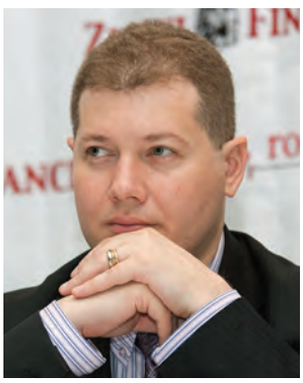
Cybersecurity Trends

Numéro spécial / Numero speciale

CE VOLUME VOUS EST OFFERT PAR :
QUESTO VOLUME VI È OFFERTO DA :

CLUSIS
Association Suisse de la Sécurité de l'Information

Les menaces de type „Ransomware"



Aurelian Mircea Grigore,
Membre actif d'ISACA Roumanie et membre collaborateur de l'ANSSI

Toma Cîmpeanu,
CEO de l'ANSSI (Association Nationale pour la Sécurité des Systèmes Informatiques)

Les logiciels malveillants existent sous une des formes très variée, comme les key-loggers, les virus, les vers, des chevaux de Troie, les ransomwares, les logiciels espions, les publiciels ou encore les botnets, pour n'en nommer que quelques-uns.
Le logiciel malveillant peut être incorporé dans différents types de fichiers et peut être activé simplement en accédant au dossier infecté ou à un lien figurant dans un courrier électronique.

Ces programmes peuvent aussi être „plantés", intentionnellement ou accidentellement, dans des sites Web. Aussi, les logiciels malveillants peuvent se répandre via les logiciels de communication (courriers électroniques, chats, etc.), les supports mobiles d'archivage (unités de stockage USB le stockage, CD-roms, disquettes), le wi-fi, les dispositifs mobiles infectés, voire par un réseau entier compromis.

Le logiciel malveillant exploite les points faibles des systèmes des logiciels des systèmes d'exploitation (OS), des logiciels d'application, mais aussi les fragilités du hardware (par exemple certaines puces de l'ordinateur).

La complexité des logiciels fournit un avantage à tous ceux qui développent des logiciels malveillants, de sorte que les logiciels malveillants sophistiqués, et leurs utilisateurs, peuvent cacher leurs activités couvrir leurs traces en fournissant des adresses fausses, en déviant des trafics de données, en effaçant leurs activités (par exemple en supprimant des fichiers et des informations dans les journaux de logs), en disséminant des informations fausses ou en travaillant à l'extérieur du pays ciblé par leur activité.

Les logiciels malveillants polymorphes changent leur signature (par exemple le nom des fichiers et de leurs emplacements) et/ou d'autres indicateurs compromettants, de sorte que le logiciel antivirus ne puisse pas identifier les composants du programme pour les éliminer.

Quelques types de logiciels malveillants sont très difficiles à éliminer, parce qu'ils peuvent se cacher en modifiant les paramètres des fichiers et les permissions d'accès aux répertoires.

Dans quelques cas, certains logiciels malveillants donnent l'impression d'avoir été éradiqués, alors qu'ils se réinstallent tout seuls, au moment du redémarrage de l'ordinateur.

Le phénomène des logiciels malveillants est passé de la catégorie des événements simplement inquiétants ou dérangeants à celle des logiciels et des systèmes qui peuvent compromettre des ordinateurs gouvernementaux, capturer des informations d'accès ou peut encore voler de l'argent à un individu. Ceux qui contrôlent le logiciel malveillant peuvent obtenir des informations personnelles et financières, peuvent affecter les entreprises et les institutions financières, menaçant ainsi les moyens d'existence des individus et la richesse personnelle.

Les développeurs des logiciels malveillants ont créé des applications pour contrôler d'autres programmes dangereux ou des réseaux entiers d'ordinateurs infectés. C'est ainsi que sont apparus des réseaux d'ordinateurs et de terminaux de type botnet, contrôlés par des centres de commande et de contrôle (C & C).

Parmi les utilisations d'un bot ou d'un *botnet*, on soulignera:

- Le déclanchement d'une attaque de type *distributed denial-of-service* (DDoS), qui peut transmettre des flux importants de paquets *User Datagram Protocol* (UDP), des demandes Internet au *Message Protocol Control* (ICMP) ou des requêtes synchronisées au *Transmission Control Protocol* (TCP).

- L'infection d'autres ordinateurs d'un réseau par la prise de contrôle intégrale d'un appareil victime.
- L'utilisation et le partage de grandes quantités de largeur de bande dans le cas des communautés de hackeurs.
- L'installation d'un *backdoor* pour en maintenir l'accès après une première exploitation réussie.
- L'hébergement de données illégales sur un système en l'intégrant dans un réseau de partage d'informations illégales (logiciels ou films piratés).

Pour infecter ou compromettre un système informatique, une attaque cybernétique passe par trois phases:

1 **Pré-compromission** – cette étape consiste à:
a. Identifier la cible ou de la victime
b. Personnaliser des programmes malveillants destiner à provoquer des dommages, obtenir des données et espionner la cible.
c. Etablir d'un moyen d'accès.

2 **Compromission** – pendant cette étape, le système-cible est exploité à l'avantage de l'attaquant (hacker) et, ensuite, le logiciel malveillant est installé sur les systèmes vulnérables.

3 **Post-compromission** – une fois que les systèmes vulnérables du réseau sont compromis, l'attaquant établit un centre de C&C pour diriger ses futures attaques cybernétiques.

Les infracteurs cybernétiques n'utilisent pas seulement des programmes malveillants pour avoir accès aux informations du propriétaires, sensibles et personnelles, mais aussi pour appliquer des techniques de type *„piggy-backing"* pour:

- Capturer les informations d'accès au e-banking.
- Transmettre des sources et des destinations d'Internet Protocol (IP) ainsi que des listes de courriels.
- Manipuler des sites de jeu de hasard en ligne, à leur avantage.
- Surveiller les pratiques inadéquates de l'actualisation des systèmes.
- Etudier les habitudes et les routines de navigation de la cible.
- Capturer les activités de navigation par les systèmes mobiles de la cible.
- Etudier les réseaux sociaux et les sites de messageries utilisés par la cible.

Les pratiques inadéquates de programmation et le temps à disposition ont permis aux infracteurs cybernétiques de devenir très organisés, et, conscients du fait que bien des gens ne disposent pas de la meilleure sécurité possible, ils ont commencé à viser les personnes les moins préparées.

L'évolution du Ransomware

L'utilisation, de la part des criminels, des instruments de ransomware et les résultats obtenus ont naturellement conduit au développement et à la diversification de ce type de programmes malveillants. Au cours de quelques mois seulement, les chercheurs ont rapporté, pour la première fois, **un ransomware capable de crypter des fichiers sans connexion à internet**, ne nécessitant plus aucune communication avec les serveurs C & C des malfrats tout au long du processus de cryptage.

Bio - Aurelian Mircea Grigore

Aurelian Mircea est actif depuis 15 ans dans le domaine de la cybersécurité, avec une vaste expérience accumulée durant son parcours professionnel. Il a occupé des fonctions d'administrateur de système, de spécialiste en technologies de sécurité, de consultant en sécurité informatique, d'auditeur de systèmes informationnels
Il a de même développé des services de sécurité cybernétique pour les infrastructures critiques, les systèmes de contrôle et SCADA industriels, mais aussi pour les institutions publiques, bancaires et les PME. Il a participé à la traduction et à l'adaptation des standards de sécurité pour l'ASRO, est membre actif d'ISACA Roumanie et membre collaborateur de l'ANSSI. Il a collaboré avec la fondation CAESAR set la task force de l'AMCHAM pour la promotion de la sécurité cybernétique.

Bio - Toma Cîmpeanu

Toma Cîmpeanu a été chef de promotion pour ses BSc à la Faculté de Mathématiques et à la Faculté d'Automatisation et des Ordinateurs. Il a un doctorat et un master dans les systèmes de coordination et de contrôle, ainsi qu'un MBA en administration d'entreprises. Dans les derniers quinze ans, il a occupé des postes de direction dans plusieurs sociétés privées ou gérées par l'État, comme SN Radiocommunicatii, TAROM, Informatica Feroviara, ou encore auprès des groupes SCOP Computers, eSign România et TotalSoft.
Il a été Secrétaire d'État au Ministère des Télécommunications, représentant roumain et membre du Conseil de l'ENISA, Président de l'Agence Nationale des Services de la Société de l'Information et vice-président du Centre national „Roumanie Numérique". Son nom est lié à la stratégie eRomania, au système national de „e-appels d'offre" et au „Point de Contact Unique" de l'Etat. Toma Cîmpeanu a aussi enseigné à l'Université de Craiova et a dirigé les opérations de l'Institut de Management et de Développement durable, la seule ONG roumaine qui a coordonné au niveau global un groupe de travail de l'ONU. En 2015, il est le CEO de l'ANSSI (Association Nationale pour la Sécurité des Systèmes Informatiques).

Parmi les nouveaux instruments recensés, nous remarquerons le ***Locky*** ransomware, dont le mode opératif ressemble au cheval de Troie bancaire ***Dridex***, mais aussi une nouvelle variante du ***CTB-Locker*** qui attaque les serveurs internet. Le CTB-Locker vise des sites web WordPress, dont il crypte les fichiers pour demander ensuite au propriétaire de payer une rançon pour les récupérer.

Par ailleurs, les offres de ***RaaS*** (Ransom-as-a-Service) sont de plus en plus populaires sur les sites fermés du Deep-Web et les forums Darknet. Ces services permetternt aux attaquants potentiels de créer facilement des souches de ransomwares, dont les profits seront issus des prochaines infections réussies. Ainsi, on a identifié il y a peu un nouveau RaaS „baptisé" ***Cerber*** ransomware, qui est proposé par un forum souterrain de Russsie. Avant lui, on trouvait ***ORx-Locker***, offert comme service par l'intermédiaire d'une plateforme hébergée par un ***onion server***.

Le ransomware est un phénomène en pleine explansion, et peut prendre de nouvelles formes, y compris les traditionnels liens postés sur les courriels ou les sites de phishing.

L'utilisation de JavaScript dans le Ransomware

Les chercheurs en sécurité ont découvert une nouvelle variante de *Ransomware-as-a-service:* ***Ransom32***. Elle se distingue des autres, y compris des célèbres ***Tox*** et ***FAKIN***, par une différence majeure: elle utilise un framework JavaScript nommé NW.js. Computerworld a signalé cette évolution au courant du mois de janvier déjà. **Ransom32** demande à ses victimes de payer une rançon dans un délai de quatre jours, faute de quoi, au terme d'une semaine, le disque dur tout entier sera détruit. Le problème réside dans le fait que NW.js est un framework légitime, ce qui rend compliqué l'ajout de Ransom32 parmi les solutions de détection de programmes de malware basés sur des signatures. Les acteurs du marché de la sécurité rapportent que nombre d'entre eux n'ont pas eu une couverture de détection suffisante durant les premières semaines suivant la découverte du logiciel.

Le Ransomware, en plein boom

L'an dernier, les attaques ransomware et les menaces connexes ont connu une croissance significative, aussi bien en raffinement qu'en quantité. Les variantes précédentes de ransomware ont souffert, pour les criminels qui les utilisent encore, une dépréciation de 10 à 30 % en termes de profit, tandis que Ransom32 a augmenté le bénéfice de 25 la %.

Jusqu'à ce jour, Ransom32 n'a été observé que dans l'infection de PC de type Windows, mais il serait naïf de s'attendre à ce qu'il reste limité à cet OS durant longtemps, les cybercriminels étant connus pour leur talent à créer des paquets pour Linux et Mac afin d'élargir leur spectre d'action.

Cerber Ransomware – Nouveau, mais déjà mûr

Un nouveau ransomware cryptographique, nommé ***Cerber*** par ses créateurs, a récemment commencé à viser les utilisateurs de Windows.

Le comportement de Cerber est similaire à celui de la majorité des ransomwares:

- Il code une vaste gamme de fichiers du système (y compris les „shares" de Windows et de réseau) avec un cryptage AES-256, auquel il ajoute l'extension .cerber
- Il évite d'infecter des utilisateurs dans la plupart des états de l'ex-URSS
- Il présente des „factures" de rançon avec instructions sur les modalités de paiement (au début, il demandait 1,24 Bitcoin), et offre la possibilité de décrypter un fichier comme signe de bonne volonté.

Un autre phénomène intéressant est le fait que Cerber n'est pas propagé par ceux qui l'ont développé. En échange, ils l'offrent comme „service" aux visiteurs d'un forum souterrain fermé de Russie.

Jusqu'à aujourd'hui, les victimes n'ont eu aucune possibilité de décrypter elles-mêmes les fichiers, aussi bien que celles-ci soit paient la rançon et **espèrent** que les infracteurs vont leur envoyer la clé de décryptage, soit ils se résignent à renoncer à jamais à leurs fichiers.

KeRanger – Un nouveau ransomware qui vise pour la première fois les Macs

Les hackers ont infecté des Macs avec le ransomware ***KeRanger*** par une copie contaminée de Transmission, un programme populaire pour le transfert de données par l'intermédiaire de réseaux de partage de fichiers peer-to-peer de type BitTorrent.

KeRanger, qui bloque les données sur les Macs, les rendant inaccessibles à leur propriétaire, a été téléchargé près de 6500 fois avant qu'Apple et ses développeurs ne soient capables de le contrer. Dans ce sens, les experts en cyber-sécurité prévoient, pour les prochains mois, une croissance d'attaques portant sur les Macs.

Distribution des ransomware

La plus grande partie des vecteurs de distribution de souches ransomware impliquent l'usage de l'ingénierie sociale. Par exemple, on utilise des courriels, des fichiers Office malveillants, des messages de type spam avec liens malveillants ou encore des campagnes de publicité nocive qui exploitent les sites WordPress vulnérables ou les sites Joomla avec un code malware incorporé. De même, la distribution profite de l'avantage des commandes macro et des kits d'exploits (exploit kits), comme Nuclear ou encore Angler. Quelquefois, ils exploitent les vulnérabilités du browser ou utilisent des certificats numériques volés.

La manipulation des attaques Ransomware

Une vague d'attaques ransomware a été observée au niveau global, avec un grand nombre d'infections rapportées aux U.S.A., en Grande-Bretagne, en Allemagne et en Israël. Les attaquants ne semblent pas avoir un objectif spécifique, les cibles étant très différentes entre elles: hôpitaux, institutions financières, entreprises, sans pour autant que l'on puisse identifier un type d'industrie visée de façon plus intensive que d'autres.

Ci-après, vous trouverez nos suggestions sur les actions recommandées pour éviter les attaques de type ransomware, mais aussi les modes adéquats de réaction après une infection.

Défendez votre entreprise contre les attaques potentielles

▸ Entraînez vos employés – la composante humaine est le maillon faible de la cyber-sécurité des entreprises ; la majorité des attaques implique l'utilisation de l'ingénierie sociale visant un ou plusieurs employés. Etablissez des règles concernant l'utilisation des systèmes de l'entreprise et montrez des exemples réels de messages de phishing, afin que tous sachent les reconnaître.

▸ Augmentez le degré de prise de conscience en ce qui concerne l'acceptation de fichiers attachés aux courriels: instruisez vos employés afin qu'ils n'ouvrent pas des pièces attachées à des courriels reçus de la part d'expéditeurs inconnus. Une politique d'entreprise concernant comment aborder de tels fichiers. Nous vous recommandons le blocage ou l'isolement systématique de fichiers avec les extensions suivantes: .js (JavaScript), .jar (Java), bat (Batch file), .exe (executable file), .cpl (Control Panel), .scr (Screensaver), .com (COM file) et .pif (Program Information file).

▸ Désactivez les scripts macro qui sont installées sur des documents Office transmis par e-mail – durant les derniers mois, on a pu observer de nombreux cas d'attaques de type ransomware ayant utilisé les macros comme vecteur. D'habitude, les commandes Macro sont désactivées en mode implicite et nous ne recommandons pas d'en permettre la réactivation. De plus, nous vous suggérons d'utiliser le software Office Viewer pour ouvrir les documents Word et Excel que vous n'avez pas besoin d'éditer ou de retoucher.

▸ Limitez les privilèges des utilisateurs et surveillez constamment le parc informatique – une gestion attentive des privilèges des utilisateurs et des administrateurs peut aider à éviter la dissémination de ransomware dans le réseau de l'entreprise. Plus encore, surveiller l'activité du parc informatique vous sera utile pour déceler de façon précoce toute infection et bloquer sa multiplication dans d'autres systèmes et ressources du réseau.

▸ Créez des processus qui bloquent les programmes d'exécution de dossiers AppData / LocalAppData. De nombreuses variantes de ransomware sont exécutées par ces registres, y compris le CryptoLocker. En conséquence, la création de telles normes peut réduire le risque de cryptage de façon significative.

▸ Gardez vos systèmes constamment actualisés. Dans de nombreux cas, les hackers profitent de systèmes vieillis pour s'infiltrer dans le réseau. Des actualisations fréquentes des systèmes OS et la mise en œuvre de mesures de sécurité publiées peuvent réduire drastiquement les risques d'infection.

▸ Utilisez un software tiers spécialement dédié pour faire face aux menaces. Par exemple, AppLocker pour Windows, qui est inclus dans le système OS, aide à combattre les malwares. Nous vous recommandons de contacter un fournisseur de sécurité d'entreprise pour prendre en considération toutes les solutions qui sont aujourd'hui sur le marché.

Procédures à suivre si vous êtes infecté

▸ Restaurer les fichiers - certains instruments ransomware créent une copie du fichier, la cryptent et ensuite effacent le fichier original. Si l'effacement se réalise à travers les fonctions natives du système OS, il existe une chance de rétablir les fichiers originaux, puisque, souvent, le système d'opération ne réécrit pas immédiatement les fichiers.

▸ Décrypter les fichiers cryptés – le décryptage est possible si vous avez été victime de l'un de ces trois types de ransomware: Bitcryptor, CoinVault ou Linux.Encoder.1. En conséquence, l'identification du type et du genre exact du ransomware qui a attaqué votre PC est un élément crucial.

L'ANSSI – Partenaire permanent de Cybersecurity Trends

L'Association Nationale pour la Sécurité des Systèmes Informatiques a été fondée en 2012, pour constituer un pont entre le secteur public et l'environnement privé, promouvoir les bonnes pratiques et faciliter les échanges culturels dans le domaine de la sécurité de l'information.

L'association identifie et notifie les facteurs de risque de concert avec les autorités d'Etat en cas de déficiences dans le marché de l'IT, mais sa préoccupation constante est d'œuvrer à fédérer les formes de partenariats Public-Privé qui peuvent mener à l'augmentation de l'efficacité et de l'opérativité des systèmes informatiques existants en Roumanie.

L'ANSSI est une organisation non gouvernementale, sans but lucratif, professionnelle et indépendante. Elle rassemble 40 membres, à savoir des entreprises comptant un total d'environ 20,000 salariés, représentant 25 % du nombre total des employés du secteur privé actifs dans les TIC.

Les membres de l'ANSSI, par le grand spectre et la différence de leurs capacités techniques et professionnelles, forment ainsi un groupe représentatif au niveau sectoriel, dont les sujets d'intérêt reflètent les véritables préoccupations du domaine.

L'ANSSI est activement impliquée dans la société, organisant seule ou en partenariat avec les autorités et les institutions nationales ou les ambassades, des conférences et des colloques nationaux et internationaux, dans des domaines connexes comme ceux des communications électroniques, des solutions de e-gouvernance et de e-administration, l'accès aux outils structurels, le développement des standards professionnels, en bref tous les domaines dans lesquels la composante de sécurité technologique de l'infrastructure TIC constitue une préoccupation centrale.

▸ Effectuez des sauvegardes pour tous vos fichiers sur un dispositif d'archivage séparé, de façon régulière – une bonne pratique pour éviter les dommages produits par une attaque de type ransomware est de faire une sauvegarde de tous les fichiers importants sur un dispositif déconnecté du réseau de l'entreprise, puisque certaines variantes de ransomware sont capables de crypter des fichiers stockés sur des dispositifs tiers, connectés. Par exemple, les chercheurs ont rapporté récemment un ransomware qui crypte les fichiers stockés dans le dossier Cloud Sync.

▸ Si un ransomware est détecté dans votre entreprise, déconnectez immédiatement du réseau l'équipement infecté. Ne cherchez pas à éliminer malware et ne redémarrez pas le système avant d'avoir identifié la variante du ransomware. Dans certains cas, si vous effectuez l'une de ces actions, vous rendrez le décryptage impossible, même en payant la rançon. ■

web for your business
swiss webacademy

together with:

SecurityBrokers · intelSeCo · AGORA

Presents:

CYBERSECURITY IN ROMANIA CONGRESS
4th Edition

A Central European Public-Private Dialogue Platform

September 14-16, 2016, Sibiu, Romania

https://cybersecurity-romania.ro

Under the aegis and with the support of:

ITU

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

ROMANIA SRI Patria a priori SERVICIUL ROMÂN DE INFORMAȚII

ROMANIA CENTRUL NAȚIONAL CYBERINT SERVICIUL ROMÂN DE INFORMAȚII

IGPR POLIȚIA ROMÂNĂ

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

POLICE GENÈVE

CTS Centrul de telecomunicații speciale

CSC Centrul pentru Securitatea Cibernetică

RÉGION-IHEDN FRANCHE-COMTÉ

SIBIU COUNTY COUNCIL

Asociația Națională ANSSI

Romanian Association for Information Security Assurance

ANIS employers' association of the software and services industry

ULBS Universitatea "Lucian Blaga" din Sibiu

CLUSIS Association Suisse de la Sécurité de l'Information

Posteitaliane