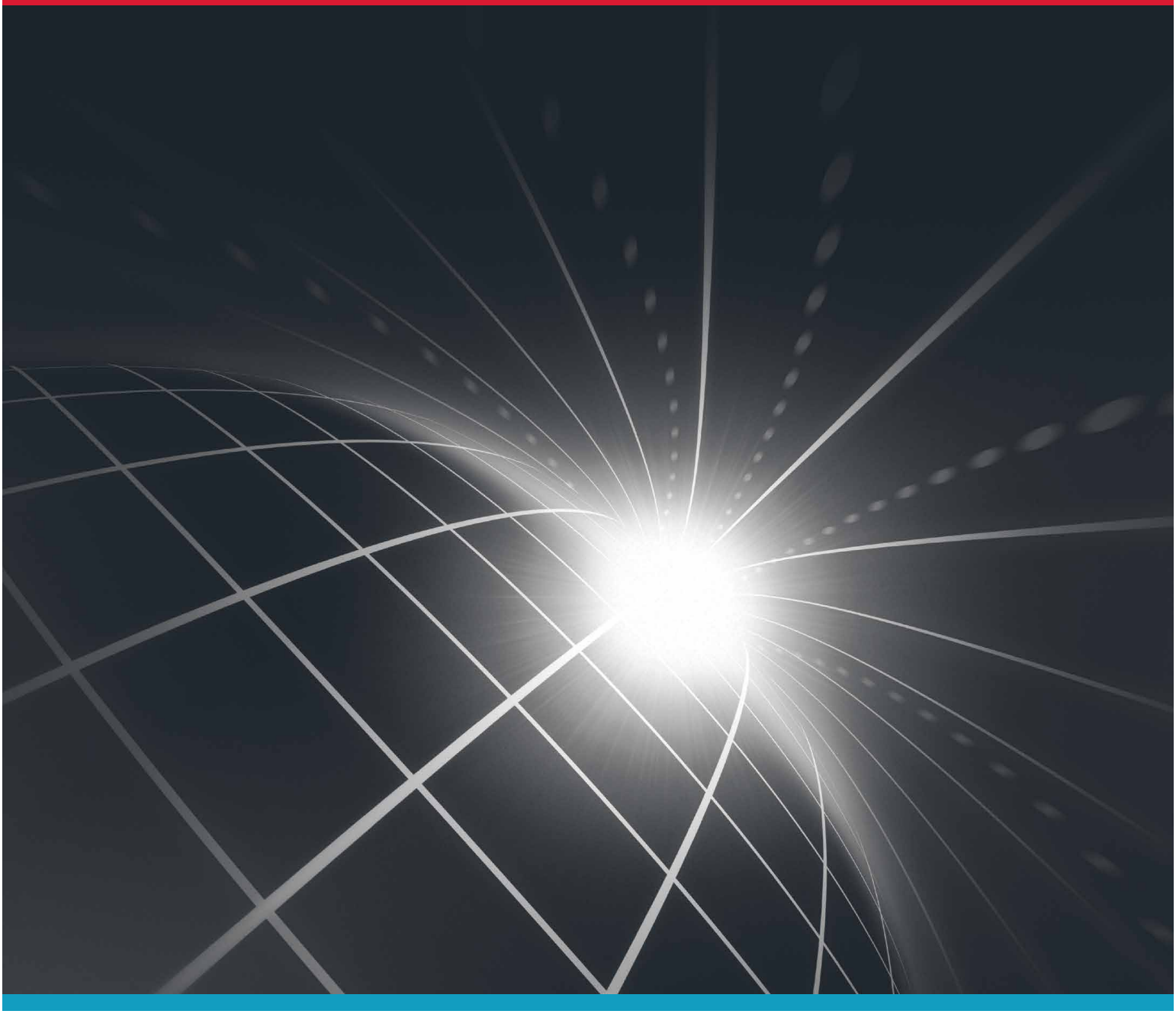
FireEye™

À la recherche de traces numériques : sept indices pour identifier l'auteur d'une cyberattaque avancée



Sommaire

Résumé

Dans le paysage actuel des cybermenaces, l'identification de l'ennemi joue un rôle clé dans toute stratégie de défense. Pour protéger efficacement vos données et autres éléments de propriété intellectuelle, il est essentiel de percer à jour l'identité des auteurs d'attaque, leur modus operandi et les objectifs qu'ils poursuivent.

Heureusement, les systèmes informatiques compromis, à l'instar de n'importe quelle scène de crime, recèlent de précieux indices. L'auteur d'une cyberattaque avancée peut se trahir par l'intermédiaire du code de son logiciel malveillant (*malware*), de ses emails d'hameçonnage, des serveurs de commande et de contrôle qu'il utilise, et même de son comportement. Tout comme les relevés d'empreintes et les analyses de l'ADN ou des fibres sont devenus des outils indispensables de la police scientifique, le recoupement de tous les indices laissés par une cyberattaque avancée peut permettre de démasquer les pirates les plus ingénieux, pour autant que les chercheurs sachent quelles pistes explorer.

Fondé sur un échantillon de près de 1 500 campagnes d'attaques analysées par FireEye®, le présent document se penche sur les diverses facettes des attaques de logiciels malveillants et sur les indices qu'elles révèlent souvent au sujet des coupables :

- **Disposition du clavier.** Les tentatives d'hameçonnage recèlent des informations sur la configuration du clavier de l'auteur de l'attaque, qui varie selon la langue et la région.
- **Métadonnées des logiciels malveillants.** Le code source du logiciel malveillant contient des détails techniques qui laissent deviner la langue de son auteur, son emplacement géographique et d'éventuels liens à d'autres campagnes.
- **Polices incorporées.** Les polices utilisées dans les e-mails d'hameçonnage donnent des indications sur l'origine de l'attaque même si les polices ne sont généralement pas utilisées dans la langue maternelle de l'auteur.
- **Enregistrement DNS.** Les domaines utilisés dans les attaques permettent d'en localiser l'auteur. Des informations d'enregistrement récurrentes permettent de lier plusieurs domaines à un même coupable.
- **Langue.** Les artefacts linguistiques incorporés dans les logiciels malveillants donnent souvent des indications sur le pays d'origine du cybercriminel. Qui plus est, la rétroconception d'erreurs linguistiques courantes dans les e-mails d'hameçonnage permet parfois de déterminer la langue maternelle de l'auteur.
- **Configuration des outils d'administration à distance.** Les outils de création de logiciels malveillants les plus populaires incluent une pléthore d'options de configuration. Le choix d'options est souvent révélateur du cybercriminel qui se sert de l'outil, ce qui permet aux chercheurs d'associer des attaques distinctes à un même auteur.
- **Comportement.** Les caractéristiques comportementales, notamment les méthodes et les cibles, peuvent fournir des indices sur les techniques et les motivations de l'auteur de l'attaque.

L'étude de ces différents éléments permet aux professionnels de la sécurité informatique d'identifier plus rapidement les auteurs des menaces et de mieux défendre leurs organisations contre les futures cyberattaques.

Introduction

Bien que les cyberattaques aient gagné en sophistication et en résilience au cours des dernières années, le crime parfait n'existe pas. Chaque étape de la chaîne de frappe de l'attaque — la reconnaissance, la conception de « l'arme », la distribution, l'exploitation, l'installation, la commande et le contrôle ainsi que les actions propres à l'objectif de l'attaque (généralement l'exfiltration)[1] — peut laisser des traces numériques.

En effet, chaque phase exige un point de contact quelconque entre l'auteur de l'attaque et sa cible. Dans certains cas, il s'agit d'un contact direct, par exemple par un e-mail d'hameçonnage, et dans d'autres, il est indirect, notamment lors d'un rappel connectant les ordinateurs pris pour cible au système du cybercriminel. Quel que soit le type de contact, il représente une occasion d'en apprendre davantage sur l'auteur de l'attaque. Si elles sont analysées correctement, les informations collectées permettent aux professionnels de la sécurité de mieux maîtriser les dommages, de réparer les systèmes compromis et d'anticiper les futures attaques.

Mise en garde. Bien que les techniques d'investigation numérique présentées dans ce rapport se soient avérées utiles pour les chercheurs de FireEye, les indices sont souvent trompeurs et contradictoires. L'analyse des preuves est une tâche complexe et de longue haleine — un mariage subtil de science et d'art qui met rarement au jour une preuve « irréfutable ». Les cybercriminels sont passés maîtres dans l'art de brouiller les pistes ; il ne faut donc prendre aucun indice pour argent comptant. FireEye recommande vivement d'analyser et de comparer des preuves de plusieurs sources et de faire appel à un expert en investigation numérique avant d'émettre une conclusion définitive sur l'origine d'une attaque.

1. Disposition du clavier

Les chercheurs peuvent déterminer la disposition de clavier utilisée pour créer un logiciel malveillant en examinant l'attribut « charset » (jeu de caractères) de l'en-tête des e-mails d'hameçonnage. Dans la plupart des cas, les auteurs de tentatives d'hameçonnage utilisent une disposition de clavier standard qui ne révèle rien sur le pays d'origine. En revanche, l'emploi d'un clavier non standard fournit un indice probant.

Les chercheurs de FireEye ont découvert que de nombreux aspects de campagnes de logiciels malveillants dénotent l'utilisation d'un clavier mandarin (GB2312) propre à la Chine. De la même façon, le jeu de caractères KPS 9566, spécifique de la Corée du Nord, facilite l'identification des attaques émanant de cette région.

Cela étant, le recours à une telle méthode pour retracer l'origine d'une attaque n'est pas totalement fiable. En théorie, un ressortissant russe pourrait, par exemple, employer un clavier nord-coréen pour dissimuler son identité et son emplacement géographique.

En mars 2012, Alex Lanstein, chercheur chez FireEye, a envoyé un e-mail à plusieurs activistes tibétains pour les avertir d'une cyberattaque dont ils étaient la cible. Les auteurs de l'attaque sont parvenus à obtenir une copie de l'e-mail d'Alex Lanstein de l'une des cibles et s'en sont servi pour appâter d'autres activistes. À la différence de l'e-mail d'origine, associé au clavier occidental standard (Windows-1252), le message utilisé comme leurre provenait d'un expéditeur qui utilisait la disposition de clavier chinoise GB2312.

1 Eric M. Hutchins, Michael J. Cloppert et Rohan M. Amin (Lockheed Martin). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Novembre 2010.

La figure 1 illustre l'e-mail utilisé comme leurre. La figure 2 montre les informations d'en-tête de l'e-mail qui révèlent la disposition du clavier.

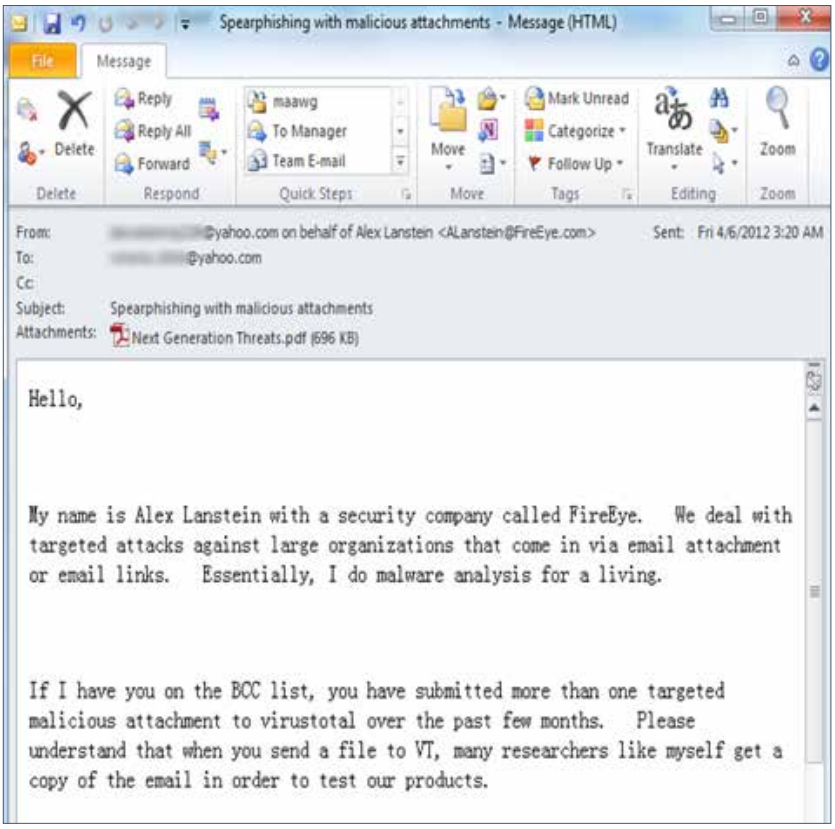


Figure 1 — E-mail d'hameçonnage envoyé comme leurre à des militants tibétains.

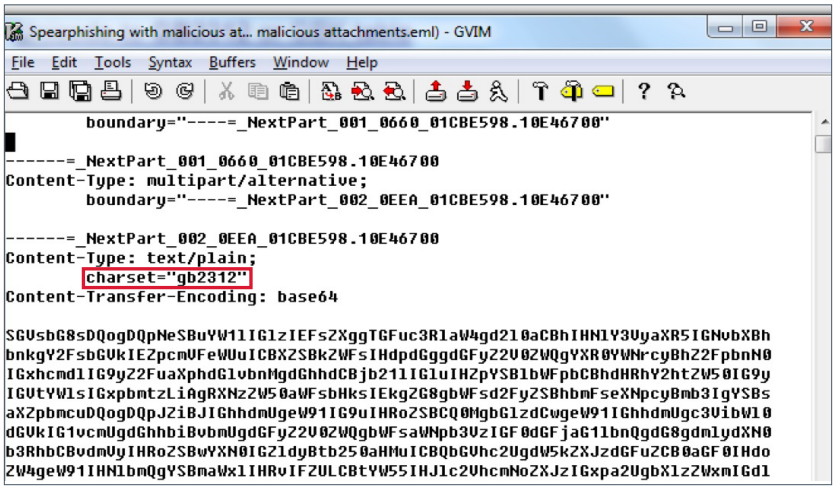


Figure 2 — Codage du jeu de caractères dans un e-mail d'hameçonnage (voir figure 1).

2. Métadonnées des logiciels malveillants

Le code exécutable d'un logiciel malveillant référence souvent le répertoire source d'origine qui organise la structure du code source. De la même façon, un programme écrit en langage C++ fait référence à un nom de projet. Ce code sous-jacent peut révéler la langue ou le pays d'origine de l'auteur de l'attaque, même si le code et d'autres aspects de l'attaque sont personnalisés en fonction de la langue de la cible.

La figure 3 illustre le code source de la troisième phase d'une attaque récente. Ici, son auteur insulte l'éditeur de logiciels antivirus chinois Beijing Rising (épelé phonétiquement « Ruixing ») International Software Co.

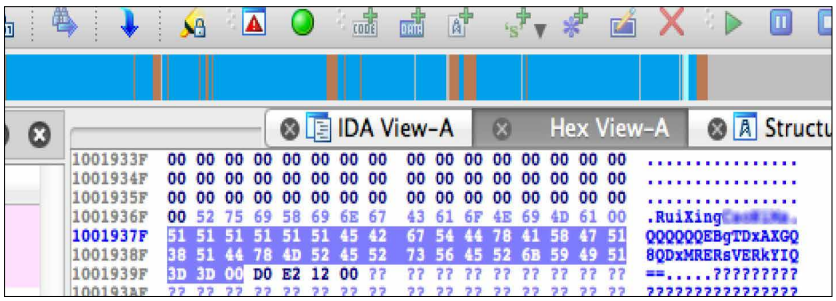


Figure 3 — Code source du logiciel malveillant insultant l'éditeur de logiciels antivirus chinois Beijing Rising (épelé phonétiquement « Ruixing »). L'insulte a été délibérément gommée dans la capture d'écran.

La figure 4 montre le code source de la deuxième phase d'une attaque dont la publication a été précédemment annulée, à savoir un fichier exécutable dissimulé sous la forme d'un fichier PNG. Il a été distribué au système d'extrémité après la compromission initiale. Le code inclut une référence à un fichier de débogage de processus (PDB, Process Debugging) hébergé sur le disque dur de l'auteur du logiciel malveillant sous « E:\pjts2008\moon\Release\MoonClient2.pdb ». (Les fichiers PDB sont créés pour les programmes écrits dans l'environnement Windows .NET Framework.) Le fichier « MoonClient » auquel il est fait référence est une variante du logiciel malveillant WEBC2 utilisé par le groupe de pirates chinois APT1, également connu sous le nom « CommentGroup ».

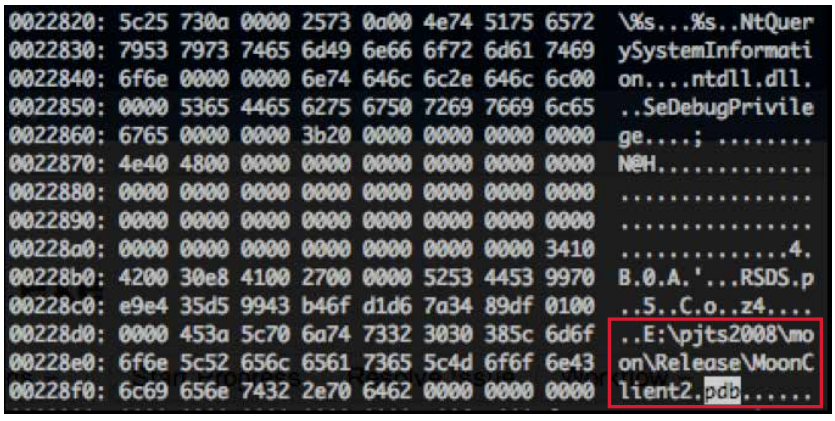
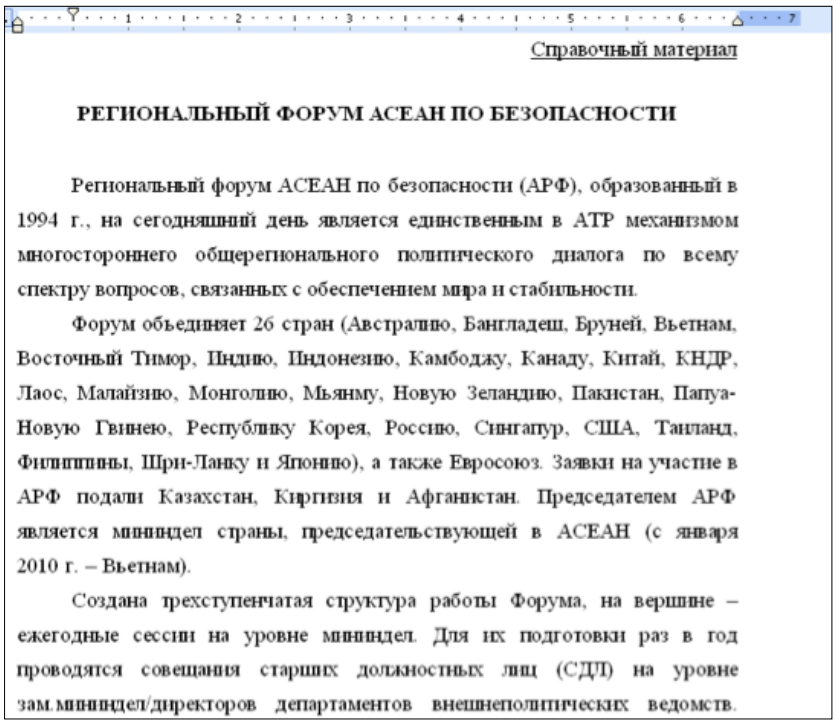


Figure 4 — Fichier exécutable décodé (avec mise en évidence de la référence PDB).

3. Polices incorporées

À l'instar de l'attribut « charset » décrit dans la section « Disposition du clavier », la police utilisée dans les e-mails d'hameçonnage et d'autres documents malveillants peut parfois être utile pour retracer la source d'une menace persistante avancée.

Prenons l'exemple de la menace persistante avancée Sanny, récemment découverte par les chercheurs de FireEye. La figure 5 montre le document utilisé comme leurre pour appâter les cibles.



Справочный материал

РЕГИОНАЛЬНЫЙ ФОРУМ АСЕАН ПО БЕЗОПАСНОСТИ

Региональный форум АСЕАН по безопасности (АРФ), образованный в 1994 г., на сегодняшний день является единственным в АТР механизмом многостороннего общерегионального политического диалога по всему спектру вопросов, связанных с обеспечением мира и стабильности.

Форум объединяет 26 стран (Австралию, Бангладеш, Бруней, Вьетнам, Восточный Тимор, Индию, Индонезию, Камбоджу, Канаду, Китай, КНДР, Лаос, Малайзию, Монголию, Мьянму, Новую Зеландию, Пакистан, Папуа-Новую Гвинею, Республику Корея, Россию, Сингапур, США, Таиланд, Филиппины, Шри-Ланку и Японию), а также Евросоюз. Заявки на участие в АРФ подали Казахстан, Киргизия и Афганистан. Председателем АРФ является министр страны, председательствующей в АСЕАН (с января 2010 г. – Вьетнам).

Создана трехступенчатая структура работы Форума, на вершине – ежегодные сессии на уровне министров. Для их подготовки раз в год проводятся совещания старших должностных лиц (СДЛ) на уровне зам.министров/директоров департаментов внешнеполитических ведомств.

Figure 5 — Document-leurre écrit en caractères cyrilliques mais utilisant une police coréenne.

Bien que le document-leurre ait été rédigé en russe pour cibler des intérêts russes, il emploie les polices coréennes Batang et KPCheongPong. Ce choix de polices corrobore de précédentes preuves communiquées par d'autres sources et qui pointaient du doigt la Corée du Nord, dont le nom de l'auteur et les serveurs de commande et de contrôle utilisés pour lancer l'attaque. Ensemble, ces éléments de preuve lèvent le doute sur l'origine de l'auteur de l'attaque.

4. Enregistrement DNS

Dans certains cas, les auteurs de menaces paient des frais d'enregistrement de domaines afin d'échapper à la détection des systèmes de protection standard contre les logiciels malveillants, par exemple les listes noires de domaines. Souvent, ces enregistrements DNS permettent d'identifier directement le pays d'origine du cybercriminel.

Même les enregistrements DNS comportant des adresses et des noms factices peuvent être utiles pour identifier le coupable. Dans certains cas, les auteurs d'attaques réutilisent les fausses informations de contact pour l'enregistrement de plusieurs domaines. Grâce à ces informations récurrentes, les chercheurs peuvent lier rapidement plusieurs attaques à un même auteur et recouper les informations recueillies sur chaque attaque.

À titre d'exemple, citons l'affaire « Sin Digoo ». Entre 2004 et 2011, une personne utilisant une adresse de messagerie Hotmail a enregistré plusieurs domaines sous le même nom. Elle donnait comme adresse physique une boîte postale dans la ville de « Sin Digoo, Californa », une variante phonétique mal orthographiée de « San Diego ». Grâce aux informations d'enregistrement récurrentes, les chercheurs ont pu associer des attaques de logiciels malveillants isolées à un réseau plus large de menaces persistantes avancées[2].

De même, Nart Villeneuve, chercheur spécialisé en logiciels malveillants, a utilisé des informations d'enregistrements DNS pour faire le rapprochement entre l'Université de Zhejiang en Chine et une attaque lancée en 2010 contre l'organisation Amnesty Hong Kong, des journalistes et des défenseurs des droits de l'homme[3].

FireEye a récemment utilisé des données d'enregistrements DNS pour établir un lien entre plusieurs échantillons de logiciels malveillants chargés sur le site Web d'analyse antivirus VirusTotal (figure 6). Le but de leur auteur était vraisemblablement de déterminer si ces échantillons étaient détectés par la communauté antivirus.

Figure 6 — Exemple de chargement d'un échantillon de logiciel malveillant.

Si la première phase, à savoir la tentative de commande et de contrôle, est masquée, la seconde, révélée uniquement par l'exécution du logiciel malveillant dans une infrastructure opérationnelle, utilise le domaine secureplanning.net (figure 7) enregistré au nom d'une personne associée à une adresse apparemment fausse de New Delhi.

```
POST /download/ad.php HTTP/1.0
Accept: text/plain, text/html
Content-Type: multipart/form-data; boundary=--------------------------
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV2)
Host: secureplanning.net
Content-Length: 4565
Pragma: no-cache
```

Figure 7 — Informations de chargement de l'échantillon de logiciel malveillant sur le site VirusTotal.

2 Joe Stewart (Dell SecureWorks). *The Sin Digoo Affair*. Février 2012.

3 Nart Villeneuve. *Nobel Peace Prize, Amnesty HK and Malware*. Novembre 2010.

Les informations d'enregistrement ne constituent pas une preuve irréfutable en soi : un pirate rusé peut générer des données de contact trompeuses pour entraîner les chercheurs sur une fausse piste. Mais, dans ce cas, les chercheurs de FireEye ont noté que des versions légèrement mutantes du logiciel malveillant ont été chargées plus de 15 fois sur le site VirusTotal. Tous les échantillons ont tenté de se connecter à des domaines enregistrés avec la même adresse de New Delhi, ce qui démontrait clairement l'existence d'une stratégie globale.

5. Langue

Souvent, de nombreux indices laissent deviner que la langue utilisée dans le cadre d'une campagne de logiciels malveillants n'est pas la langue maternelle de son auteur. Certains d'entre eux permettent même d'identifier la nationalité du pirate.

En général, des erreurs typographiques et des fautes d'orthographe flagrantes sont très révélatrices. Parfois, une analyse plus approfondie met en lumière certains signes témoignant de l'utilisation d'un site de traduction. En connaissant le traitement appliqué à certains mots et expressions sur les principaux sites de traduction, les chercheurs peuvent déterminer la langue d'origine des e-mails d'hameçonnage utilisés dans une attaque.

Prenons l'exemple de l'attaque très médiatisée lancée contre la société RSA en 2011. Deux groupes vraisemblablement à la solde d'un gouvernement ont infiltré le réseau de RSA pour extraire des données sur ses produits SecurID. L'attaque exploitait une vulnérabilité inconnue de Flash, ce qui suggère une technicité élevée. Cependant, comme l'illustre la figure 8, l'e-mail d'hameçonnage employait un mauvais anglais et une formule maladroite (quoiqu'efficace au bout du compte) pour inciter le lecteur à ouvrir la pièce jointe. Dès lors, il est possible d'en déduire que l'auteur n'était pas anglophone.

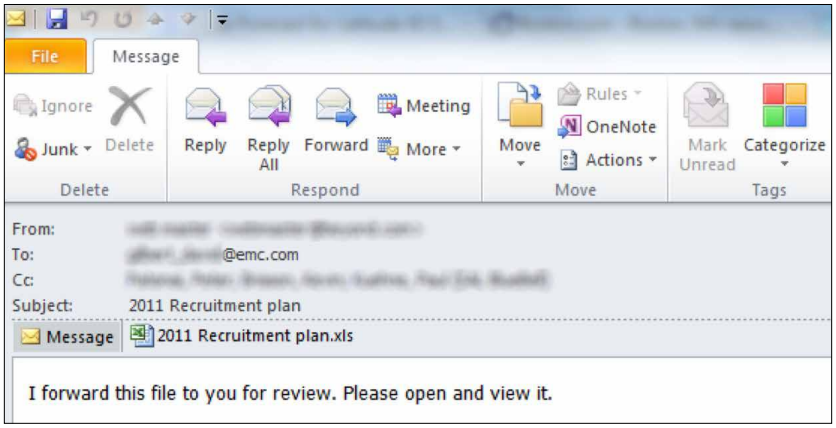


Figure 8 — E-mail d'hameçonnage utilisé dans le cadre de l'attaque contre la société RSA en 2011.

Dans d'autres cas, les langues incorporées dans le logiciel malveillant peuvent aider à identifier les pirates. Dans la figure 9, un extrait de code du logiciel malveillant Backdoor.LV utilise la langue et des noms arabes pour « marquer » les cibles.

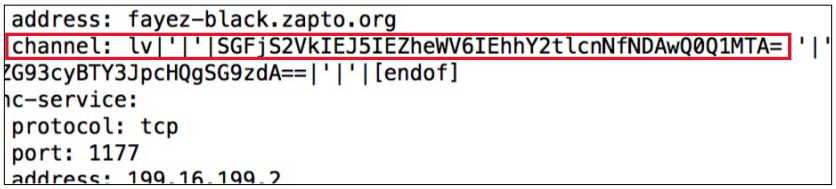


Figure 9 — Extrait du code du logiciel malveillant Backdoor.LV. Une fois décodée, la partie du code mise en évidence devient la chaîne illustrée dans la figure 10.

Cette chaîne de caractères, une fois décodée, devient « HacKed By Fayez Hacker_400CD510 » (Piraté par Fayez Hacker_400CD510), comme le montre la figure 10.

Figure 10 — Backdoor.LV décodé.

Le code indiqué à la figure 11 semble émaner du même pirate. La chaîne de caractères décodée montre la balise « 400CD510 » (figure 12), cette fois en alphabet arabe.

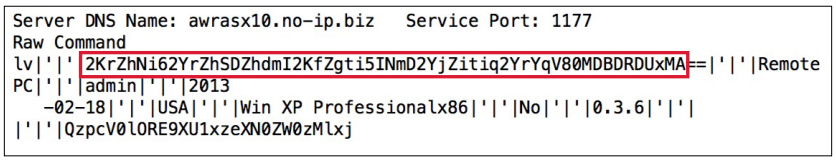


Figure 11 — Autre extrait du code de logiciel malveillant associé à Fayez. Une fois décodée, la partie du code mise en évidence devient la chaîne illustrée dans la figure 12.

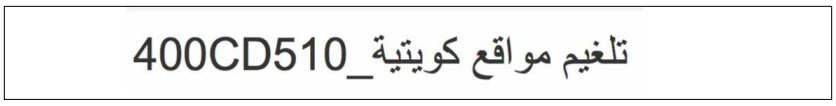


Figure 12 — Référence 400CD510, avec chaîne en alphabet arabe.

6. Configuration des outils d'administration à distance

Les outils d'administration à distance appartiennent à une classe de logiciels malveillants conçus pour offrir au pirate un contrôle en temps réel sur l'ordinateur d'une cible. Ces outils prennent en charge un large éventail de fonctions, notamment l'enregistrement de la frappe, la capture d'écran, la capture vidéo, les transferts de fichiers, l'administration du système et l'accès au shell de commandes. Gratuits ou payants, ils sont disponibles publiquement et très appréciés des cybercriminels car ils sont généralement bien testés et proposent des fonctionnalités très complètes.

De premier abord, on pourrait croire que les outils d'administration à distance compliquent l'identification d'un auteur de logiciels malveillants puisqu'ils sont accessibles à tous et employés par de nombreux groupes différents. Toutefois, leurs nombreuses options de personnalisation créent une combinaison de paramètres de configuration propre à chaque pirate. Lorsque plusieurs attaques ont recours à un outil d'administration à distance configuré de la même façon, elles permettent de désigner un même auteur.

Prenons l'exemple de Poison Ivy, un outil qui existe depuis huit ans déjà et très populaire au sein de la communauté cybercriminelle. Certaines options, et tout particulièrement l'ID, le groupe, le mot de passe et le mutex, offrent des indications précieuses sur son utilisateur.

La figure 13 illustre les champs d'ID et de mot de passe de la fenêtre de configuration de la connexion de Poison Ivy.
La figure 14 montre, quant à elle, le champ relatif au mutex dans la fenêtre de configuration avancée.

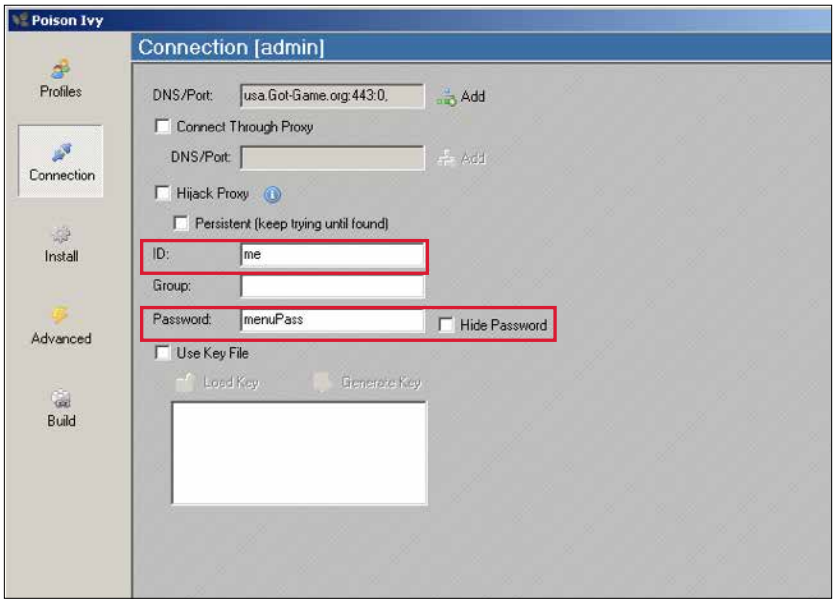


Figure 13 — Fenêtre de configuration de la connexion de Poison Ivy (avec mise en évidence des champs d'ID et de mot de passe).

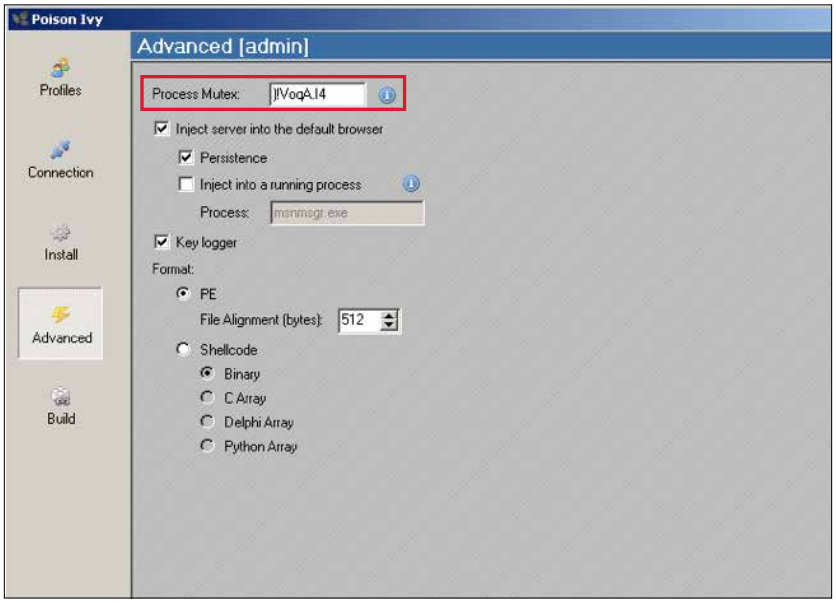


Figure 14 — Fenêtre de configuration avancée de Poison Ivy (avec mise en évidence du champ du mutex de processus).

Ces options de configuration peuvent être extraites des outils d'administration à distance compilés à l'aide de Volatility, une plate-forme à code source libre d'investigation numérique basée sur la mémoire qui opère sur les fichiers de vidage de la mémoire.

Dans Poison Ivy, les champs de l'ID et du groupe sont configurés par le pirate pour marquer et organiser des groupes de cibles. Lorsque les mêmes ID ou noms de groupes apparaissent dans plusieurs attaques, les chercheurs peuvent en conclure que celles-ci sont liées.

Le champ du mot de passe sert de clé de chiffrement des communications de Poison Ivy. Il est configuré par défaut avec la valeur « admin » et reste souvent inchangé. Toutefois, lorsqu'un mot de passe spécifique est défini, il peut constituer une forme d'empreinte numérique puisqu'il est généralement unique et souvent réutilisé par le pirate dans le cadre de campagnes d'attaques ciblées.

En informatique, un mutex est un objet de programmation conçu pour éviter que plusieurs threads d'un programme n'utilisent les mêmes ressources en même temps. Dans Poison Ivy, le mutex sert de marqueur pour déterminer si l'outil est déjà exécuté sur un système infecté afin qu'il n'exécute pas plus d'une instance de lui-même. La valeur par défaut du mutex dans Poison Ivy est)!VoqA.I4. Au même titre que les mots de passe définis dans Poison Ivy, toute chaîne de mutex autre que la valeur par défaut est généralement unique, ce qui en fait un marqueur utile.

7. Comportement

Nous, êtres humains, avons tendance à reproduire certains comportements ou habitudes. Les auteurs de logiciels malveillants n'échappent pas à la règle, et leur comportement peut ainsi devenir prévisible au fil du temps. Ils se concentrent sur les mêmes cibles et les mêmes secteurs d'activités, et utilisent les mêmes serveurs de commande et de contrôle. Cette constance dans les tactiques peut permettre de deviner les méthodes, les objectifs et la localisation des pirates. C'est à ce niveau que le profilage des cybercriminels peut s'avérer utile. À l'instar du profilage criminel qui aide les enquêteurs à se concentrer sur des suspects potentiels, il permet aux professionnels de la sécurité d'observer les pirates sur une certaine période et d'identifier certains traits comportementaux. Grâce à ces informations, ceux-ci peuvent déceler la propension d'un groupe donné à adopter des approches et des styles particuliers.

De la même façon, les tactiques et les kits d'outils d'exploit employés par un pirate facilitent son profilage. La figure 15 illustre quatre attaques distinctes qui utilisent des exploits différents, des leurres différents et des implants de logiciels malveillants différents lors de la première phase de l'attaque. En revanche, elles ciblent toutes des militants religieux. En outre, comme le révèlent les informations d'en-tête (figure 16), les attaques sont toutes lancées à partir du même serveur — certaines par le service de messagerie Web de Yahoo! et d'autres au moyen d'un script. Ces éléments de preuve indiquent la collaboration de plusieurs auteurs appartenant à une même équipe et utilisant la même infrastructure.

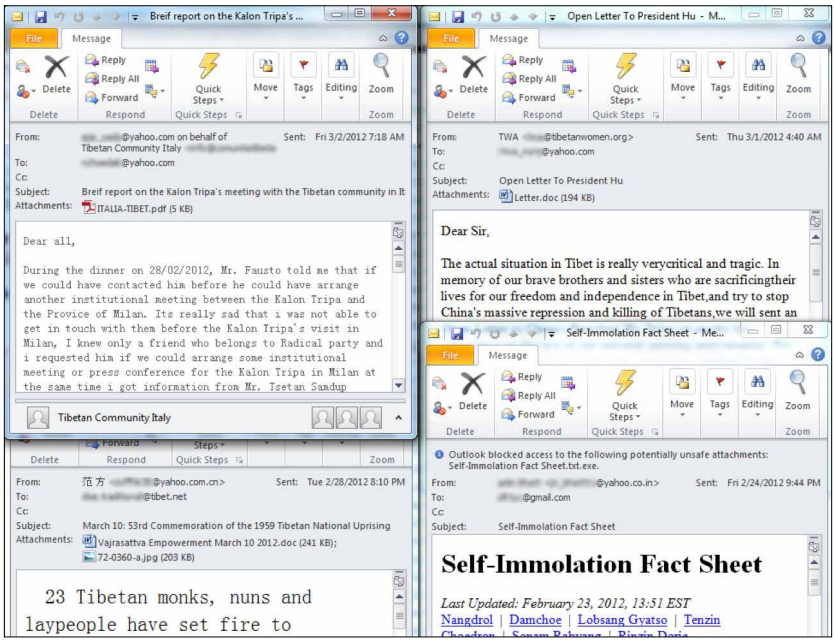


Figure 15 — Quatre e-mails d'hameçonnage.

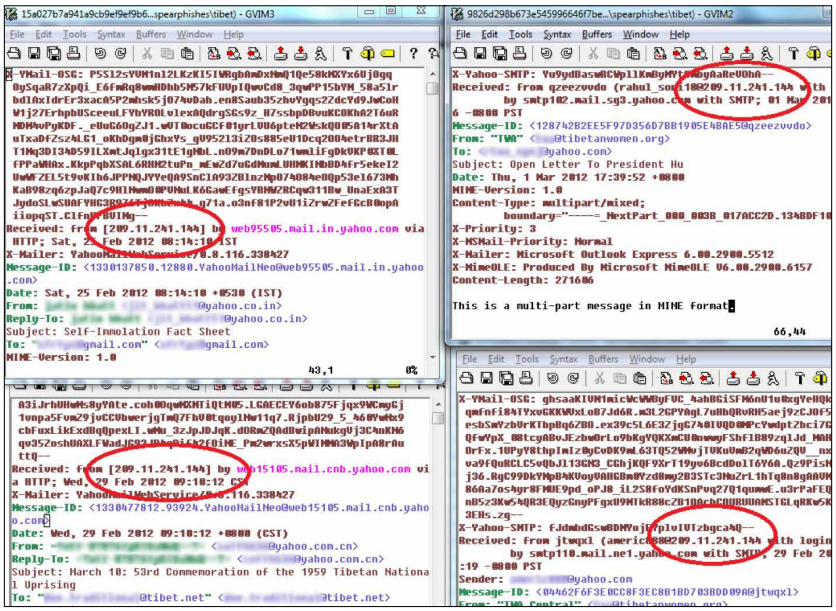


Figure 16 — Informations d'en-tête d'e-mail d'hameçonnage (avec mise en évidence des adresses IP).

Conclusion

Individuellement, aucun de ces éléments ne constitue une preuve irréfutable. En revanche, quand plusieurs indices conduisent au même auteur, les chercheurs peuvent déduire avec un degré de certitude élevé l'identité du responsable d'une attaque donnée. Grâce à ces informations, il devient plus simple d'anticiper les méthodes et les motivations de l'attaque, ce qui permet aux professionnels de la sécurité de prévoir plus efficacement les futures attaques et de protéger les données et les systèmes visés.

Comparée à certaines tâches prioritaires, par exemple limiter et réparer les dommages d'une attaque, l'identification de la source de l'attaque peut sembler accessoire. Rien n'est moins vrai. Lorsqu'une entreprise connaît les méthodes et l'objectif du cybercriminel qui l'a prise pour cible, elle est à même de prendre diverses mesures :

- Réaffecter immédiatement des ressources à la protection des données vulnérables
- Faire appel à une aide supplémentaire (ressources internes ou forces de police)
- Analyser de façon plus approfondie d'autres vecteurs parfois négligés et précédemment utilisés par le pirate dans le cadre d'autres campagnes

Connaître la source d'une attaque peut s'avérer particulièrement utile lorsque ces informations sont associées à celles recueillies sur des attaques précédentes lancées par le même auteur contre d'autres objectifs. Des solutions telles que le cloud FireEye® Dynamic Threat Intelligence™, qui partage des informations anonymisées sur les menaces avec les clients toujours plus nombreux de FireEye, fournissent des renseignements sur les tactiques, les protocoles, les ports ainsi que les canaux de rappel utilisés par les pirates informatiques.

Pour savoir comment la plate-forme de protection contre les menaces de FireEye peut vous aider à mieux vous défendre contre les cyberattaques, visitez le site de FireEye à l'adresse http://www.FireEye.com.

À propos de FireEye

FireEye® a développé une plate-forme de sécurité virtualisée et spécialisée qui offre aux entreprises et aux administrations publiques du monde entier une protection en temps réel contre la nouvelle génération de cyberattaques. Plus sophistiquées que jamais, ces cyberattaques contournent sans aucune difficulté les défenses traditionnelles basées sur les signatures, telles que les pare-feux de nouvelle génération, les solutions IPS, les logiciels antivirus et les passerelles. La plate-forme FireEye assure une protection dynamique en temps réel contre les menaces sans utiliser de signatures et met ainsi les organisations à l'abri des attaques sur les principaux vecteurs (environnement Web, messagerie électronique et fichiers) à tous les phases de leur cycle de vie. La plate-forme FireEye repose sur un moteur d'exécution virtuel et sur des informations dynamiques sur les menaces pour identifier et bloquer les cyberattaques en temps réel. FireEye compte plus de 1 000 clients dans plus de 40 pays, dont plus d'un tiers figure au classement Fortune 100.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | france@FireEye.com | www.FireEye.com