent à un rythme rapide, s'accélérant en avant, mais en même temps nous donnant des raisons de questionnement, et d'insécurité, des visions radicales entre générations, pour voir les effets majeurs de la mise en œuvre des innovations. Un aspect spécial et assez important est occupé par toute la sécurité de l'information et des stratégies / méthodes pour combattre toutes les attaques possibles. Les virus dit informationnels sont ceux qui nous donnent des maux de tête, quelle que soit la situation ou les raisons cachées. Ils pénètrent les profondeurs de toute cette sphère et pénètrent profondément dans le système [1]. Cela fait un moment que je n'ai plus de virus, nous avons appris à vivre ensemble. Les choses ont changé si vite que ceux qui gèrent les problèmes, c'est-à-dire ceux qui sont responsables de la sécurité des systèmes, n'ont pas le temps de parler de leur travail. Lancer une machine informatique, sur laquelle nous comptons toujours, peut un jour nous apporter des surprises. Même les programmes antivirus ne peuvent pas nous protéger complètement contre tous les problèmes. Maintenant, il semble que les choses soient devenues plus claires, ou du moins que la protection contre eux soit devenue une partie intégrante de la sécurité informatique, grâce aux travaux du Virus Security Institute, formé par des chercheurs de renommée mondiale.

Aujourd'hui, la sécurité informatique signifie: protection des systèmes et services offerts contre tout dommages naturels et artificiels; garantir les performances du système pour remplir correctement ses fonctions; assurer à l'utilisateur que le programme lancé n'ait pas d'effets secondaires [2].

Courte Histoire

Le premier virus a été lancé en 1971 et était connu sous le nom de Creeper. Le but de la conception était expérimental, son créateur était un employé du département informatique du gouvernement américain.

Creeper lui-même n'a eu aucun effet négatif, il a juste affiché un message sur les moniteurs: "Je suis Creeper, attrape-moi si tu peux!" et est installé à l'intérieur du réseau ARPANET. Et pour permettre de le détruire, un autre programme appelé Antidote a été créé, "The Reaper", maintenant connu sous le nom d'antivirus.

Il existe un autre virus appelé Elk Cloner, qui à son tour a été écrit par Rich Skrenta en 1982. Sa propagation était assez simple, il était attaché au système d'exploitation Apple DOS, à savoir dans le secteur de démarrage des disquettes, puis est installé sur l'ordinateur. Son mode d'action était le suivant, Elk Cloner affichait divers messages à l'écran et faisait clignoter l'image d'innombrables fois [3].

Virus et leurs classifications

Les virus d'information sont de petits logiciels malveillants spécialement créés avec des fonctions destructrices et l'incorporation de ses enfants dans d'autres programmes, qui interfèrent avec le fonctionnement normal d'un ordinateur s'installant sans le consentement de l'utilisateur, causant des dommages au système d'exploitation et aux matériels (physique) de l'ordinateur. Ils sont créés dans les mêmes langages de programmation et IDE que tout autre programme. Pour la personne qui a créé le virus, il s'agit d'un programme avec une valeur positive, tandis que pour l'utilisateur moyen, c'est un virus [4].

Classifications par mode d'infection: fichiers infectant des virus; virus de virus système ou de démarrage; infections virales de répertoire;

Les virus infectent les fichiers en attachant leur propre code à ce fichier, modifiant ainsi les informations du fichier. Les infections de virus système ou de démarrage affectent le contenu des secteurs de codage 0 et 1, ils se cachent dans ces secteurs, et déplacent leur contenu ailleurs, et établissent la connexion appropriée avec l'utilisateur, afin que nous ne nous en rendions pas compte. Lorsque le système démarre, le virus prend le relais et déforme le DOS aux adresses modifiées par celui-ci, sinon le système ne démarrera pas [2].

Les virus infectant les répertoires modifient les entrées des répertoires, ils ne modifient pas les fichiers et ne prennent pas le contrôle avant leurs exécutions.

Selon les particularités de l'algorithme de travail:

- Virus résistant (virus résident)
- Virus invisible (virus furtif)
- Virus polymorphe
- Spyware (virus de logiciel espion)
- Virus morphique (virus morphique)
- Virus non résistant (virus Runtime)

Effets sociaux et juridiques

Les ordinateurs personnels sont conçus pour un seul utilisateur, et tous n'ont pas de système de protection élevé. Dans certaines situations imprévues et involontairement, une personne peut accéder aux informations de notre ordinateur et peut les modifier ou les supprimer du disque dur. Pour accéder à un seul et même ordinateur, il faut également revoir les normes de sécurité. Les mesures générales peuvent être classées en 3 niveaux: protection du système; protection des programmes; protection des données;

La protection au niveau du système consiste à interdire l'accès aux personnes non autorisées en demandant à l'utilisateur d'entrer un mot de passe pour accéder au système. Cette façon de protéger les programmes contribue également à la protection contre les virus.

De cette manière, un utilisateur qui utilise des programmes infectés, n'ayant pas le droit d'écrire uniquement dans l'espace qui lui est accordé, ne peut infecter que cet espace [5].

La protection des données stockées dans les systèmes informatiques se fait par la méthode de cryptage, la plus simple étant la permutation circulaire de l'alphabet utilisé (Exemple: au lieu de A, il s'écrit C, au lieu de B, il s'écrit D). Aujourd'hui, plusieurs méthodes de cryptage sont utilisées et considérées comme sécurisées: DES (Data Encryption Standard) et RSA (Rivest Algorithm, Shamir, Adleman) [6].

Sources d'infection

Pour pouvoir combattre efficacement les dangers qui nous attendent, nous devons les connaître de tous les points de vue possibles. Connaître les scénarios possibles nous permet de mieux se protège contre eux, et ainsi nous pouvons minimiser les dommages qu'ils causent.

Les souches infectieuses agissent via un programme, le vecteur porteur du virus est un programme, un paquet de données ou une disquette. Sources d'infection:

a) Utilisation de programmes d'origines illégales - Programme illégal ou copie piratée d'un logiciel qui n'a pas été enregistré, afin que nous puissions utiliser les programmes gratuitement, seul l'utilisateur assume le risque de la confiance accordée à celui qui a volé le programme.

b) Système de tableau d'affichage (BBS)- Les bibliothèques de programmes qui peuvent être contactées par modem dans le cas des BBS, ou qui peuvent être contactées via Internet, peuvent être des sources d'infection.

c) Courriel - Non seulement les caractères ASCII sont transmis par courrier électronique, mais ils peuvent également servir de moyen de propager un virus et de l'activer via des messages électroniques.

d) Sabotage - Le sabotage des employés d'une entreprise est l'exposition la plus fréquente à la sécurité des systèmes / réseaux informatiques. Les conflits qui peuvent survenir conduisent à des manipulations d'informations.

e) Terrorisme - Attaques terroristes contre la société de l'information, pénétrant le réseau, essayant de détruire les réseaux et les données stockées.

f) Espions - Un programme antivirus peut être introduit dans le réseau assez facilement, étant doté d'une intelligence assez élevée, il se propage assez rapidement, avant d'être notifié, une fois qu'il entre dans le réseau, il est pratiquement impossible de l'éliminer.

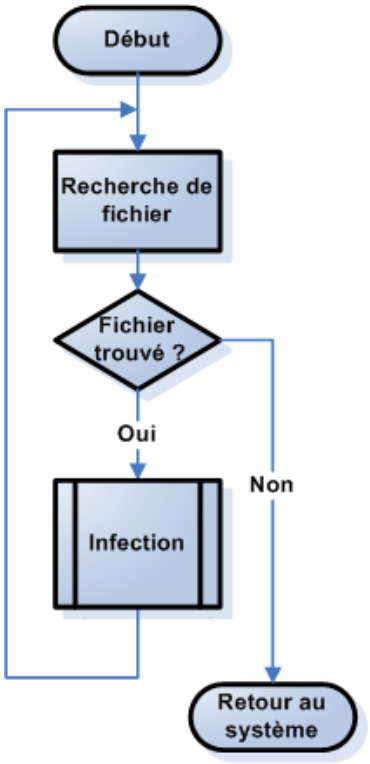

Figure 1. Schéma d'infection par un virus simple

g) Systèmes financiers - Les plus souvent exposés aux risques. Pour les hackers, il n'y a pas de code indéchiffrable ou de mot de passe inconnu. Ils entrent dans le système bancaire en détectant les lacunes du système de protection, puis ils peuvent manipuler sans limite une fois entré dans le système [2,7].

Programmes antivirus

Les programmes antivirus sont diverses applications spécialement développées pour la prévention et la suppression des virus informatiques, des vers et des chevaux de Troie, ainsi que pour la détection et la suppression des logiciels publicitaires, des logiciels espions et des logiciels malveillants. Les méthodes de protection, de détection et de désinfection peuvent être passives et actives. *Méthode passive* - si le lancement du programme de prévention dépend de l'utilisateur

Méthode active - si, après l'installation, le programme devient gourmand en mémoire et exécute des fonctions antivirus dans tous les cas lorsque le système d'exploitation ou un programme effectue des opérations d'écriture / lecture sur tous les lecteurs de disque.

Les méthodes utilisées par les progiciels sont les suivantes: méthode de détection des séquences d'identification; méthode de vérification de l'intégrité des fichiers; méthode de recherche -sheistic; méthode de protection multiple.

Ces méthodes se sont développées avec l'avènement de générations de virus, avec l'émergence d'un nouveau virus qui passe tout niveau de détection connu jusqu'au moment de l'émergence - une nouvelle technique de détection et de désinfection doit être développée.

Les programmes antivirus nous protègent contre de nombreux virus mais pas contre tous les programmes destructeurs [8].

Conclusion

Les technologies ont changé et continueront de changer la façon dont la vie est organisée, menée et exploitée à tous les égards. Ainsi, le développement progressif des technologies de l'information nous oblige à adapter notre réflexion et nos ressources en fonction des besoins

D'une manière générale, il est difficile d'observer et de découvrir ce qui vous semble normal, à première vue, étant un simple programme informatique. Ceux qui conçoivent des virus informatiques sont des programmeurs expérimentés. Dans le domaine de la technologie, il est difficile et parfois même impossible de rester en sécurité, de ne jamais faire face à un virus informatique, d'avoir un assortiment d'applications, qui peuvent présenter des failles de sécurité, à travers lesquelles d'autres personnes peuvent contrôler certaines applications et appareils. Tout appareil possède une protection contre les virus. Cependant, il n'existe pas de protection parfaite.

La protection antivirus est une méthode d'auto- amélioration, elle est nécessaire jusqu'à ce que les utilisateurs protestent contre l'architecture matérielle existante et les systèmes d'exploitation inadéquats et forcent les fabricants à concevoir des ordinateurs de manière qu'ils soient faciles à utiliser, à protéger et invulnérables aux attaques de virus. Les nouvelles générations de programmes antivirus sont toujours à la recherche de niches par lesquelles échapper à la vue des programmes antivirus, trouvant ainsi plus de surfaces d'attaque, inventant de nouvelles techniques de propagation et implicitement de nouvelles technologies de programmation.

Compte tenu du contexte épidémiologique dans lequel nous nous trouvons, la quasi-totalité des services ont été mis en ligne, et il nous reste à nous adapter et à survivre à toutes les révolutions technologiques mises en œuvre pour un meilleur fonctionnement et une meilleure existence.

Références:

1. Vârjan Daniela. Internet change la face du monde; [Accédé le 10.02.21], sur le site web: http://store.ectap.ro/articole/895_ro.pdf
2. József Vásárhelyi, Zoltán Kása; Mythe et vérité sur les virus PC, Maison d'édition bleue, Cluj Napoca,1996, 231 p, ISBN 9739215238;
3. Ressource électronique. Guide électronique de la cybersécurité. [Accédé le 10.02.21], sur le site web: https://www.competentedigitale.ro/it/it_virusi.php
4. Logiciel malveillant. [Accédé le 11.02.21], sur le site web: https://www.wikiwand.com/ro/Software_r%C4%83u_inten%C8%9Bionat
5. Mihaela Capmare,Dumitru Lazar; Projet de compétences en recherche: virus informatiques; [Accédé le 10.02.21], sur le site web: https://idoc.pub/documents/virusi-de-calculator-mwl11og5x1lj
6. Vasii Elena; Introduction à la science de l'information, 2004, Maison d'édition de l'Université d'Oradea, 240 p, ISSN 973-613-755-4.
7. Dictionnaire informatique électronique [Accédé le 11.02.21], sur le site web: https://web.archive.org/web/20140108053635/http://www.malwarecity.ro/site/Main/listDictionary
8. Dumitru Oprea; Protection et sécurité des systèmes d'information, 2017,190 p; [Accédé le 11.02.21], sur le site web: http://www.feaa.uaic.ro/doc/l2/ie/Securitatea%20sistemelor%20informationale.pdf