DARKHOTEL, LA MENACE PERSISTANTE AVANCÉE

UN HÔTE INHABITUEL DANS LES HÔTELS

Version 1.1
Novembre 2014

Global Research and Analysis Team

KASPERSKY lab

Table des matières

Résumé analytique

La menace persistante avancée Darkhotel est un acteur, dans le monde du cyber-espionnage, dotée de caractéristiques de toute évidence incohérentes et contradictoires. Certaines sont évoluées, d'autres assez rudimentaires. Opérant depuis près d'une décennie dans les hôtels, cette menace sévit actuellement. Les activités offensives perpétrées par ce programme peuvent être associées au wi-fi ainsi qu'aux connexions physiques des hôtels et des centres d'affaires, mais également aux réseaux p2p/de partage de fichiers. Il a également la réputation de mener des attaques par phishing ciblé. Les outils Darkhotel portent, entre autres, des noms du type « Tapaoux », « Pioneer », « Karba » et « Nemim ». La liste suivante répertorie les caractéristiques des pirates :

- Compétences opérationnelles visant à compromettre, utiliser de manière abusive et maintenir l'accès à l'échelle mondiale aux ressources de réseaux commerciaux dignes de confiance avec une précision stratégique et ce, depuis des années ;
- Compétences d'attaque mathématiques et cryptoanalytiques avancées et aucune crainte de compromettre la fiabilité des autorités de certification et de la PKI ;
- Infection des systèmes à l'aveugle avec une connaissance certaine des ressources fiables et non fiables permettant de développer et de mener des opérations d'ampleur de type botnet ;
- Enregistreurs de frappe de faible niveau mais bien développés, intégrés à des outils efficaces et cohérents ;
- Campagnes axées sur des catégories spécifiques de victimes les identifiant ;

- Infrastructure dynamique et largement déployée reposant sur des serveurs Web Apache, des enregistrements DNS dynamiques, des bibliothèques cryptographiques et des applications Web php ;
- Accès zero-day régulier. Déploiement récent d'une faille d'exploitation zero-day Adobe Flash intégrée et déploiement rare d'autres ressources zero-day pour soutenir des campagnes plus importantes sur plusieurs années.

Introduction

Lorsque des clients peu méfiants, notamment des cadres d'entreprise et des dirigeants du secteur de la haute technologie, voyagent dans divers hôtels et se connectent à Internet, ils sont infectés par un cheval de Troie, menace persistante avancée rare, se faisant passer pour une mise à jour importante d'un logiciel connu. Il peut s'agir de GoogleToolbar, d'Adobe Flash, de Windows Messenger, etc. La première étape du programme malveillant permet aux assaillants d'identifier les victimes les plus intéressantes, les conduisant au téléchargement sélectif d'outils de piratage plus perfectionnés.

Dans les hôtels, ces programmes sont distribués de manière sélective à des personnes ciblées. Le groupe de pirates semble connaître au préalable la date d'arrivée et de départ de ces clients à leur hôtel haut de gamme. Les assaillants sont donc dans l'attente jusqu'à ce que les voyageurs arrivent et se connectent à Internet.

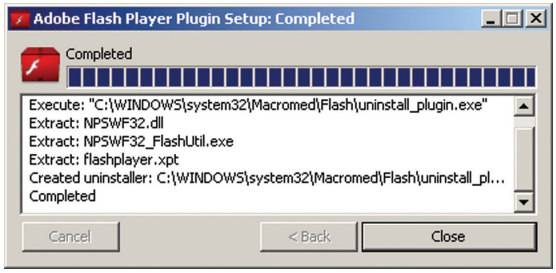
Le FBI a émis des avis relatant des incidents similaires à l'encontre d'hôtels ; les autorités du gouvernement australien ont également rapporté des cas identiques ciblant des clients médiatiques. Alors qu'une annonce du FBI relative à des piratages visant les clients d'hôtels à l'étranger a été publiée en mai 2012, des exemples de piratage Darkhotel similaires avaient déjà eu lieu en 2007. Et des journaux de données du serveur Darkhotel montrent l'existence de connexions depuis le 1er janvier 2009. En outre, l'implantation d'un programme malveillant largement diffusé au sein de réseaux p2p et des attaques de phishing ciblé zero-day montrent que la menace persistante avancée Darkhotel dispose d'un ensemble d'outils efficaces et une opération sur le long terme derrière l'hospitalité toute relative qu'il offre aux clients des hôtels visés.

Analyse

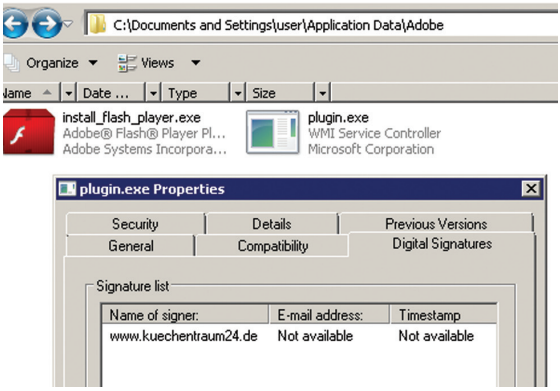
Cible - Hôtels/centres d'affaires et propagation aveugle

Propagation dans les hôtels et centres d'affaires

La propagation du malware précis de menace persistante avancée Darkhotel a été observée au sein de plusieurs réseaux d'hôtels, où les visiteurs se connectant au wifi sont incités à installer les mises à jour logicielles de logiciels courants.



Ces packages étaient en fait des programmes d'installation pour les backdoors de menace persistante avancée, ajoutés aux programmes d'installation légitimes d'Adobe et de Google. Les backdoors Darkhotel signées numériquement étaient installées avec les packages légitimes.



Le plus intéressant concernant cette méthode de diffusion est le fait que les hôtels demandent à leurs clients d'utiliser leur nom et leur numéro de chambre pour s'identifier. Cependant, seuls quelques clients ont reçu le package

Darkhotel. Lors de la visite des mêmes hôtels, nos systèmes de recherche « pots de miel » n'ont pas pu attirer de cyber-attaque Darkhotel. Ces données ne sont pas concluantes, mais elles mettent en évidence la possibilité d'un usage détourné des informations d'enregistrement.

Porter atteinte à l'infrastructure du réseau

La menace Darkhotel a maintenu une intrusion efficace à l'encontre des réseaux des hôtels, fournissant un accès important à des points d'attaques inattendus pendant plusieurs années. Ces points d'arrêt procurent également aux assaillants un accès aux informations d'arrivée et de départ ainsi que d'identité des visiteurs des hôtels haut de gamme et de luxe.

Notre recherche nous a menés, dans le cadre d'une enquête en cours, à des iframes intégrés au sein des réseaux d'hôtels qui redirigeaient les navigateurs Internet des victimes vers de faux programmes d'installation. Les assaillants ont été très prudents en plaçant ces iframes et ces éléments exécutables sur des ressources de confiance, les portails d'identification du réseau des hôtels eux-mêmes. Ils ont également été très prudents en effaçant toute trace de leurs outils immédiatement après avoir perpétré une attaque avec succès. Ces portails sont désormais vérifiés, nettoyés et soumis à une vérification supplémentaire ainsi qu'à un durcissement. Nous avons observé des traces de quelques-uns de ces incidents fin 2013 et début 2014 sur le réseau d'un hôtel victime. Les assaillants ont mis en place l'environnement et touché leurs cibles individuelles avec précision. Une fois le séjour de leur cible terminé et l'attaque menée à bien, les assaillants supprimaient leur positionnement iframe et leur programmes d'infiltration exécutables du réseau de l'hôtel. Les assaillants ont effacé avec succès les traces des travaux de leurs attaques précédentes dans un autre hôtel, mais leurs techniques d'attaque étaient les mêmes. Des rapports extérieurs relatifs au même type d'activité dans d'autres hôtels fournissent suffisamment de données visant à confirmer les mêmes opérations vigilantes dans ces lieux-là.

La technique d'attaque mêle quelques tactiques courantes de menace persistante avancée ; « attaques de point d'eau » ou « compromissions Internet stratégiques » plutôt imprécises et des techniques de phishing ciblé plus précises. Dans ce cas, les assaillants Darkhotel attendent que leur victime se connecte à Internet par le biais du wifi de l'hôtel ou du câble situé dans leur chambre. Il existe une forte probabilité que les cibles se connectent par le biais de ces ressources et que les assaillants se fient à cette probabilité, s'apparentant à une attaque de point d'eau. Mais les assaillants conservent également des informations de ciblage très précises relatives à la visite de la victime, de la même manière qu'ils auraient connaissance de son adresse e-mail

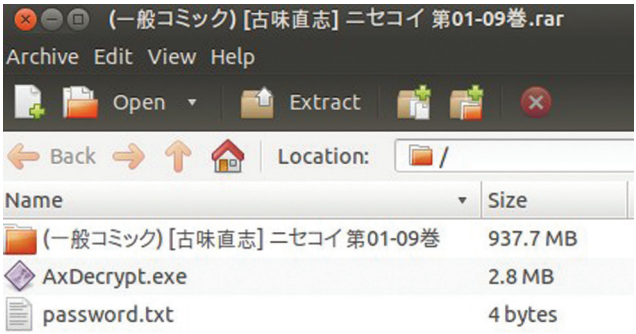
et des ses intérêts en matière de contenu lors d'une attaque de phishing ciblé. Lors de la préparation de l'attaque, les assaillants Darkhotel connaissaient la date d'arrivée et de départ de leur cible, son numéro de chambre et son nom complet, entres autres. Ces données leur permettent de présenter l'iframe malveillant à cette cible en particulier. Nous avons donc ici encore une autre caractéristique unique de ces assaillants : ils utilisent une approche offensive vaguement certaine mais très précise.

Propagation à grande échelle

Un exemple de la propagation aveugle du malware de menace persistante avancée Darkhotel est illustré par la manière dont il s'implante dans les sites japonais de partage p2p, où le programme malveillant est diffusé en tant qu'élément d'une archive rar de taille importante (environ 900 Mo). L'archive est également propagée par le biais de bittorrent, comme expliqué ci-dessous. Darkhotel utilise cette méthode afin de propager son cheval de Troie Karba. Ces archives japonaises, traduites pour les utilisateurs de langue chinoise, sont à caractère sexuel, une scène partielle de dessin animé à caractère sexuel/militaire, exposant les intérêts probablement en jeu des cibles potentielles.

Ce package Darkhotel a été téléchargé plus de 30 000 fois en moins de six mois. L'offre Darkhotel bittorrent p2p est listée ici, publiée le 22/11/2013. Elle a été propagée tout au long de 2014.

（一般コミック）［古味直志］ニセコイ 第01–09巻.rar



Ce torrent produit un fichier de presque 900 Mo. L'archive rar est décompressée en un répertoire comprenant quantité de fichiers zip chiffrés, le déchiffreur associé et un fichier de mots de passe pour le déchiffrement des zip. Mais ce qui ressemble au déchiffreur AxDecrypt.exe est lié à la fois au vrai déchiffreur et

à l'injecteur du cheval de Troie Karba Darkhotel Catch.exe. Lorsqu'un utilisateur télécharge le torrent et déchiffre les fichiers zip, le cheval de Troie est installé de manière clandestine et exécuté sur le système de la victime.

Catch.exe, détecté comme Backdoor.Win32.Agent.dgrn, communique avec la commande Darkhotel suivante et contrôle les serveurs :

```
microdelta.crabdance.com
microyours.ignorelist.com
micronames.jumpingcrab.com
microchisk.mooo.com
microalba.serveftp.com
```

D'autres exemples de cette backdoor Darkhotel liés au sein d'un torrent partagé comprennent des dessins animés japonais avec un contenu pour adultes, entre autres. Ces torrents individuels sont téléchargés des dizaines de milliers de fois.

“torrent\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化\(comic1☆7）[莉零（小鹿りな，古代兵器)] 凌 -shinogi-（闪乱カグラ）[中文] “

et

“動漫\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化”）

La backdoor Darkhotel associée était hébergée sur bittorrent, emule, etc... sous une variété de noms de bandes dessinées. Les exemples comprennent des offres de bandes dessinées et des dessins animés. Les domaines de serveurs de commande et de contrôle Darkhotel liés comprennent :

```
microblo5.mooo.com
microyours.ignorelist.com
micronames.jumpingcrab.com
microchisk.mooo.com
microalba.serveftp.com
```

Campagnes de phishing ciblé Darkhotel

Des campagnes Darkhotel impliquant des implantations de phishing ciblé Tapaoux typiques sont apparues publiquement en plusieurs parties, plusieurs fois ces cinq dernières années. Ces démarches de sous-projet visaient la base industrielle de défense (BID), le gouvernement et les organisations non gouvernementales. Un e-mail sur les thèmes de l'énergie nucléaire et les capacités en matière d'armes était utilisé comme leurre. Les premiers rapports ont été publiés sur contagio, décrivant

les attaques perpétrées sur les organisations non gouvernementales et les décideurs gouvernementaux. Cette activité de phishing ciblé se poursuit en 2014. Les attaques suivent la procédure de phishing ciblé classique et au cours des derniers mois, ont exploité des exécutables de téléchargement récupérés sur les systèmes des serveurs Internet tels que hxxp://office-revision.com/update/files22/update.exe ou hxxp://trade-inf.com/mt/ duspr.exe

Ces dernières années, le groupe a envoyé des liens par e-mail qui redirigent les navigateurs des cibles vers des failles d'exploitation zero-day d'Internet Explorer. Parfois, la pièce jointe elle-même contient une faille d'exploitation Adobe zero-day.

Déploiement zero-day récent

Ces pirates déploient parfois des failles d'exploitation zero-day mais les gravent lorsque cela est nécessaire. Ces dernières années, ils ont déployé des attaques de phishing ciblé zero-day visant les produits Adobe et Microsoft Internet Explorer, notamment cve-2010-0188. Début 2014, nos chercheurs ont mis au jour leur utilisation de cve-2014-0497, une attaque Flash zero-day décrite sur Securelist début février.

Les assaillants ont piraté avec une attaque de phishing ciblé un ensemble de systèmes cibles connectés à Internet par le biais d'un FAI chinois et ont développé des compétences au sein des failles d'exploitation zero-day pour pouvoir manœuvrer les systèmes matériels Windows 8.1. Il est intéressant de constater que les objets Flash étaient intégrés à des documents coréens intitulés « Liste des derniers AV wind japonais et comment utiliser les torrents. docx » (traduction française à partir d'une traduction anglaise approximative). Le téléchargeur (d8137ded710d83e2339a97ee78494c34) avait diffusé un logiciel malveillant similaire à la fonctionnalité du composant de « vol d'information » résumée ci-après et détaillée dans l'annexe D.

Certificats numériques et délégitimation de la fiabilité de l'autorité de certification

Les menaces Darkhotel signent généralement leurs backdoors avec des certificats numériques d'un genre ou d'un autre. Cependant, les certificats initialement choisis par ces pirates sont très intéressants en raison de faibles clés de chiffrement et de leur détournement probable par des assaillants. Voici une liste des certificats couramment utilisés pour signer le malware Darkhotel et qui demandent des compétences mathématiques avancées afin de factoriser les clés de chiffrement à ce moment-là. Il ne s'agit pas des seuls certificats utilisés par le groupe. Une activité plus récente évoque la possibilité que le groupe ait volé les certificats pour signer le code.

Certificat racine	CA/Émetteur subordonné(e)	Propriétaire	Statut	Valide du	Valide jusqu'au
GTE CyberTrust	Identifiant de serveur Digisign (enrichi)	flexicorp.jaring.my sha1/ RSA (512 bits)	Expiré	17/12/2008	17/12/2010
GTE CyberTrust	Certificat SureServer Cybertrust	inpack.syniverse.my sha1/RSA (512 bits)	Révoqué	13/02/2009	13/02/2011
GTE CyberTrust	Certificat SureServer Cybertrust	inpack.syniverse.com sha1/RSA (512 bits)	Révoqué	13/02/2009	13/02/2011
GTE CyberTrust	Autorité de certification Anthem Inc	ahi.anthem.com sha1/ RSA (512 bits)	Signature non valide	13/01/2010	13/01/2011
GlobalSign	Deutsche Telekom CA 5	www.kuechentraum2 4.de sha1/RSA (512 bits)	Révoqué	20/10/2008	25/10/2009
GTE CyberTrust	Identifiant de serveur Digisign (enrichi)	payments.bnm.gov.m y sha1/RSA (512 bits)	Signature non valide	07/12/2009	07/12/2010
GTE CyberTrust	TaiCA Secure CA	esupplychain.com.tw sha1/RSA (512 bits)	Expiré	02/07/2010	17/07/2011
GTE CyberTrust	Identifiant de serveur Digisign (enrichi)	mcrs2.digicert.com. my sha1/RSA (512 bits)	Signature non valide	28/03/2010	28/03/2012
GTE CyberTrust	Certificat SureServer Cybertrust	agreement.syniverse. com sha1/RSA (512 bits)	Signature non valide	13/02/2009	13/02/2011
GTE CyberTrust	Certificat SureServer Cybertrust	ambermms.syniverse. com sha1/RSA (512 bits)	Signature non valide	16/02/2009	16/02/2011
Equifax Secure eBusiness CA-1	Equifax Secure eBusiness CA-1	secure.hotelreykjavik.i s md5/RSA (512 bits)	Signature non valide	27/02/2005	30/03/2007
GTE CyberTrust	Cybertrust Educational CA	stfmail.ccn.ac.uk sha1/ RSA (512 bits)	Signature non valide	12/11/2008	12/11/2011
GTE CyberTrust	Identifiant de serveur Digisign (enrichi)	webmail.jaring.my sha1/ RSA (512 bits)	Signature non valide	01/06/2009	01/06/2011
GTE CyberTrust	Cybertrust Educational CA	skillsforge.londonmet. ac.uk sha1/RSA (512 bits)	Signature non valide	16/01/2009	16/01/2012
GTE CyberTrust	Identifiant de serveur Digisign (enrichi)	anjungnet.mardi.gov. my sha1/RSA (512 bits)	Signature non valide	29/09/2009	29/09/2011

Certificat racine	CA/Émetteur subordonné(e)	Propriétaire	Statut	Valide du	Valide jusqu'au
GTE CyberTrust	Autorité de certification Anthem Inc	dl-ait-middleware@anthem.com sha1/RSA (512 bits)	Signature non valide	22/04/2009	22/04/2010
GTE CyberTrust	Cybertrust Educational CA	ad-idmapp.cityofbristol.ac.uk sha1/RSA (512 bits)	Signature non valide	11/09/2008	11/09/2011
Verisign	Verisign Class 3 Secure OFX CA G3	secure2.eecu.com sha1/RSA (512 bits)	Signature non valide	25/10/2009	26/10/2010
Agence racine	Agence racine	Microsoft md5/RSA (1 024 bits)	Signature non valide	09/06/2009	31/12/2039
GTE CyberTrust	CyberTrust SureServer CA	trainingforms.syniverse.com sha1/RSA (512 bits)	Signature non valide	17/02/2009	17/02/2011

Tous les cas associés au programme malveillant Darkhotel partagent la même autorité de certification racine et la même autorité de certification intermédiaire ayant émis des certificats disposant de clés md5 faibles (RSA 512 bits). Nous sommes convaincus que la cyber-menace Darkhotel a dupliqué de manière frauduleuse ces certificats pour signer son malware. Ces clés n'ont pas été volées. Nombre de ces certificats ont été signalés dans une publication de 2011 de Fox-IT « RSA-512 Certificates Abused in the Wild ».

Pour étayer ces spéculations, nous attirons votre attention sur l'avis de sécurité Microsoft non spécifique ci-dessous, l'avis Mozilla faisant alors état du problème, et les réponses d'Entrust.

Avis de sécurité du jeudi 10 novembre 2011 :

« **Microsoft sait que DigiCert Sdn. Bhd, une autorité de certification subordonnée malaisienne (CA) de Entrust et GTE CyberTrust, a émis 22 certificats avec de faibles clés de chiffrement 512 bits.** Ces faibles clés de chiffrement, lorsqu'elles sont cassées, peuvent permettre à un assaillant d'utiliser les certificats de manière frauduleuse pour imiter le contenu, lancer des attaques de phishing, ou des attaques dites de l'homme du milieu contre tous les utilisateurs de navigateurs Internet, notamment les utilisateurs d'Internet Explorer. Bien qu'il ne s'agisse pas d'une vulnérabilité d'un produit Microsoft, ce problème touche toutes les versions prises en charge de Microsoft Windows.

Aucune indication ne permet de déterminer que ces certificats ont été émis de manière frauduleuse. En revanche, les clés faibles en matière de chiffrement ont permis à certains des certificats de se dupliquer et d'être utilisés de manière frauduleuse.

Microsoft fournit une mise à jour pour toutes les versions de Microsoft Windows prises en charge, révoquant sa confiance en DigiCert Sdn. Bhd. La mise à jour révoque la confiance placée dans les deux certificats CA intermédiaires suivants : Identifiant de serveur Digisign – (Enrichi), émis par Entrust.net Certification Authority (2048) **Identifiant de serveur Digisign (Enrichi)**, émis par **GTE CyberTrust Global Root** »

La réponse de Mozilla en 2011 :

« Bien qu'aucune indication **ne permette de dire qu'ils ont été émis de manière frauduleuse, les faibles clés ont favorisé la compromission des certificats**. En outre, les certificats de cette CA contiennent plusieurs problèmes techniques. Il leur manque une extension EKU spécifiant l'usage prévu et ils ont été émis sans informations liées à la révocation. »

La réponse d'Entrust :

« Aucune preuve n'indique que les autorités de certification malaisiennes Digicert aient été compromises. »

Le piratage des clés

Voici quelques remarques relatives au coût et aux exigences techniques pour attaquer ces certificats.

La puissance de calcul requise pour pirater et réusiner un code RSA 512 bits était de 5 000 dollars et la durée requise était d'environ deux semaines. (voir http://lukenotricks.blogspot.co.at/2010/03/rsa-512-factoring-service-two-weeks.html)

En octobre 2012, Tom Ritter a rapporté que le coût s'élèverait à 120-150 dollars, voire même à une somme aussi modeste que 75 dollars.

Si l'on revient plus en arrière encore, il y avait une grande discussion relative aux méthodes techniques de piratage de ces clés :
L'article de DJ Bernstein en 2001 sur la construction d'une machine réduisant les coûts de factorisation intégrée avec les techniques Number Field Sieve, permettant de casser les codes RSA 1 024 bits.

Réaction et déclaration de 2002 de RSA à savoir si les codes RSA 1 024 bits sont cassés ou non : « Le NIST a proposé un tableau avec différentes tailles de clés pour la discussion de son « workshop » en novembre 2001 [7]. Pour les données devant être protégées en 2015 au plus tard, le tableau indique que la taille de la clé doit être au moins égale à 1 024 bits. Pour les données devant être protégées au-delà, la taille de la clé doit être au moins égale à 2 048 bits. »

Autres certificats Tapaoux

Les récentes attaques et backdoors Tapaoux comprennent un programme malveillant signé avec des certificats importants SHA1/RSA 2 048 bits, ce qui suggère un vol de certificat.

Certificat racine	CA/Émetteur subordonné(e)	Propriétaire	Statut	Valide du	Valide jusqu'au
thawte	thawte Primary Root CA	Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2 048 bits)	Révoqué	18/07/2013	16/07/2014
thawte	thawte Primary Root CA	Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd. sha1/RSA (2 048 bits)	Révoqué	05/11/2013	05/11/2014

Enregistreurs de frappe et développements

L'un des composants les plus intéressants que nous avons découverts dans le cadre de cette campagne est l'utilisation d'un enregistreur de frappe avancé, signé numériquement. Il s'agit d'un logiciel malveillant de noyau propre et bien écrit. Les langues de ses segments sont un mélange d'anglais et de coréen. Il est signé avec le certificat numérique familier « belinda.jablonski@syniverse.com ».

Cet enregistreur de frappe est déposé par le code qui s'exécute au sein de svchost.exe sur WinXP SP3, qui entretient un segment de débogage intéressant : d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb

Remarque 일반 signifie « Général » en coréen

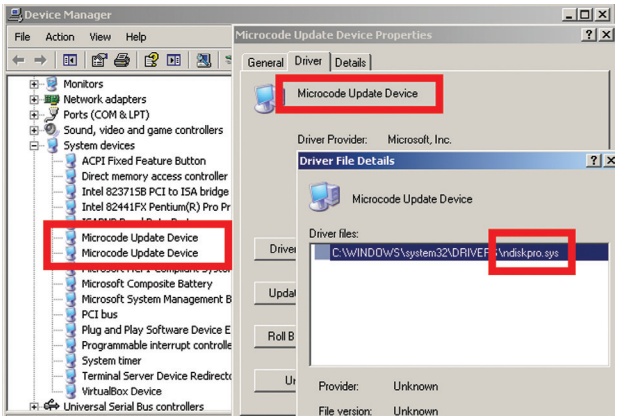
Il a probablement été développé dans le cadre d'un projet entre mi 2009 et fin 2009 :
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.c

Code d'enregistreurs de frappe

Ce package pilote est conçu pour ressembler à un appareil du système Microsoft bas de gamme légitime. Il est installé comme un service « Ndiskpro » du pilote du noyau système, décrit comme un « appareil de mise à jour du microcode ». Il est un peu surprenant qu'aucune fonctionnalité rootkit ne cache ce service.

```
SERVICE_NAME: Ndiskpro
DISPLAY_NAME: Ndiskpro
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

Lorsqu'il est téléchargé, le pilote DISKPRO.SYS se fixe sur les deux INT 0x01 et INT 0xff et récupère des données de frappe directement à partir du port 0x60, le contrôle du clavier principal. Il met les données du composant de mode utilisateur exécuté en cache puis les communique aux utilisateurs connectés. Ce composant chiffre ensuite et inscrit les valeurs récupérées sur le disque dans un fichier .tmp dont le nom est aléatoire comme ffffz07131101.tmp. Ce fichier se trouve dans le même répertoire que l'injecteur original, qui persiste à effectuer des amorces avec un simple ajout à la clé d'exécution HKCU.



Le module d'enregistreur de frappe chiffre et stocke les données recueillies dans un fichier journal, comme énoncé précédemment. Son algorithme de chiffrement est similaire au RC4. Ce qui est intéressant, c'est que le module génère la clé de manière aléatoire et la stocke à un emplacement inattendu : au milieu du nom du fichier journal. La partie numérique du nom de fichier est donc utilisée comme un implant pour le générateur de nombres pseudo aléatoires. La fonction rand est statistiquement liée pour garantir les mêmes résultats sur différents ordinateurs.

Composants intéressants des programmes malveillants

Les outils Darkhotel consistent en une série de composants ayant été légèrement modifiés au fil du temps. Ces outils sont injectés par les programmes d'installation des hôtels imitant des programmes d'installation de logiciels légitimes, liés à des ensembles torrent, ou déposés par des exploitations de failles ou des liens hypertexte provenant d'e-mails de phishing ciblé.

Des outils plus avancés, tels que l'enregistreur de frappe décrit plus haut, sont ensuite téléchargés par le système de la victime par l'un de ces implants. Récemment, des documents Word intégrés avec des fichiers flash swf zero-day ont injecté ces backdoors ou les ont téléchargés et exécutés à partir de serveurs Web à distance. Ces outils affaiblissent l'enregistreur de frappe, volent des informations du système ou téléchargent d'autres outils.

- module de téléchargement de petite taille
- outil de vol d'informations
- cheval de Troie
- dropper et injecteur
- virus sélectif

Les comportements les plus intéressants de ces composants comprennent

- une durée conditionnelle très inhabituelle de 180 jours des communications de commande et de contrôle
- des programmes d'auto-destruction lorsque la page de codes par défaut du système est paramétrée en coréen
- un traitement du vol d'authentification Microsoft IntelliForm amélioré
- un module d'assistance Internet Explorer Firefox, et Chrome pour le vol d'informations
- une gestion de l'identifiant de campagne ou de phase
- une sensibilité de l'exécution de la machine virtuelle
- des programmes d'infections virales sélectives afin de concentrer la propagation du programme malveillant au sein des organisations
- programme malveillant signé (signalé précédemment)

Module de téléchargement de petite taille

Ce module est de petite taille (27 Ko) et se présente comme étant une partie du fichier WinRar SFX qui est déposé et démarre le module à partir de %APPDATA%\Microsoft\Crypto\DES64v7\msieckc.exe. Le module est conçu pour mettre à jour les composants malveillants en se connectant régulièrement au serveur C&C. Il peut également supprimer d'anciennes composantes, dont le nom est codé en dur dans le corps du malware. Le module ajoute des paramètres du registre d'auto-exécution pour permettre un démarrage automatique lors de l'amorce du système.

L'une des fonctions les plus intéressantes de cet exécutable concerne sa durée et sa persistance inhabituelle. S'il existe un fichier spécial dans le système, le module ne tentera pas de rappeler le serveur C&C avant que le fichier spécial n'ait atteint 180 jours. Donc, dans le cas où un composant malveillant critique serait supprimé durant cette période, le module actuel sauvegarde et restaure l'accès au système sous 6 mois.

Le composant recueille des informations du système et les transmet aux serveurs de commande et de contrôle Darkhotel comme expliqué dans l'annexe D.

Outil de vol d'informations

Ce module est d'une taille relativement importante (455 Ko) et se présente comme étant une partie du fichier WinRar SFX qui est déposé et démarre le module à partir de %APPDATA%\Microsoft\Display\DmaUp3. Le principal but du module est de recueillir divers secrets stockés dans un système local et de les télécharger sur les serveurs de commande et de contrôle Darkhotel.

- Mots de passe en cache provenant d'Internet Explorer 6/7/8/9 (Stockage Windows protégé)
- Secrets Mozilla Firefox stockés (<12.0)
- Secrets Chrome stockés
- Identifiants Gmail Notifier
- Identifiants et données traitées Intelliform
  - Twitter
  - Facebook
  - Yandex
  - Qip
  - Nifty

- Mail.ru
- 126.com email
- Zapak
- Lavabit (service e-mail chiffré désormais clôturé)
- Bigstring
- Gmx
- Sohu
- Zoho
- Sina
- Care2
- Mail.com
- Fastmail
- Boîte de réception
- Gawab (service e-mail du Moyen-Orient)
- 163.com
- Lycos
- Lycos mail
- Connexion Aol
- Yahoo! Connexions
- Yahoo! Connexions Japon
- Connexions Microsoft Live
- Identifiants de connexion Google

Ce module est conçu pour se fermer de lui-même sur Windows avec la page de code par défaut du système paramétrée en coréen.

Trojan.Win32.Karba.e

La taille de ce malware est de 220 Ko. Il a été créé comme une application MFC avec de nombreux appels supplémentaires qui auraient dû compliquer l'analyse de l'échantillon. Il imite une application bureau GUI mais ne crée pas de fenêtre visible ni de boîte de dialogue pour interagir avec les utilisateurs locaux. Le cheval de Troie recueille des données relatives au système et au logiciel anti-virus installé sur celui-ci et télécharge ces données sur les serveurs de commande et de contrôle Darkhotel. Plus de détails techniques sont fournis dans l'annexe D.

Chevaux de Troie dropper et injecteur (fichiers légitimes infectés)

La taille de ce malware est de 63 ko. Il est lié à une variété d'autres packages de logiciels dont le nom varie mais le package hôte est systématiquement détecté comme étant « Virus.Win32.Pioneer.dx ». Il dépose le composant « virus sélectif » igfxext.exe sur le disque et l'exécute.

Virus sélectif

Ce composant est un **virus** et est utilisé pour s'infiltrer de manière sélective dans d'autres ordinateurs par le biais de clés USB ou de partages de réseau.

Le virus récupère d'abord tous les disques disponibles et du disque n° 4 (D:\) au disque n° 20 (Z:\), il trouve des fichiers exécutables et les infecte. Le code force simplement la liste des pilotes supprimables mis en correspondance.

Lors du programme d'infection, le virus modifie le point d'entrée des fichiers exécutables, crée une section .rdat puis insère un petit chargeur dans la section et doit ensuite placer la charge principale sur le dessus. Chaque fichier infecté a des fonctionnalités décrites dans la rubrique Chevaux de Troie dropper et injecteur. Il peut donc recueillir des informations relatives à l'ordinateur, les transmettre au C&C et télécharger d'autres composants Darkhotel comme cela lui est dicté. Les composants téléchargés observés sont signés avec un certificat familier expiré provenant de www.esupplychain.com.tw, émis par Cybertrust SureServer CA.

Plus de détails techniques se trouvent également dans l'annexe D.

Codes des campagnes

Chaque backdoor de cet ensemble ou presque dispose d'un code ou identifiant de campagne interne, utilisé dans les communications C&C, comme décrit plus haut. Certains identifiants sont liés à des intérêts géographiques, quand d'autres n'ont aucune caractéristique. Nous avons établi une liste des identifiants de campagne Darkhotel détaillée ci-après. Les identifiants internes et les ressources C&C se chevauchent d'un composant à un autre, il n'y a pas de schéma de distribution correspondant pour reconnecter les ressources. L'identifiant le plus courant est « DEXT87 » :

DEXT87	NKstep2-auto
step2-auto	PANA(AMB)-auto
dome1-auto	PANA#MERA
step2-down	SOYA#2-auto
Java5.22	step2-down-u
C@RNUL-auto	(ULT)Q5SS@E.S-down
dome-down	VER1.5.1
M1Q84K3H	VICTORY
NKEX#V1.Q-auto	WINM#V1.Q

Infrastructure et victimes

L'équipe infrastructure semble exploiter des compétences moins pointues que les campagnes de premier ordre, disposant de configurations de serveur faible avec des réactions défensives et une surveillance limitée et en commettant quelques erreurs basiques. Cependant, elle est efficace en termes d'infrastructure totalement disponible pour prendre en charge les infections nouvelles et actuelles.

Dans l'ensemble, les victimes de nos journaux sinkhole et données KSN se trouvent partout dans le monde, mais la majorité au Japon, à Taiwan, en Chine, en Russie, en Corée et à Hong Kong.

Domaines Sinkhole

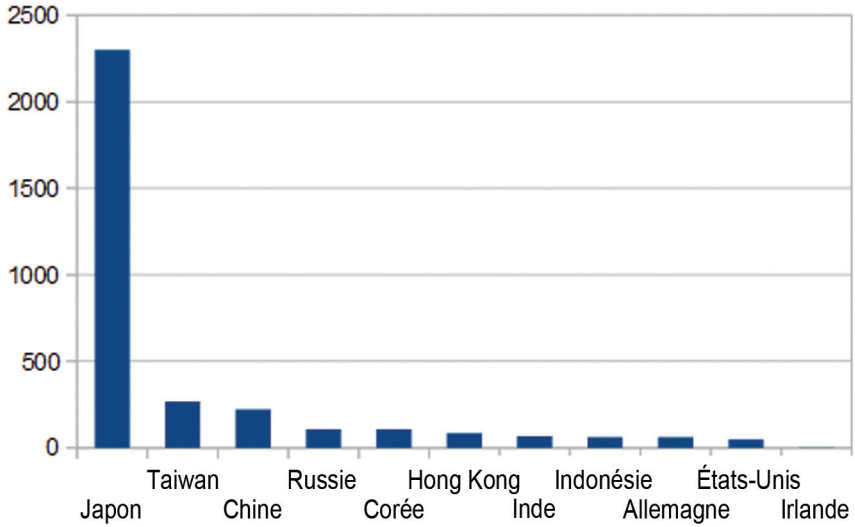
Les domaines C&C suivants ont fait l'objet d'un Sinkhole et ont été redirigés vers les serveurs Sinkhole Kaspersky.

42world.net
academyhouse.us
adobeplugs.net
amanity50.biz
autocashhh.hostmefree.org
autochecker.myftp.biz
autoshop.hostmefree.org
autoupdatfreeee.coolwwweb.com
checkingvirusscan.com
dailyissue.net
dailypatch-rnr2008.net
fenraw.northgeremy.info
generalemountina.com
goathoney.biz
jpnspts.biz
jpqueen.biz
mechanicalcomfort.net
micromacs.org
ncnbroadcasting.reportinside.net
neao.biz
private.neao.biz
reportinside.net
self-makeups.com
self-makingups.com
sourcecodecenter.org
support-forum.org
updatewifis.dyndns-wiki.com

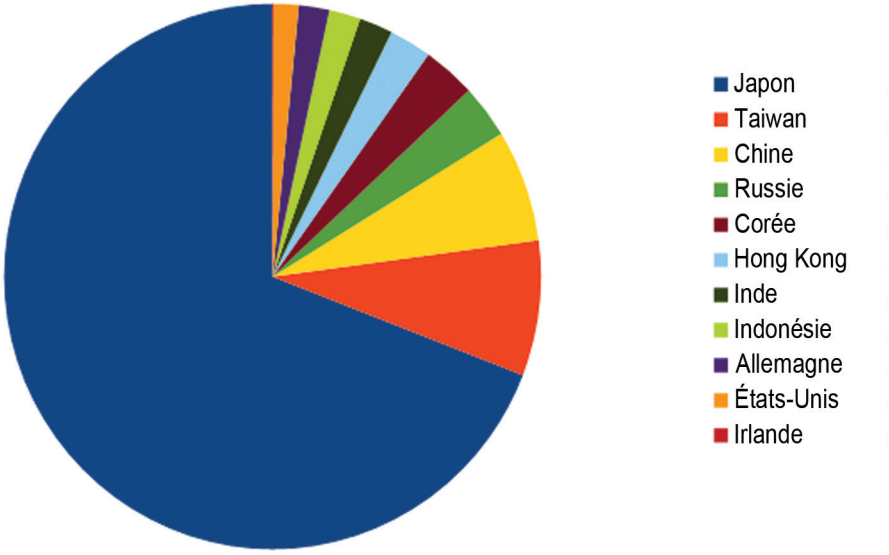
Localisation des victimes - Données KSN et Sinkhole

Données KSN

Notre réseau de sécurité, Kaspersky Security Network, a détecté des infections Darkhotel sur des milliers de machines, principalement liées aux campagnes p2p Darkhotel. Ces estimations de géolocalisation nous donnent probablement l'idée la plus précise des lieux où l'activité de Darkhotel se produit.

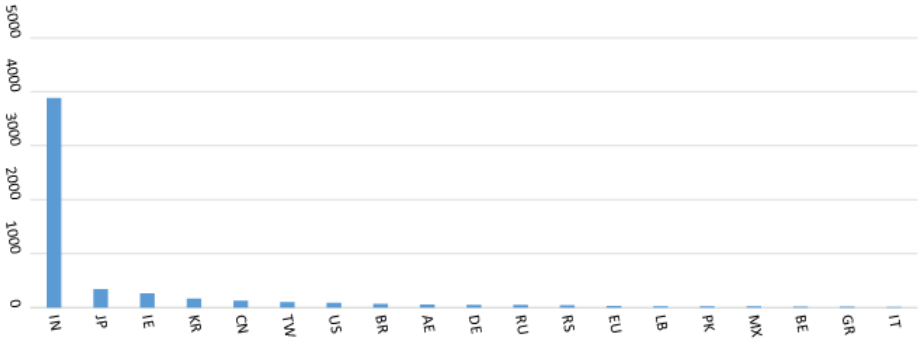


Voici un diagramme pour vous permettre de mieux visualiser les proportions des attaques dans le monde entier. Comme vous pouvez le voir, plus de 90 % de celles-ci se produisent dans les pays du top 5 : le Japon, suivi de Taïwan, la Chine, la Russie et la Corée.



Données Sinkhole

Les opérateurs ayant développé de manière très active les serveurs de commande et de contrôle, il est difficile de disposer de suffisamment de domaines Sinkhole pour avoir une idée générale précise de la localisation du système des victimes sur la base de ces données. En outre, de nombreux systèmes de recherche sont connectés aux domaines Sinkhole. Cependant, le graphique des rappels Sinkhole présente une répartition peu fiable de la géolocalisation des victimes lorsque l'Inde, le Japon, l'Irlande, la Corée, la Chine et Taïwan sont en tête de liste. Lorsque l'on supprime l'Irlande et l'Inde, l'ensemble correspond plus à nos données KSN.



Données de victimes ddrlog disponibles

Nombre de ces C&C disposent d'un chemin de répertoire courant distribuant un ddrlog. Ils apparaissent pour conserver les données de rappel que les assaillants veulent mettre de côté grâce à des journaux d'erreur. De nombreuses URL de rappel contiennent des erreurs, certaines proviennent de séries d'adresses IP indésirables et d'autres sont clairement des rappels indésirables de système sandbox de chercheurs.

Une description des valeurs d'URL de reconnexion détaillées et de leur système d'encodage xor/base64 est incluse dans les notes techniques de l'annexe D « Interesting Malware Trojan.Win32.Karba.e ».

Le C&C Darkhotel conserve ces structures de répertoire pour stocker et fournir du contenu ddrlog :

- /bin/error/ddrlog
- /patch/error/ddrlog

Les structures suivantes sont courantes parmi les serveurs mais ne produisent pas de ddrlog et n'ont pas de répertoire /erreur/ répertoire :

- /u2/
- /u3/
- /patch2/
- /major/
- inor/
- /asp/
- /update3/

Deux saisies de rapports de fichiers ddrlog à partir du 1er janvier 2009 à 9 h 16.

- autozone.000space.com
- genuinsman.phpnet.us

Tous les journaux disposent d'un nombre de saisies significatif, près de 50 000, assorties d'un simple tampon « B » ou « L ». Ces enregistrements sont formatés comme suit :

```
2009.01.01 09:16:00 150.70.xxx.xx --> B
2009.01.01 09:16:33 150.70.xxx.xx --> B
2009.01.01 09:14:52 220.108.x.xxx --> L
2009.01.01 09:16:04 112.70.xx.xx --> L
```

Seules 120 adresses IP ont exécuté la saisie « B » et 90 % d'entre elles se trouvent dans la série 150.70.97.x. La série complète appartient à Trend Micro à Tokyo, Japon.

Quelques-unes des adresses restantes, telles que 222.150.70.228, proviennent d'autres séries dont le propriétaire est Trend Micro au Japon. Le FAI El Salvadoran est une exception et une autre est connectée à un FAI japonais. Environ 20 000 adresses IP effectuent la saisie « L ».

D'autres ddrlogs peuvent comprendre les balises « A » également.

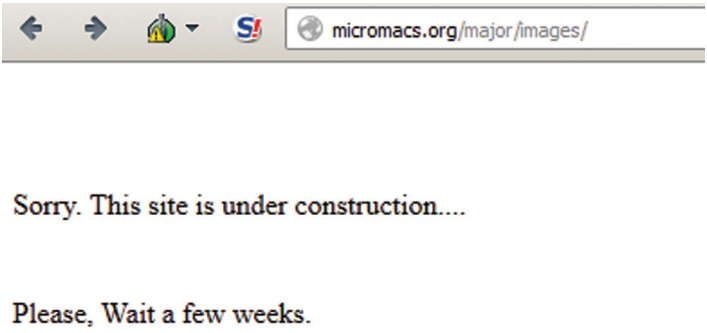
La balise « A » caractérise les visites non souhaitées de la part de localisations non ciblées telles que la Hongrie et l'Italie. La balise « B » caractérise les visites non souhaitées de la part des adresses IP Trend Micro.

La balise « L » caractérise les visites non souhaitées de la part de différentes adresses, mais comprend des IP irrégulières telles que l'adresse de boucle, 127.0.0.1, qui est de toute évidence une erreur.

Les saisies dans ces journaux comprennent des URL de rappel incluant des espaces et des caractères inhabituels non conformes au dictionnaire de caractères base64 requis.

Communications et structure C2

Page principale habituelle:



Pour begatrendstone.com, la structure de répertoire est la suivante :

/bin
    -read_i.php (script C&C principal)
    -login.php (inconnu, répond « Identifiant erroné () »)
/bin/error (journaux des erreurs disponibles ici)
    -ddrlog
/bin/tmp
 /bin/SElhxxwiN3pxxiAPxxc9
    -all.gif
    /i
    - contenu chiffré volé du système des victimes
    /L
    /f

Pour auto2116.phpnet.us, nous avons la structure de répertoire suivante :

/patch
    -chkupdate.php (script de commande et de contrôle principal)
/patch/error
    -ddrlog

Le groupe chiffre les données des victimes sur ses serveurs avec des combinaisons utilisateur/mot de passe unique pour plusieurs victimes. Lorsqu'un utilisateur non autorisé tente d'accéder à l'interface Web Darkhotel de gestion des victimes en ne disposant pas du mot de passe correct, la page html et la mise en page du tableau s'affichent correctement mais toutes les valeurs de données sur la page ressemblent à du chiffre-texte confus.

Gestion des victimes

Les systèmes des nouvelles victimes sont systématiquement contrôlés. Les assaillants disposent d'une interface Web pour contrôler les systèmes des nouvelles victimes. Tout d'abord, les assaillants listent et trient les systèmes de leurs victimes en fonction de leur dernière visite C&C. Les données recueillies sont probablement présentées dans l'ordre d'importance :

1. nom de connexion de l'utilisateur
2. système d'exploitation et processeur
3. « Ping sec » ou à quelle distance le système de la victime se trouve-t-il du C&C
4. « In » ou le procédé que le code dll des assaillants exécute
5. Vac : Identification du produit antivirus
6. système IP LAN
7. réseau IP WAN

Voici un exemple de l'une de ces pages Web :

Last connection	Information
0d 0h 2m 17s	Sys@User : [redacted] (0411) C P U : Intel(R) Pentium(R) M processor 1600MHz System OS: Microsoft Windows XP (Service Pack 3) Ping sec : [redacted]ms -> average [redacted]ms In : C:₩WINDOWS₩system32₩alg.exe Vac : Net card : [redacted] ([redacted]) Inter IP : [redacted]
0d 3h 10m 49s	Sys@User : [redacted] (0411) C P U : Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz System OS: Windows 7 Professional () Ping sec : [redacted]ms -> average [redacted]ms In : c:₩program files (x86)₩uTorrent₩uTorrent.exe Vac : TR, Net card : [redacted] ([redacted]) Inter IP : [redacted]

Activité des chercheurs

Il est évident que des activités d'analyse automatisées impliquant des outils sandbox de chercheurs remplissent ces journaux. De juin 2013 à avril 2014 (une période de presque 11 mois), dans seulement 15 fichiers ddrlog, nous observons presque 7 000 connexions à partir de systèmes sandbox de recherche. Les connexions au réseau fournissent des valeurs a1= à a3= identifiant un sandbox provenant d'un QEMU, toutes provenant uniquement d'adresses IP 485 WAN. Les adresses IP en dessous de 30 lan sont toutes enregistrées dans la même série 172.16.2.14-126. Ce(s) système(s) utilise(nt) un compte utilisateur « Dave » et un nom de système Windows « HOME-OFF-D5F0AC ».

Ces caractéristiques correspondent à l'activité de réseau générée par les outils du logiciel « CWsandbox » de GFI, appartenant désormais à « ThreatTrack Security ».

Conclusions

Ces sept dernières années, une cyber-menace importante du nom de Darkhotel, également connue sous celui de Tapaoux, a mené à bien nombre d'attaques à l'encontre d'une grande diversité de victimes du monde entier. Cette menace emploie des méthodes et des techniques allant bien au-delà du comportement cybercriminel habituel.

Les compétences des pirates de Darkhotel leur permettent de lancer des attaques cryptographiques intéressantes, comme par exemple le réusinage de code RSA 512 bits. Leur utilisation des zero-days est une autre indication d'une cyber-menace importante.

Le ciblage de cadres haut placés de diverses grandes entreprises dans le monde, pendant leur séjour, dans certains « hôtels sombres », est l'un des aspects les plus intéressants de cette opération. La méthode exacte de ciblage reste pour l'heure inconnue, notamment, pourquoi certaines personnes sont-elles ciblées alors que d'autres ne le sont pas. Le fait que la plupart du temps les victimes sont des cadres haut placés indique que les assaillants ont connaissance des activités de leurs victimes, notamment leur nom et le lieu de leur séjour. Ceci dépeint un piège sombre et dangereux dans lequel les voyageurs peu méfiants peuvent facilement tomber. Nous ne savons pas exactement pourquoi certains hôtels sont vecteurs d'attaques. Certains soupçons indiquent cependant une compromission encore plus importante. Nous enquêtons toujours sur cet aspect de l'opération et nous publierons plus d'informations à ce sujet à l'avenir.

Une autre caractéristique intéressante est le déploiement de divers types de campagnes, à la fois ciblées et botnet. Ceci est de plus en plus courant en ce qui concerne les menaces persistantes avancées, lorsque des attaques ciblées sont utilisées pour compromettre des victimes particulièrement visibles et que des opérations de style botnet pour une surveillance à grande échelle ou d'autres actions telles que le fait de lancer des attaques DDoS (déni de service) à l'encontre de tiers hostiles ou simplement en utilisant des outils d'espionnage plus sophistiqués envers des victimes antérieures.

Nous nous attendons à voir les pirates de Darkhotel continuer leurs activités à l'encontre des secteurs de la Base industrielle de défense, du gouvernement et des ONG. L'annexe publiée avec ce document fournit des indicateurs techniques de compromission qui devraient aider les victimes à identifier tout trafic malveillant et permettre aux cibles de mieux se protéger contre les attaques.

Siège de Kaspersky Lab

39A/3 Leningradskoe Shosse
Moscou, 125212
Fédération de Russie

autres coordonnées

Tél : +7-495-797-8700
Fax : +7-495-797-8709

E-mail : info@kaspersky.com
Site Web : www.kaspersky.com