Computrace

Le 12 février 2014, deux experts en sécurité de Kasperky Lab, Sergey Belov et Vitaly Kamluk, ont posté un article intitulé « Absolute Computrace Revisited », consacré à un logiciel appelé Computrace (https://www.securelist.com/en/analysis/204792325/Absolute_Computrace_Revisited). On trouve ce papier traduit et résumé en français par Korben (http://korben.info/computrace-lojack-absolute.html).

Computrace est un logiciel espion créé par une entreprise américaine, Absolute, basée à Austin, au Texas. Il permet de prendre la maîtrise à distance d'un ordinateur, d'une tablette ou d'un smartphone. Tout est possible :

- examiner le contenu de l'appareil ;
- lire, écrire ou effacer les données qui se trouvent sur la mémoire de masse, y compris dans le Registry de Windows ;
- localiser l'appareil ;
- télécharger des fichiers (*download* et *upload*) ;
- installer ou désinstaller des programmes, etc.

Par exemple, il est possible d'activer « la capture des séquences de touches » (*keylogging*) [1], ce qui permet d'espionner tout ce que l'utilisateur tape sur son clavier, y compris ses mots de passe.

Sous Windows, pour savoir si on est infecté, on peut faire une recherche sur les fichiers qui composent le logiciel :

- rpcnet.exe
- rpcnetp.exe
- rpcnet.dll
- rpcnetp.dll
- wceprv.dll
- identprv.dll
- upgrd.exe

Computrace comprend aussi un implant intégré dans la ROM au moment de la fabrication de l'ordinateur. Ce module se charge de surveiller que les fichiers qui constituent Computrace sont bien présents. S'il détecte que ce n'est pas le cas, il réinstalle le logiciel. Les communications entre le serveur et l'appareil s'effectuent par le canal du navigateur (Internet Explorer, Firefox ou Safari).

L'implant fonctionne en mode SMM (*system management mode*), ce qui permet au logiciel de fonctionner même si l'ordinateur est éteint.

La ROM étant en lecture seule, on ne peut ni modifier ni effacer le code qu'elle contient (il s'agit de *firmware* et non de *software*). Il est donc impossible de supprimer Computrace.

---

[1] http://www.absolute.com/en/resources/datasheets/absolute-computrace, accès le 30 mai 2014.

Il existe toutefois un programme, Computrace Lojack Checker, qui semble capable d'empêcher le logiciel de fonctionner (http://sourceforge.net/projects/computrace-lojack-checker).

Normalement, le logiciel est activé par Absolute à la suite de la conclusion d'un contrat avec un propriétaire, l'objectif étant double :

- en cas de vol, donner au propriétaire la possibilité de retrouver son appareil.
- fournir à l'employeur un moyen de surveiller ses collaborateurs : selon la documentation d'Absolute, il est possible de créer « des alertes à envoyer aussitôt qu'une modification non autorisée est détectée » [2].

Si un ordinateur est déclaré volé à Absolute, l'entreprise peut le geler ou effacer tout son contenu. Elle collabore ensuite avec la police pour lui permettre de localiser l'appareil.

Belov et Kamluk ont découvert que Computrace fonctionne sur des ordinateurs qui ne sont pas enregistrés chez Absolute, et cela alors que l'utilisateur n'était même pas conscient que le logiciel se trouvait sur son ordinateur. Cela signifie que Computrace fonctionne sans autorisation sur un nombre inconnu d'ordinateurs, sans qu'on sache par qui il a été activé et, ce qui est plus grave, à qui il transmet les données espionnées.

Absolute a réagi aux affirmations de Kaspersky en disant que leur logiciel est sûr depuis qu'il a été amélioré en 2009. À cette date, Anibal Sacco et Alfredo Ortega, des experts en sécurité, avaient fait une présentation à ce sujet aux Black Hat Briefings, un symposium tenu à Las Vegas [3]. La réponse de Kaspersky à Absolute a été que les analyses ont été faites sur des ordinateurs neufs datant de 2012 et non des machines datant d'avant 2009 [4].

L'utilisation de Computrace soulève plusieurs problèmes fondamentaux : l'espionnage, la vie privée, la sécurité des données et le secret des affaires.

Le problème de l'espionnage

Pour ce qui est de l'espionnage, les révélations de William Binney, Thomas Drake, Edward Loomis, Kirk Wiebe et Edward Snowden ont montré la gravité de la situation. On sait que la NSA met en œuvre des moyens informatiques astronomiques pour espionner les communications du monde entier. On suppose que son budget annuel est de l'ordre de dix milliards de dollars et il semble qu'elle compte 30'000 employés au moins. La majorité travaillent à Ford Meade, dans la banlieue sud de Baltimore, mais il existe des bases dans le monde entier.

On sait que la NSA crée elle-même des logiciels espions qui sont implantés en *firmware* et utilisent le mode SMM. Elle l'a fait pour infecter des serveurs Hewlett-Packard, des routeurs et des pare-feu Juniper, des routeurs Cisco [5], etc. L'omniprésence de la NSA dans les satellites, la téléphonie, la messagerie électronique et le web a été montrée par Glenn Greenwald, un juriste spécialisé dans les

---

[2] http://www.absolute.com/en/resources/datasheets/absolute-computrace, accès le 30 mai 2014.

[3] Anibal Sacco, Alfredo Ortega, « Deactivate the Rootkit », Black Hat Briefings 2009 USA, Las Vegas, 30 juillet 2009, http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=publication&name=Deactivate_the_Rootkit.

[4] John Leyden, « Devs angrily dismiss Absolute Computrace rootkit accusation », *The Register*, 17 février 2014, http://www.theregister.co.uk/2014/02/17/kaspersky_computrace.

[5] Peter Gutman, « Crypto Won't Save You Either », Université d'Auckland, accès le 31 mai 2014, http://regmedia.co.uk/2014/05/16/0955_peter_gutmann.pdf ; « Cisco calls for curb on NSA surveillance efforts », *BBC News*, 19 mai 2014, http://www.bbc.com/news/technology-274- 68794 ; Leo Kelion, « Q&A: NSA's Prism internet surveillance scheme », *BBC News*, 1er juillet 2013, http://www.bbc.com/news/technology-23051248.

droits civils, dans un ouvrage intitulé *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* [6].

L'activisme de la NSA fait penser qu'elle est susceptible d'avoir conclu un accord avec Absolute, mais on ne peut être sûr de rien à cause de l'épais couvercle qui recouvre la sécurité nationale aux États-Unis. Si les dirigeants d'Absolute ont fourni une porte dérobée à la NSA, ils n'ont pas le droit de le dire et ils encourraient des peines d'emprisonnement s'ils l'admettaient publiquement.

La philosophie dont Absolute se réclame constitue un autre élément en faveur de l'existence d'un accord. La feuille de présentation de Computrace se termine pas la phrase : « L'équipe peut être fière d'avoir contribué à la récupération de plus de 30 000 appareils en collaborant étroitement avec les polices du monde entier » [7]. On ne voit pas pourquoi cette fierté ne s'étendrait pas à la collaboration avec la NSA.

Si l'accord entre Absolute et la NSA existe, les États et les entreprises du monde entier ont de quoi être inquiets. Même les ordinateurs dont les données sont chiffrées ne sont pas forcément sûrs. Certains algorithmes de chiffrement sont faibles, par exemple parce qu'il sont dotés d'une porte dérobée, mais, surtout, le fait que Computrace permette d'installer un keylogger a potentiellement pour effet de rendre inopérant tout système de chiffrement dont la clé a été tapée au clavier (et Absolute peut le désinstaller à tout moment, ce qui lui permet de couvrir ses traces).

La question de la vie privée

Un autre point délicat est celui de la vie privée. Le problème est que Computrace permet de suivre secrètement les trajets de l'ordinateur infecté, mais aussi d'inventorier son contenu et de surveiller tout ce qui se passe. On l'a vu, Absolute déclare explicitement dans sa documentation que Computrace permet de téléinstaller silencieusement un keylogger.

Le droit à la vie privée est un droit fondamental garanti par l'article 17 du Pacte international relatif aux droits civils et politiques, entré en vigueur en France en 1980, en Belgique en 1983 et en Suisse en 1992 :

> 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.
>
> 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Soit dit entre parenthèses, les États-Unis ont également ratifié ce traité en 1992, mais le problème est que, là-bas, le droit international ne prime pas sur le droit fédéral. Les deux sont de même niveau : « La présente Constitution, ainsi que les lois des États-Unis qui en découleront, et tous les traités déjà conclus, ou qui le seront, sous l'autorité des États-Unis, seront la loi suprême du pays » (Constitution, art. VI). Cela veut dire que les règles habituelles s'appliquent aux traités, à commencer par deux principes importants : la loi postérieure déroge à la loi antérieure (*lex*

---

[6] Glenn GREENWALD, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*, McClelland & Steward, Toronto, 2014.

[7] http://www.absolute.com/en/resources/datasheets/absolute-computrace, accès le 30 mai 2014.

posterior derogat priori) et ce qui est général ne déroge pas à ce qui est spécial (*generalia specialibus non derogant*). Or la législation dite « antiterroriste » est apparue après les attentats de 2001. Non seulement elle constitue la *lex specialis*, mais elle est postérieure au Pacte. Cela a pour conséquence que la protection des droits fondamentaux est très fragile aux États-Unis [8].

La Convention européenne des droits de l'homme protège également la vie privée (art. 8). Elle est entrée en vigueur en Belgique en 1955 et en France et en Suisse en 1974.

> 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

En France, le droit à la vie privée découle de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, qui a rang constitutionnel. Il est vu comme un élément de la liberté.

> **Art. 2.** Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression.

Il est aussi garanti par l'article 9 du Code civil : « Chacun a droit au respect de sa vie privée ».

En Belgique et en Suisse, il est protégé par la Constitution. En Belgique, c'est à l'article 22 : « Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi ». En Suisse, c'est à l'article 13 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications ».

Pour que la légalité de l'emploi de Computrace en entreprise ne pose pas de problèmes de respect de la vie privée, il me semble que les conditions suivantes devraient être remplies :

1° Le programme devrait pouvoir être supprimé. En Europe, la légalité d'un logiciel espion qu'il est matériellement impossible de désinstaller me paraît difficile à admettre.

2° L'employeur devrait avertir les collaborateurs concernés de l'existence de ce logiciel.

3° Les employés devraient être mis au courant des conséquences concrètes du fonctionnement de ce logiciel sur son ordinateur.

4° Les employés devraient avoir donné leur accord écrit.

Et il me semble qu'il plane un doute même si ces conditions sont respectées. Il est certain que l'employeur a le droit de prendre des mesures de sécurité, mais est-ce que le chiffrement du

---

[8] Par exemple, le Military Commissions Act protège les militaires et les agents américains qui seraient coupables d'avoir violé les Conventions de Genève contre toutes poursuites engagées par des combattants ennemis dits « non privilégiés » (H.R. 2647, p. 387, section 948b (e) ; http://www.mc.mil/Portals/0/MCA20Pub20Law200920.pdf). Cette disposition est en violation flagrante avec l'article 3 commun des quatre Conventions de Genève, qui s'applique aux civils comme aux combattants et aux guerres civiles comme aux conflits internationaux (les États-Unis ont ratifié ces textes en 1955).

disque des ordinateurs ne constituerait pas une protection contre le vol plus appropriée que l'emploi d'un logiciel espion ? Contrairement à un logiciel espion, le chiffrement n'ébrèche en rien la sphère privée de l'employé et, s'il est sûr, il offre une très bonne protection contre les accès non autorisés. Quant aux alertes qui se déclenchent si l'utilisateur fait une modification non autorisée [9], on peut les remplacer par un paramétrage restrictif du système.

À mon avis, on peut donc défendre l'idée que l'emploi de Computrace n'est ni proportionné ni nécessaire. Le chiffrement et le paramétrage permettent de protéger les intérêts de l'employeur sans porter atteinte à la sphère privée de l'employé.

La question de la sécurité des données

Une autre difficulté est que la législation sur la sécurité des données fait obligation aux entreprises qui gèrent des données personnelles de protéger ces données contre les accès non autorisés.

En France, c'est l'objet de l'article 34 de la Loi 78-17 relative à l'informatique, aux fichiers et aux libertés :

> Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.
> Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

En Belgique, cette règle est définie à l'article 16 de la Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel :

> § 4. Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

En Suisse, c'est l'article 7 de la Loi sur la protection des données :

> [1] Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

Si, par exemple, l'ordinateur d'un agent d'assurance contient des informations sur la santé de ses clients, il s'agit de données personnelles sensibles qu'il ne peut pas communiquer à un tiers. Cette

[9] http://www.absolute.com/en/resources/datasheets/absolute-computrace, accès le 30 mai 2014.

interdiction est-elle compatible avec la présence de Computrace sur son ordinateur ? Cela me paraît douteux.

Il y a aussi des conséquences qui ne sautent pas forcément aux yeux mais qui ne sont pas moins sources d'ennuis potentiels. Par exemple, un employeur a peut-être intérêt à ne pas céder un vieux notebook à un employé pour son usage privé parce que cela pourrait constituer une infraction à la législation sur la sécurité des données.

Il y a longtemps que l'Europe se déclare préoccupée par les actions d'espionnage électronique commises par le gouvernement des États-Unis. C'est ainsi qu'en 2001 le rapporteur Gerhard Schmid a fourni au Parlement européen une analyse de 200 pages intitulée « Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon) » [10]. Plus récemment, il y a eu notamment un rapport de la Commission au Parlement : « Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique » [11]. Les directives 95/46/CE, 2002/58/CE et 2009/136/CE portent aussi sur la question [12].

Le secret d'affaires

Le problème de la confidentialité ne concerne pas seulement les accès par des malfaiteurs, il touche aussi les secrets d'État et le droit des affaires : beaucoup de contrats contiennent une clause de confidentialité.

La question qui se pose est simple : une garantie de confidentialité est-elle compatible avec la présence de Computrace sur l'ordinateur qui contient les informations à protéger ? À moins d'utiliser des moyens de chiffrement impossibles à casser, je ne vois pas comment on pourrait certifier qu'un secret d'affaires ne tombera pas sous les yeux d'un tiers si l'ordinateur qu'on utilise abrite un logiciel espion dont la fonction est justement de donner libre accès à un tiers.

Cette question se poserait même si les dirigeants d'Absolute pouvaient fournir la preuve que leur porte dérobée ne peut pas être détournée et qu'ils sont seuls à accéder aux données des ordinateurs dotés de Computrace. Tout accès par un tiers non autorisé est interdit. Or aucune entreprise n'a jamais signé une clause de confidentialité qui exigerait le secret « sauf en ce qui concerne Absolute ».

Pierre Jaquet, 1er juin 2014 http://jaquet.org/pdfs/computrace.pdf

---

[10] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=FR.

[11] http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52013DC0846&rid=9.

[12] Directive 95/46/CE : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML ; Directive 2002/58/CE : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002L0058. Directive 2009/136/CE : http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8258260282A05125AD7EFFA685360F09.tpdjo01v_1?cidTexte=JORFTEXT000021492156&dateTexte=. Portail d'accès à la législation européenne : http://eur-lex.europa.eu/homepage.html.