Mesures anti-rançonnage numérique

1ère version du guide présentée au copil d'octobre 2020

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

TABLE DES MATIERES

EMERGENCE D'UN PHENOMENE DURABLE

Le rançonnage numérique est un phénomène qui émerge depuis quelques années et qu'on ne peut plus considérer comme cantonné aux USA : M6, Fleury Michon, CHU de Rouen sont des noms (extraits de la récente publication de l'ANSSI et du ministère de la Justice [1]) qui fleurent bon la France et qui témoignent de la réalité du phénomène et de la diversité des organisations victimes.

Pour savoir comment s'y préparer spécifiquement, il est nécessaire de comprendre pourquoi le phénomène est apparu, quels sont les facteurs qui concurrent à son développement, avant d'aborder les mesures concrètes.

FACTEURS INTERNES A L'ORGANISATION

La première raison de l'émergence des rançonnages numériques d'entreprises est la **dépendance accrue** des organisations à leurs systèmes informatiques. Pour reprendre l'exemple d'un CHU et pour caricaturer, il y a 20 ans, un hôpital utilisait un système informatique pour sa comptabilité, mais les ordonnances des médecins, les bilans de laboratoires restaient la référence sur papier. Une tentative de rançonnage numérique aurait été vaine faute d'otage.

Avec la dématérialisation de ces actes, l'informatique est devenue ce qu'elle aspirait à être : le système d'information central de l'organisation. Quand le « SI » est bloqué, c'est maintenant l'usine, la production, la distribution ou les services qui s'arrêtent. Mais comme l'évolution a été progressive, les systèmes informatiques n'ont pas toujours été adaptés aux nouvelles exigences de résilience qui en résultaient. La meilleure preuve est que si les bilans comptables font l'objet de plans de contrôles externes (commissaires aux comptes, cours des comptes) pour s'assurer d'une certaine véracité des comptes, les cyber-audits *indépendants* sont rarement *institutionnalisés*.

Ensuite les systèmes informatiques se sont exposés par un certain nombre de « **pratiques de confort** ». Avant l'an 2000, une salle informatique était encore souvent équipée de consoles, écran & clavier, où les informaticiens venaient configurer « in situ » les serveurs. Du fait de la climatisation, c'était des conditions de travail exposant au froid et au bruit.

Aujourd'hui, l'**administration de serveurs** se fait presque exclusivement **à distance**, dans des bureaux du même site ou plus souvent hors site. Et alors que la sécurité physique venait seconder la sécurité informatique (il fallait être sur site, dans la salle, avec une entrée verrouillée par un badge ou une clé), la sécurité logique se retrouve exposée à nu. Les mots de passe qui suffisaient car agissant comme des codes PIN d'une carte bancaire deviennent des faiblesses coupables et exploitables depuis tous les postes de travail de l'entreprise.

Car dans le même temps, les organisations ont souvent pris le parti de **ne pas cloisonner leurs réseaux internes**. En contre-exemple, si on observe un ensemble immobilier constitué d'une centaine d'appartements, il y a aussi plusieurs centaines d'ordinateurs, d'ordiphones et équipements réseaux divers (imprimantes, appareils connectés de tous types). Par contre, si depuis Internet un attaquant arrive à pénétrer le réseau d'un appartement, cela ne lui donne aucun avantage pour pirater celui du voisin d'étage.

A contrario, dans la plupart des organisations, les réseaux WAN sont construits « à plat », où chaque machine voit toutes les autres, avec des restrictions minimes. Il est de notoriété publique que les attaques sur Saint-Gobain ou Altran ont pris racines dans des filiales d'Europe de l'Est (Ukraine et Roumanie respectivement). Pour le management, le nœud du problème est de prendre conscience que, si un montage juridique en filiales à responsabilité limité, protège le capital et les bénéfices de la maison mère, il n'y a pas souvent de cloisonnement numérique équivalent.

Un dernier facteur explique la fréquence des actes de rançonnage. Les parcs informatiques d'entreprises présentent de grandes similarités. Ils sont presque exclusivement constitués de machines Windows, associées à des Active Directory (AD). D'abord conçu comme un système de management local, les AD ont généralement adopté une architecture centralisée avec des parcs de plusieurs milliers voire plusieurs dizaines de milliers de PC pilotés par un **Active Directory unique**. Le contrôle des machines cœur (les contrôleurs du domaine) est devenu un **point névralgique** du SI.

CHEMIN TYPE DE PENETRATION

Même lorsque la première infection est difficile à reconstituer par faiblesse de la journalisation d'événements, la plupart des rançonnages suivent un chemin très semblable

Le plus souvent, la tête de pont est créée par **phishing**. Un collaborateur de l'organisation est invité à cliquer sur un lien ou directement une pièce jointe qui comporte une charge capable de compromettre un PC individuellement.
Pour les métiers qui ont pour vocation la relation avec les clients ou usagers, les secrétariats également, il est illusoire de penser qu'aucun PC ne sera vérolé dans l'organisation, même par des rappels réguliers à « l'hygiène informatique ». La discipline individuelle est nécessaire mais pas suffisante pour lutter contre des épidémies.
Il faut bien sûr *lutter contre le phishing* (et nous renvoyons aux *tests d'autodiagnostic* déjà mis à disposition les années précédentes sur https://ssi.economie.gouv.fr pour sécuriser les flux de messagerie). Tenir un *décompte du nombre de machines reformatées* pour cause de virus est aussi une *excellente mesure de salubrité* informatique, car elle permet de valider les progrès. Mais il ne faut pas s'auto-convaincre qu'on n'aura jamais la grippe sous prétexte qu'on n'en a pas fait depuis 10 ans. Il y aura des messages de phishing qui feront mouche, si l'attaquant est un peu déterminé.

D'ailleurs, comme la criminalité traditionnelle, les groupes cybercriminels sont structurés par spécialité. Equivalent du braqueur, le spécialiste du phishing revend l'accès clé en main à des PC d'entreprises vérolés. Il passe la main au spécialiste de la **prise de contrôle d'AD**. Si le phishing est largement automatisée, il faut des capacités d'adaptation pour découvrir les rebonds et points d'appui qui vont permettre de progresser au sein des LAN et des WAN. L'*équivalent du perceur de coffre-fort* fait son miel des mots de passe et des hashes trouvés dans des fichiers (notamment les fichiers partagés trop librement par les documentations du support informatique) ou des outils d'analyse mémoire comme Mimikatz. A ce propos, même des

administrateurs chevronnés n'ont pas conscience que lorsqu'ils se connectent avec des droits d'administrateurs de domaine (superadmin) sur un serveur, ils laissent une empreinte qui suffira à un attaquant pour usurper leur identité auprès d'autres serveurs. Même s'ils utilisent des cartes à puce, ces jetons d'accès existent parce que l'AD n'utilise pas de la cryptographie asymétrique de bout en bout, comme SSH le fait par exemple.

Le secret de polichinelle des auditeurs AD est que, **dans 80% des cas**, un spécialiste motivé (attaquant ou un alter ego auditeur) va réussir à escalader ses **droits jusqu'au niveau d'administrateur de domaine, en moins d'une semaine**. Cela peut sembler étonnant tant les mouvements de l'attaquant à l'intérieur du réseau sont semblables à ceux d'un visiteur qui furète et tente d'ouvrir toutes les portes dans les étages d'un immeuble mais la plupart du temps, aucune alerte n'est levée.

A partir de la compromission des contrôleurs de domaines, l'attaquant peut faire faire à peu près ce qu'il veut à toutes les machines du parc. Pour préparer l'étape suivante, il va probablement désactiver les anti-virus, bloquer les mécanismes de sauvegardes, désinstaller Windows Defender etc. Mais le plus souvent, le témoin sera passé à un autre acteur de la bande, le « cerveau » et trésorier chargé du rançonnage proprement dit, avec paiement en crypto-monnaie.

La prise en otage se manifeste généralement par un chiffrement des disques durs de l'ensemble du parc, mais certains attaquants exfiltrent les données pour ajouter le chantage à la divulgation de données. Comble de l'ironie, le rançonneur **déploie un agent sur chaque machine**, généralement avec les propres fonctionnalités de l'AD. A l'heure de sa préférence (les attaques ont **généralement** lieu **le week-end** pour éviter des administrateurs trop présents qui surveilleraient les journaux en direct), il lance le chiffrement de tous les disques.

Pour opérer, les attaquants n'utilisent que des *moyens largement disponibles à faibles coût* : PC avec Windows, Internet, quelques serveurs relais dans le « cloud » pour masquer leurs traces, codes en libre circulation. On ne parle que des attaques qui ont réussi mais il y en a probablement plus qui échouent à divers stades. Etant donné que pratiquement aucun groupe de criminel n'a fait l'objet de condamnation en justice, il est **logique et raisonnable de penser que le nombre d'attaquants ne va pas diminuer**, d'autant que les crypto-monnaies facilitent l'anonymat et la répartition des gains entre membre des gangs.

MESURES

A chaque étape, il est possible d'entraver ou au minimum de gêner la progression de la bande de cybercriminels. Mais comme nous allons le voir, il faut adopter un dispositif de défense en profondeur car un bon attaquant est tout à fait en position de s'adapter et de contourner les protections. Ce n'est pas l'occasion non plus de ressasser tous les mots d'ordre de l'hygiène informatique, mais de se focaliser sur les mesures

réalistes[1] qui ont le plus grand impact pour rendre réellement improbables et infructueuses les attaques pour rançonnage.

Sauvegardes et suites anti-virus

Les unes comme les autres sont **indispensables**. Les sauvegardes protègent des rançonnages par chiffrement mais aussi des multiples causes de défaillances dans l'exploitation des données. Nous renvoyons au guide publié pour une campagne précédente du mois européen de la cybersécurité, récemment actualisé.
Les suites anti-virus luttent contre l'exécution de code malveillant. Certaines sont dotées de module pour reconnaître la réécriture en grand nombre de fichiers chiffrés et bloquer rapidement le processus.

Mais comme nous l'avons signalé dans le chemin type de pénétration, un attaquant peut désactiver les deux dispositifs. Il convient de soigner leur mise en œuvre mais aussi les compléter par d'autres dispositifs. D'autre part, les sauvegardes ne suffisent pas si l'organisation n'est pas en mesure de reconstruire son SI. Il y a des cas bien connus du milieu où une entreprise victime a essayé de reconstruire son SI depuis ses sauvegardes pendant plusieurs semaines avant de jeter l'éponge et payer la rançon, qui s'avérait le « meilleur choix économique ».

Une cyber-assurance protège encore moins des effets non directement économiques des attaques (et même parfois des conséquences financières quand il y a contestation comme pour NotPetya [2])

Silo d'administration

Il est tout à fait possible et même hautement souhaitable de retrouver une configuration qui offre les **mêmes conditions de sécurité que les anciennes consoles attachées directement aux serveurs**, en créant un *silo d'administration* (selon la terminologie Microsoft [3]).

Pour cela, les **consoles d'administration** des AD sont des *PC dédiés*. Les consoles ne sont pas utilisables pour recevoir des courriels ou naviguer sur le web. Les administrateurs s'y authentifient avec un clé physique (carte à puce sous différent format) + PIN. Les connexions aux contrôleurs de domaines passent par des canaux sécurisés (VPN de différentes natures). **Réciproquement**, les serveurs de domaines sont réglés pour n'accepter *des connexions que depuis les consoles dédiées* (point régulièrement oublié dans les configurations AD).

Consoles et comptes d'administration sont invisibles depuis un LAN bureautique. Pour les consoles, leur LAN est simplement injoignable. Pour les comptes Administrateurs de domaine, ils sont rendus *inutilisables pour de l'administration ordinaire* d'autres machines du domaine, y compris des serveurs (Exchange ou autre). Comme la discipline personnelle n'est pas un garde-fou à toute épreuve, cette règle est protégée par configuration (ACL déployée par GPO).

[1] Par exemple, en matière de supervision, il est toujours aussi insatisfaisant d'être dans le brouillard complet mais il est illusoire de disposer d'une armée d'informaticiens pour scruter les journaux de tous les équipements.

Cloisonnements internes

Le silo d'administration est un exemple extrême de cloisonnement interne. Mais il doit y en exister d'autres. Dans un bâtiment de grande taille, il existe des portes coupe-feux (entre étages ou en sein de l'étage, quand le bâtiment est horizontal comme Bercy) pour éviter qu'un incendie ne se propage à toute l'immeuble. Dans un réseau de grande taille, il faut également des pare-feux internes. Ceux-ci n'empêchent pas de s'envoyer des courriels ou d'utiliser des services partagés (bien protégés) mais il est important de freiner ce vecteur d'attaque parce que si un silo d'administration entrave le cheminement de cybercriminels, ils vont explorer les voies latérales : depuis un premier PC compromis à la comptabilité, le chemin vers le PC du PDG ne passe pas forcément par le contrôleur de domaine…
Une alternative ou plus exactement un complément aux cloisonnements des réseaux internes sont les pare-feux locaux, sur les postes de travail ou les serveurs. Vu l'état de départ de nombreuses organisations, ce chantier est sans doute un des plus longs. Mais comme dit le proverbe : plus vite on aura commencé, plus vite on aura fini.

Authentifications réciproques

Historiquement, les environnements Windows souffrent d'un défaut d'architecture. Il n'y a pas systématiquement authentification réciproque des machines, ce qui offre la possibilité à un attaquant de se faire passer pour le client ou le serveur selon ses besoins.

Avec Windows Server 2016, Microsoft a revu les configurations par défaut mais pour des AD construits avant, les configurations lâches sont le cas général. Augmenter sérieusement le niveau de sécurité réclame la *signature de tous les échanges du protocole SMB* [4]

Audits indépendants

Si les systèmes informatiques sont devenus si important pour la résilience des organisations, il faut que les pratiques de contrôle soient aussi à la hauteur. Il est couramment pratiqué des revues de sécurité pour des nouvelles applications. Pour les Administrations, la PSSI de l'Etat (2014) les a même rendus obligatoires, sous le nom d'homologation. Les infrastructures partagées n'ont pas souvent ce « traitement de luxe », même si les AD réunissent tous les critères d'un point névralgique pour l'organisation.

Surtout si elle n'a pas en propre la spécialité technique, la direction générale, doit mettre en place de mécanismes institutionnels d'audits et de contrôles indépendants de la DSI ou de l'infogérant, en particulier les mécanismes de défense en profondeur (silo d'administration, cloisonnements). Un **audit d'une semaine** par un véritable expert (l'ANSSI entretient une liste de prestataires d'audit agréés [5]) constitue une première étape pour **rester lucide sur le niveau de préparation** de l'organisation.

Purges des jetons et droits d'accès

Des attaques peuvent être à plusieurs stades de progression dans le SI. De ce fait, il n'est pas illusoire de penser que des implants ont capturé des jetons ou des droits

d'accès. L'expérience montre qu'une approche « champs vierge » où on reconstruit un nouvel environnement AD est difficile à mettre en œuvre parce que les activités de l'entreprises ne s'arrêtent pas. Par contre, un grand nettoyage de printemps des jetons Kerberos [6] est une manière de reprendre la main.

Et à la moindre suspicion, cette réinitialisation doit être combinée avec un changement de tous les mots de passe utilisateurs. Une bonne occasion de leur faire acquérir les bons réflexes pour des mots de passe solides, en s'étalonnant sur un indicateur réaliste, comme démontré lors de l'édition 2019 du mois européen de la cybersécurité [7].

SYNTHESE

Le rançonnage par compromission des Active Directory est un phénomène inquiétant. C'est un puissant révélateur des capacités d'anticipation et de mise en œuvre disciplinée des méthodes de sécurisations informatiques. Les organisations ont les moyens de s'en protéger pour peu qu'elles prennent conscience du danger et qu'elles donnent les bonnes impulsions.

REFERENCES

[1] https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
[2] https://www.argusdelassurance.com/tech/cyber-attaque-notpetya-zurich-attaque-en-justice-par-le-groupe-mondelez.140269
[3] silo d'admin https://docs.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos
[4] signature SMB partout, https://support.microsoft.com/fr-fr/help/887429/overview-of-server-message-block-signing
[5] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[6]purge Kerberos TGT, usage de la commande KLIST https://docs.microsoft.com/fr-fr/windows-server/administration/windows-commands/klist
[7] https://ssi.economie.gouv.fr/motdepasse

Contact : dssi.shfds[à]finances.gouv.fr
Diffusion Intranet : https://hfds-bercy.alize.finances.rie.gouv.fr/sites/hfds-bercy/accueil.html

HFDS Bercy