Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IT Security Bulletin
Bulletin de sécurité TI

March 2008 | ITSB-49 | Mars 2008

Security Bulletin – Keyloggers and Spyware

Purpose

The purpose of this Bulletin is to advise Government of Canada (GC) departments and agencies of the security threat posed by modern "keylogger" software with enhanced data capture capabilities which utilize "stealth" techniques to hide from anti-virus and anti-spyware scanners.

Background

A 'keystroke logger' or 'keylogger' is a type of software that is commonly associated with spyware, which is any unauthorized or malicious software installed to secretly monitor user activity and/or to gather data which is stored on a compromised computer.

In reality, like many malicious hacker tools, keyloggers originated as an administrative and diagnostic tool; however, even helpful tools may be subverted and used for illegal or questionable activities. Such is the case with keylogging software.

Bulletin de sécurité – Enregistreurs de frappe et logiciels espions

Objet

Le présent bulletin a pour but d'informer les ministères et organismes du gouvernement du Canada (GC) de la menace à la sécurité que représentent les enregistreurs modernes de frappe munis de capacités améliorées de capture de données et faisant appel à des techniques furtives pour se cacher des scanneurs de virus et de logiciels espions.

Contexte

Un enregistreur de frappe, ou espion de clavier, est un type de logiciel communément associé aux logiciels espions. Les logiciels espions, également appelés espiogiciels, sont des logiciels non autorisés ou malveillants installés sur un ordinateur pour surveiller en cachette l'activité de l'utilisateur ou pour recueillir des données qui seront stockées dans l'ordinateur compromis.

En fait, comme bon nombre d'outils utilisés par les pirates informatiques, les enregistreurs de frappe sont à l'origine des outils administratifs et de diagnostique. Cependant, même des logiciels utiles peuvent être dénaturés et servir à des activités illégales ou suspectes. Tel est le cas pour les

A traditional keylogger program has the ability to record every keystroke typed at the keyboard at any time. Keyloggers have been used to capture user names, passwords, account numbers or other sensitive information typed at the keyboard. These keystrokes are saved to a log file that can be transmitted to an unknown third party – e.g., in February 2006, it was publicly reported in the EU that foreign criminal organizations utilized keylogger software to capture users' bank account numbers and passwords, and stole over 1 million Euros.

In this attack, a keylogger program was invisibly installed on users' machines through e-mail attachments or "drive-by" downloads (web content which exploits known system security problems in operating systems, web browser and messaging software to automatically download and install arbitrary code) when users visited certain Web sites.

Recently, a new type of keylogger software containing greatly enhanced features has appeared. This new generation of keylogger software not only captures keystrokes, but is also able to:

- Record mouse activity, identifying buttons and icons selected during computer use
- Monitor Internet activity, websites and web pages visited
- Record application activity, showing which programs were launched
- Capture all e-mails sent or received on the compromised PC, no matter if an e-mail client program or a web-interface is used

enregistreurs de frappe.

Un programme d'enregistrement de frappe traditionnel peut enregistrer chaque touche enfoncée au clavier à un moment donné. Des enregistreurs de frappe ont été utilisés pour capturer les ID utilisateur, les mots de passe, les numéros de compte et d'autres renseignements sensibles tapés au clavier. Ces frappes sont enregistrées dans un fichier journal qui peut être transmis à un tiers inconnu. À titre d'exemple, en février 2006, on a rapporté publiquement dans l'Union européenne que des organisations criminelles étrangères avaient utilisé un enregistreur de frappe pour capturer les numéros de compte de banque d'utilisateurs et les mots de passe connexes pour voler plus d'un million d'euros.

Dans cette attaque, un programme d'enregistrement de frappe s'était installé sur l'ordinateur des victimes, à leur insu, par l'intermédiaire d'un fichier joint à un courriel ou d'un téléchargement « à la volée » (contenu Web qui exploite les problèmes de sécurité connus dans les systèmes d'exploitation, les navigateurs Web et les logiciels de messagerie pour télécharger et installer automatiquement un code arbitraire) lorsqu'elles ont visité certains sites Web.

Un nouveau type d'enregistreur de frappe doté de fonctions grandement améliorées est apparu récemment. Cette nouvelle génération d'enregistreur non seulement capture les frappes, mais peut également :

- enregistrer l'activité de la souris et identifier les boutons et les icônes sélectionnés durant l'utilisation de l'ordinateur;
- surveiller l'activité Internet, les sites et les pages Web visités,
- enregistrer l'activité des applications en précisant quels programmes ont été lancés;
- capturer tous les courriels envoyés et reçus

- Record desktop activity by making snapshots of the computer screen at regular defined intervals
- Surreptitiously send all logged data to any specified recipient via e-mail
- Use “stealth” techniques to hide from all major anti-virus and anti-spyware scanners; some variants are even capable of hiding their program folder on the hard drive (in 2007, one such program listed over 60 current anti-virus/anti-spyware scanners that it defeats, including industry leaders such as Norton and McAfee)

The advanced capability of these new keyloggers now make available to an attacker a more complete picture of the activities performed on a computer with minimal danger of discovery, and dramatically increases the risk of compromise of sensitive data.

Many of these keyloggers are now packaged as commercial software and available for anyone to download and install, increasing the threat due to insider activity.

Technical

Several common methods of “hiding” a process from the operating system or scanning software exist:

- Unlinking process entry from OS Process Table: process continues to run, but is rendered invisible to utilities used to enumerate system processes such as “Task Manager”.
- Interception of Windows API calls:

sur le PC compromis, peu importe si un programme de courriel client ou une interface Web a été utilisé;

- enregistrer l’activité du bureau en prenant des clichés de l’écran de l’ordinateur à intervalles réguliers;
- envoyer furtivement toutes les données recueillies à un destinataire précis par courriel;
- utiliser des techniques furtives pour se dérober à l’analyse des principaux scanneurs de virus et de logiciels espions; certaines variantes peuvent même cacher le répertoire de leur programme sur le disque dur (en 2007, un tel programme a listé plus de 60 scanneurs de virus et de logiciels espions qu’il a mis en échec, y compris les chefs de file de l’industrie tels qu Norton et McAfee.)

La capacité évoluée de ces nouveaux enregistreurs de frappe met désormais à la disposition de l’attaquant une image plus complète des activités exécutées sur un ordinateur avec peu de risque d’être découvert et accroît considérablement les risques de compromission des données sensibles.

Bon nombre d’enregistreurs de frappe se présentent maintenant comme des logiciels commerciaux et sont disponibles à quiconque veut les télécharger et les installer, ce qui contribue à augmenter la menace d’une attaque interne.

Renseignements techniques

Il existe plusieurs façons de cacher un processus d’un système d’exploitation ou d’un logiciel d’analyse :

- désallocation du processus de la table des processus du système d’exploitation : le processus continue de s’exécuter mais est rendu invisible aux utilitaires servant à énumérer les processus système, tel le gestionnaire des tâches (*Task Manager*)

process inserts additional code to modify the behaviour of operating system functions; there are many possible variations, but typically two common methods are used, often in conjunction with each other:

Method 1: System calls to enumerate disk directories are altered to prevent listing of files used by the keylogger. Files then become invisible to File Manager and "dir" command, so anti-virus and spyware scanners cannot see or scan the files.

Method 2: System calls to open and read files are altered so that when compromised operating system files are scanned, an unaltered version of the file is presented and passes the scan.

Such techniques are often used to make keyloggers and other spyware virtually invisible to the current generation of virus and spyware scanners, and also complicate the removal of such unwanted software because the host operating system is also compromised.

Typically, off-line "forensic"-style scanner tools are used to detect/defeat these "stealth" techniques; the disadvantages of these types of tools include the fact that system must be rebooted with the tool CD. Unlike current virus scanners which run in conjunction with user process and allow the user to continue to work, off-line tools need to boot into a protected environment to remove the influence of a compromised host operating system. As well, most tools of this nature are either proprietary or, in the case of freely

- interception des appels API de Windows : le processus insère un code additionnel pour modifier le comportement des fonctions du système d'exploitation. Il existe de nombreuses variations possibles mais deux méthodes sont généralement utilisées, souvent en conjonction l'une de l'autre :

  Méthode 1 : Les appels système servant à énumérer les répertoires du disque sont modifiés pour empêcher le listage des fichiers utilisés par l'enregistreur de frappe. Les fichiers deviennent donc invisibles au gestionnaire de fichiers et à la commande « dir », de sorte qu'il est impossible pour les scanneurs de virus et de logiciels espions de voir ou d'analyser les fichiers.

  Méthode 2 : Les appels système servant à ouvrir et à lire les fichiers sont modifiés de telle façon que, lorsque des fichiers compromis du système d'exploitation sont analysés, une version non altérée du fichier est présentée au scanneur qui ne détectera rien.

De telles techniques sont souvent utilisées pour rendre les enregistreurs de frappe et autres espiogiciels virtuellement invisibles à la génération actuelle de scanneurs de virus et de logiciels espions. Elles compliquent également la suppression de ces programmes indésirables parce que le système d'exploitation hôte est également compromis.

Règle générale, on utilise des outils d'analyse autonomes de style « judiciaire » pour détecter et mettre en échec ces techniques furtives; ces outils comportent toutefois l'inconvénient de nécessiter le redémarrage du système à l'aide du CD de l'outil. Contrairement aux scanneurs de virus actuels qui s'exécutent en conjonction avec les processus de l'utilisateur, permettant ainsi à ce dernier de continuer son travail, les outils autonomes ont besoin de démarrer dans un environnement protégé pour se soustraire à l'influence d'un système

available toolsets, still experimental or undergoing active development.

All operating systems (Windows, Unix/Linux/MacOS) are vulnerable to similar techniques, although Windows tends to be the primary target due to the large number of installations.

The new Microsoft Windows Vista operating system contains features (e.g., the Hypervisor) that makes it more resistant, but not immune, to such “stealth” techniques. A number of commercial keylogger packages already advertise full Windows Vista compatibility.

Impact on Government of Canada Departments

Traditionally, the risk arising from traditional keyloggers is high but considered as having only minimal impact because the amount of data that can be typed at a keyboard is comparatively low and without context (i.e., the application or system a password is for may not be evident in a keystroke log).

However, beyond the threat resulting from compromise of user names, passwords and other data typed in from a keyboard that traditional keyloggers pose, the new generation of enhanced key and data loggers introduce several serious security threats to GC departments and agencies:

- Increased contextual content (e.g., states which application is launched) increases the likelihood of successful attacks using the captured keystrokes
- Ability to capture screen images can result in a disclosure of sensitive GC communications and documents

d’exploitation hôte compromis. Par ailleurs, la plupart des outils de cette nature sont exclusifs ou, dans le cas de boîtes à outils disponibles gratuitement, sont encore au stade expérimental ou en cours de développement.

Tous les systèmes d’exploitation (Windows, Unix/Linux/MacOS) sont vulnérables à des techniques similaires, quoique Windows soit une cible privilégiée en raison du grand nombre d’installations.

Le nouveau système d’exploitation Windows Vista de Microsoft renferme des fonctions (p. ex. Hypervisor) qui le rendent plus résistant, sans toutefois l’immuniser, aux techniques furtives. Un certain nombre d’enregistreurs de frappe annoncent déjà une compatibilité complète avec Windows Vista.

Incidence sur les ministères du gouvernement du Canada

Traditionnellement, le risque que posent les enregistreurs de frappe traditionnels est élevé mais est considéré comme ayant une incidence minime parce que la quantité de données qui peuvent être tapées à un clavier est relativement faible et sans contexte (c.-à-d. l’application ou le système pour lequel on tape un mot de passe peut ne pas être évident dans le journal de frappe).

Or, au-delà de la menace de compromission des noms d’utilisateur, des mots de passe et d’autres données tapées au clavier que font peser les enregistreurs de frappe traditionnels, la nouvelle génération d’enregistreurs de frappe et de données introduit plusieurs menaces sérieuses à la sécurité des ministères et organismes du GC :

- le contenu contextuel accru (p. ex. indiquant l’application lancée) augmente la probabilité d’attaques réussies par suite de la capture des frappes ;
- la capacité de capturer les images écran peut donner lieu à la divulgation de communications

- Ability to capture events and activities performed on a computer, even if no sensitive information is disclosed, may give an attacker information on work methods and procedures that might facilitate other forms of attack (e.g. social engineering)
- Ability to automatically e-mail captured data increases the scale of the compromise, and may seriously impair damage containment efforts
- "Stealth" capabilities make new keyloggers undetectable by many common virus and spyware checkers, and increase the probability that compromised systems may potentially exfiltrate sensitive data indefinitely, thereby further increasing the scale of the compromise.

Recommendation

Because new generation keyloggers may not be detectable by common virus and spyware scanners, GC departments and agencies can minimize the risks from keyloggers by:

- Ensuring users have an awareness of safe Internet usage practices to avoid viruses and spyware - "watch where you surf", and do not open unknown files or e-mail attachments. Because most instances of computer compromise arise from web, e-mail and, "instant messaging", the first line of defence lies with the user.
- Improving separation of sensitive and unclassified data by encouraging users to refrain from personal Internet activities, or at least to limit such activities to known legitimate addresses, when such activities are conducted on departmental networks containing sensitive data. In cases where

et de documents sensibles du GC;

- la capacité de capturer des événements et des activités exécutées sur un ordinateur, même si aucun renseignement sensible n'est divulgué, peut donner à l'attaquant de l'information sur les méthodes et procédures de travail qui pourraient faciliter d'autres formes d'attaques (p. ex. ingénierie sociale);
- la capacité d'envoyer automatiquement par courriel les données capturées augmente l'ampleur de la compromission et peut sérieusement nuire aux efforts de limitation des dégâts;
- les capacités furtives rendent les nouveaux enregistreur indétectables par de nombreux vérificateurs de virus et de logiciels espions et augmentent la probabilité que des systèmes compromis peuvent « exfiltrer » des données sensibles indéfiniment, augmentant par le fait même l'ampleur de la compromission.

Recommandation

Étant donné qu'il est possible que les enregistreurs de frappe de nouvelle génération ne puissent pas être détectés par les scanneurs communs de virus et de logiciels espions, les ministères et organismes du GC peuvent réduire au minimum les risques posés par ces enregistreurs en :

- s'assurant que les utilisateurs sont au courant des pratiques sécuritaires d'utilisation d'Internet afin d'éviter les virus et les logiciels espions. Les utilisateurs doivent faire attention aux sites qu'ils visitent et ne pas ouvrir les fichiers inconnus ou les pièces jointes de courriels inconnus. Étant donné que la plupart des compromissions d'ordinateurs tirent leur source du Web, du courriel et de la messagerie instantanée, l'utilisateur constitue la première ligne de défense;
- en améliorant la séparation entre les données sensibles et les données non classifiées en

access to Internet sites of unknown content is required, a standalone or personal machine for such purposes should be used. Refrain from using public Internet terminals or untrusted computers for processing sensitive data.

- Ensuring departmental computers are updated with the latest operating system security patches and anti-virus/anti-spyware definitions, and that scans are run on a regular basis. Even if not all keylogger software is detectable by virus and spyware scanners, such tools remain an important part of overall system security.
- Ensuring that user accounts have the minimum of privileges required to perform day-to-day activities, as spyware usually relies on a user operating with Administrative privileges. Users that require elevated privileges (e.g., system administrators) should only enable such privileges when absolutely required and use regular unprivileged accounts for normal operations.
- Upgrading to Windows Vista or using an alternate operating system, where the IT department has approved such installations, can help reduce the risk from keylogger attacks.
- Establishing a program of regular off-line system scanning to ensure that computer systems have not been compromised with unauthorized software, particularly if sensitive data protection requirements are warranted.

encourageant les utilisateurs à s'abstenir d'effectuer des activités Internet personnelles ou du moins à limiter de telles activités à des adresses légitimes connues, lorsque de telles activités sont exercées sur des réseaux ministériels renfermant des données sensibles. Dans les cas où on doit accéder à des sites Internet dont on ne connaît pas le contenu, un ordinateur autonome ou un ordinateur personnel devrait être utilisé à cette fin. Il faut s'abstenir d'utiliser des terminaux Internet publics ou des ordinateurs non fiables pour le traitement de données sensibles;

- faisant en sorte que les plus récents correctifs de sécurité des systèmes d'exploitation, de même que les plus récentes définitions de virus et de logiciels espions, soient installés sur les ordinateurs du ministère, et qu'on exécute des analyses sur une base régulière. Même si les enregistreurs de frappe ne peuvent pas tous être détectés par les scanneurs de virus et de logiciels espions, ceux-ci n'en demeurent pas moins une part importante de la sécurité générale des systèmes;
- en s'assurant que les comptes utilisateurs ont le minimum de privilèges nécessaires pour exécuter les tâches quotidiennes étant donné que les logiciels espions comptent sur les utilisateurs possédant des privilèges administrateur. Les utilisateurs qui nécessitent des privilèges plus élevés (p. ex. les administrateurs système) ne devraient activer ces privilèges qu'en cas de nécessité absolue et devraient utiliser des comptes non privilégiés pour leurs opérations régulières;
- en mettant à niveau les ordinateurs à Windows Vista ou en utilisant un autre système d'exploitation là où le service des TI a approuvé de telles installations, afin d'aider à réduire le risque d'attaques par enregistreurs de frappe;

- en établissant un programme d'analyse système hors ligne sur une base régulière afin d'assurer que les ordinateurs n'ont pas été compromis au moyen de logiciels non autorisés, plus particulièrement si les exigences en matière de protection des données sensibles le justifient.

Contacts and Assistance

Head, IT Security Client Services
Communications Security Establishment Canada
PO Box 9703, Terminal
Ottawa, Ont K1G 3Z4

Telephone: (613) 991-8495
e-mail : itsclientservices@cse-cst.gc.ca

Aide et renseignements

Chef, Services à la clientèle, Sécurité des TI
Centre de la sécurité des télécommunications Canada
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4

Téléphone : (613) 991-8495
Courriel : itsclientservices@cse-cst.gc.ca

La directrice de la Gestion de la mission de la Sécurité des TI,

Originally signed by /
Signé initialement par

Gwen Beauchemin
Director, IT Security Mission Management