

**EDITO**  
**AGENDA**  
**ACTUALITES** P2

**L'ESSENTIEL** P3

- Les rootkits : Etat de l'art (1/2)

**ZOOM** P5

- Vulnérabilités des réseaux informatiques industriels



Directeur de la publication :  
Edouard Jeanson

Agence ESEC  
Sogeti Infrastructures Services  
6-8 rue Duret  
75016 Paris - France  
Tél : 33 (0)1 58 44 26 79

Société par Actions Simplifiées  
au capital de 15 999 790 €  
RCS Paris 479 942 583

Edition Septembre 2007



## EDITORIAL

Ça y est, le coup d'envoi est lancé ! Alors que la coupe du monde de Rugby a commencé en France, on rêve déjà d'un « 98 ». Malheureusement, nous ne sommes pas les seuls : Avec la sortie et les premiers déploiements de Windows Vista, les pirates rêvent eux aussi d'un « 98 » ... Windows 98 ! En effet, certaines attaques qui ont vu le jour sous Windows 98 ou antérieur (ex : *land attack*) et que nous étions prêts à classer dans nos archives font de nouveau leur apparition ...

Alors les rootkits ? Une technique ancienne elle aussi ? Même si ce principe est connu depuis longtemps des attaquants et des experts sécurité, aucune solution définitive n'a été trouvée à cause de l'évolution rapide des contournements utilisés. Le premier article aura donc pour objectif de faire un état de l'art de cette menace qui, aussi ancienne soit-elle, est toujours aussi dangereuse.

Ensuite, nous verrons que la sécurité de l'information sort du périmètre de nos machines voire de notre réseau puisqu'elle englobe tous les actifs de l'entreprise elle-même. Ainsi, même si cette dernière planifie au mieux la sécurité de son Système d'Information, elle maîtrise rarement ses données de bout en bout. Alors que de plus en plus souvent les dirigeants ont besoin d'avoir accès aux commandes sensibles à distance, ils créent dans le même temps des failles dans le Système d'Information. Ici, les enjeux sont tels que bien souvent, seule la victoire de l'entreprise sur l'attaquant est permise.

Alors contre les pirates, prêt à marquer l'essai de la victoire ?



## AGENDA

### **Conférence Black Hat 2007 – Tokyo (Japon), du 23 au 26 octobre 2007**

Conférences et formations sur les nouvelles techniques d'attaques issues des pirates et des laboratoires de recherche en sécurité informatique.

**Plus d'infos :** <http://www.blackhat.com>

### **Salon CARTES et Identification 2007 – Paris-Villepinte, du 13 au 15 novembre 2007**

Lors de cette nouvelle édition, de nombreux sujets seront abordés tels que : la biométrie, la sécurité de la carte SIM, les solutions pour les puces RFID, la sécurisation des paiements, la personnalisation et les valeurs ajoutées des cartes numériques, etc. ...

**Plus d'infos :** <http://www.cartes.com/fr/>

### **Salon de la sécurité informatique 2007 – Paris-La-Défense, les 21 et 22 novembre 2007**

Cette année, le congrès propose des formations et des conférences sur des sujets divers tels que :

- La sécurité de la Voix sur IP ;
- La norme ISO 27001 ;
- La sécurité SOA (Architecture Orientée Services) ;
- Business Continuity.

**Plus d'infos :** <http://www.infosecurity.com.fr>

## ACTUALITES

### Phishing : toujours une attaque de choix pour les pirates ...

Après la vague de mai où un bon nombre de banques françaises ont été ciblées par des attaques de type *phishing* et malgré les efforts de sensibilisation envers les utilisateurs, il semblerait que cette attaque fonctionne toujours aussi bien ! En effet, en un mois, le nombre d'alertes n'a pas diminué [1]. De plus, nous remarquons que les secteurs touchés sont de plus en plus diversifiés : après les banques, les sites de paiement, un fournisseur d'accès et

un site de vente en ligne entre autres. Conclusion, mieux vaut être vigilant en toute circonstance !

Mais un peu d'optimisme, des investigations sont lancées contre les pirates et ça marche ! Par exemple, la police allemande a interpellé dix personnes présumées coupables de tels délits [2]. En effet, la plupart du temps, le but de cette attaque est d'en retirer un bénéfice financier important. Or, cela

passé rarement inaperçu et c'est ainsi que les attaquants se font remarquer dans la majorité des cas.

#### Pour en savoir plus :

[1] <http://www.secuser.com/>

[2]

<http://www.vulnerabilite.com/phishing-allemande-police-arrestation-actualite-20070917205509.html>

[3] <http://www.zataz.com/dossier-zataz/phishing/32/>



### Un compagnon pas très sympa !

Il y a quelques jours, Microsoft nous annonce, via un bulletin de sécurité [1], que le compagnon d'Office, que nous côtoyons à longueur de journée pour certains, est vulnérable via son contrôle ActiveX.

Heureusement, pour les utilisateurs d'une version récente de Microsoft Office, pas de danger car cet utilitaire a disparu [2].

Mais pour les versions Windows 2000 SP4 et antérieur, le problème est bien présent. Et d'ailleurs, les pirates s'en sont donné à cœur joie puisque des codes d'attaque sont apparus en moins d'une journée ! Ainsi, les machines des personnes n'ayant pas appliqué le correctif au plus vite ont été vulnérables à une faille qui permet à l'attaquant d'exécuter du code arbitraire sur le poste cible.

#### Pour en savoir plus :

[1]

<http://www.microsoft.com/france/technet/security/bulletin/ms07-051.mspx>

[2]

<http://www.lesnouvelles.net/articles/attaques/893-vulnerabilite-agent-clippy-windows-2000.html>



### Les supermarchés discount : un nouveau vecteur de propagation ?

Les ordinateurs neufs, vierges de tout virus ? Pas si sûr ! A son insu, une chaîne de supermarchés discount a diffusé sur ses réseaux de vente allemands et danois des PCs portables ... infectés ! [1] En effet, cette chaîne, a mis en vente plusieurs dizaines de milliers de PCs ainsi compromis. Pour ajouter au côté insolite, il s'agit d'un virus vieux de pas moins de 13 ans !

Appelé « Angelina », ce virus s'attaque au secteur d'amorçage du disque dur. Mais que l'on se rassure, le code malveillant en question ne se propage que par disquette, support qui n'est quasiment plus utilisé et sans grand danger aujourd'hui. De plus, Bullguard a mis en ligne un utilitaire pour éradiquer le programme intrus [2].

#### Pour en savoir plus :

[1]

<http://www.vulnerabilite.com/medion-virus-angelina-portable-boot-allemande-actualite-20070919221531.html>

[2]

<http://www.bullguard.com/support/tech-guides/how-to-remove-stonedangelina.aspx>



### Rapport semestriel X-Force d'IBM : moins de vulnérabilités... mais de plus en plus méchantes

IBM relève de nombreux points en termes de sécurité informatique [1, 2]. Tout d'abord, son analyse, publiée le mois dernier, montre que le marché des exploits est en pleine expansion. Ceci explique que les vulnérabilités publiées sont de moins en moins nombreuses, ce qui n'était pas arrivé depuis dix ans.

Ensuite, le rapport met l'accent sur les chevaux de Troie qui sont de plus en plus utilisés par les pirates dans leur stratégie d'attaque.

Des attaques de plus en plus sophistiquées donc où les sites WEB représentent un vecteur d'attaque privilégié des attaquants. Qui plus est, les sites utilisés par les pirates sont de moins en moins sensibles aux contrôles de sécurité des navigateurs et autres.

Selon la tendance 2008 proposée par l'équipe X-Force d'IBM, nous devrions voir apparaître de moins en moins de vulnérabilités mais plus dangereuses (le nombre de vulnérabilités critiques reste

en progression) et moins de spams (grâce à l'amélioration des techniques de filtrage) mais de plus en plus de chevaux de Troie et notamment d'espionciels.

#### Pour en savoir plus :

[1] <http://www.mag-secur.com/spip.php?article9234>

[2] [http://www.iss.net/x-force\\_report\\_images/2007/](http://www.iss.net/x-force_report_images/2007/)

## L'ESSENTIEL

### Les rootkits : Etat de l'art (1/2)

Pénétrer un Système d'Information (SI) n'est pas une chose triviale à faire. Lorsqu'un attaquant prend le contrôle d'une machine, il va chercher à pérenniser cet accès et va installer généralement une backdoor qui lui permettra de revenir sur le système quand il le désire. Cette backdoor fait partie d'un *malware* (ou code malicieux) que l'on appelle *rootkit*. Ce dernier a différentes fonctionnalités qui vont permettre à l'attaquant de voler des données, d'espionner les utilisateurs ou de lancer des attaques. Cet article se compose de deux parties. Dans la première, nous décrirons le principe de fonctionnement d'un rootkit. Dans la seconde nous parlerons de quelques techniques utilisées par les rootkits.

#### Introduction

Au début, les rootkits étaient techniquement très simples : ils ciblaient quasi exclusivement les serveurs UNIX et remplaçaient des binaires ciblés du système (*ps*, *netstat*, *ls* etc.) par des versions modifiées permettant ainsi à l'attaquant de masquer son attaque et sa présence. Cette démarche a rapidement montré ses limites, l'administrateur ayant à sa disposition de nombreux moyens pour détecter si la machine a été corrompue ou non. Du coup, le terrain de jeu s'est déplacé et les rootkits ont pénétré au cœur du Système d'Exploitation (OS). En utilisant les fonctionnalités de l'OS, ils peuvent se dissimuler et espionner de manière très efficace. Le jeu du chat et de la souris a continué et les outils de détection se sont encore améliorés. Le combat est livré plus profondément dans le système en utilisant les fonctionnalités du matériel (firmwares, fonctionnalités de virtualisation des processeurs, etc.).

Les malwares sont des logiciels conçus pour infecter ou détruire un système informatique. Classiquement les malwares sont répartis en deux familles :

- Les **codes auto-reproducteurs** comme les virus et les vers capables de dupliquer leur code ;
- Les **infections** comme les bombes logiques et les chevaux de Troie incapables de se répliquer.

Comme nous pouvons le voir, les rootkits ne rentrent pas dans ces deux catégories. En effet, ils peuvent avoir des caractéristiques communes à ces deux familles. Joanna Rutkowska [1] a proposé une taxonomie des rootkits en trois catégories :

- Ceux qui effectuent une corruption du code ;
- Ceux qui effectuent une corruption des données ;
- Ceux qui agissent au delà de l'OS.

Cette taxonomie se base en fait sur la capacité de furtivité du rootkit. Ce dernier permet à un attaquant de maintenir dans le temps un accès illégitime à un SI. Il combine pour cela des caractéristiques empruntées à d'autres

types de malwares (virus, bombes logiques, chevaux de Troie, etc.). Cependant, à la différence des vers ou des virus, il ne se réplique pas. Sa caractéristique principale est la furtivité : il essaie de se cacher au cœur du système pour ne pas être détecté.

#### Architecture

Un rootkit se compose de plusieurs éléments :

- un mécanisme d'injection (pour installer le rootkit dans le système) ;
- un mécanisme de protection en deux parties :
  - une dédiée à la furtivité ;
  - une dédiée à la résistance.
- un mécanisme de contrôle, ou encore *backdoor* (pour avoir la main mise sur le système) ;
- un mécanisme d'attaque actif (DoS, scans, etc.) ou passif (keylogger, vol d'informations, etc.) permettant à l'intrus de collecter des informations ou de lancer des attaques ;
- un mécanisme de communication (pour lancer des instructions, récupérer les résultats, etc.). Ce dispositif peut prendre la forme de canaux cachés afin de renforcer la furtivité.

La question qui se pose maintenant est : comment les rootkits s'injectent-ils dans l'OS ? Et comment se dissimulent-ils ?

#### Hooking

Le hooking (ou "crochetage") est une technique qui consiste à détourner le flux d'exécution du programme pour le faire passer par ses propres fonctions. Il permet de réaliser une sorte de "*Man-in-the-middle*" avec les fonctions utilisées par le processus. On peut le réaliser en étant en espace utilisateur ou en espace noyau.

#### Espace utilisateur

Le principe de base consiste à trouver un moyen pour injecter le rootkit dans le code du processus. Il existe plusieurs méthodes pour cela [2]. Ensuite, nous pouvons « hooker » les fonctions du processus et ainsi espionner ou dissimuler des données à l'application.

Une manière de faire est de modifier l'IAT (*Import Address Table*) de l'exécutable. Lorsque ce dernier est chargé en mémoire, le *loader* résout les adresses des fonctions importées. Si le rootkit remplace ces adresses par les siennes, il peut intercepter n'importe quel appel des fonctions en question.

#### Espace noyau

Bien que les rootkits noyau soient beaucoup plus puissants que les rootkits utilisateurs, ils ne sont pas plus répandus. Ils sont beaucoup plus difficiles à programmer et ont une compatibilité plus faible du fait de leur lien plus fort avec le noyau.

#### Filtres de périphériques

Windows utilise pour ses pilotes un framework relativement complexe appelé WDM (*Windows Driver Model*). Il a pour but de proposer un modèle unifié de pilotes qui permet une compatibilité binaire entre les différentes versions de Windows. Il existe plusieurs types de pilotes WDM :

- les "*function drivers*" qui sont les pilotes principaux pour un périphérique. Ils existent sous plusieurs types en particulier les "*class drivers*" et les "*miniport drivers*" ;
- les "*bus drivers*" sont les pilotes gérant les différents types de bus de la machine comme le bus PCI, USB, FireWire, etc ;
- les "*filter drivers*", quant à eux, s'intercalent entre d'autres pilotes. Ce sont, comme leur nom l'indique, des filtres pour les données.

Les *filter drivers* sont très intéressants pour les auteurs de rootkits, car leur capacité à se positionner entre 2 pilotes les rendent très utiles pour modifier la vue d'une application sur le matériel. On peut de cette manière programmer un *keylogger*, dissimuler un trafic réseau ou des fichiers sur une partition.

#### DKOM (Direct Kernel Object Modification)

Le problème avec les méthodes décrites précédemment est que les modifications



apportées par le rootkit reposent sur des données statiques. C'est-à-dire qu'elles ne sont pas censées être modifiées et donc, il est relativement aisé de détecter des changements. La suite logique demandera donc de modifier directement des objets censés être transformés en permanence. Pour cela, la technique adéquate est DKOM.

On peut de cette manière modifier directement les structures du noyau comme par exemple les listes des threads, des pilotes, des services, ... et ainsi faire disparaître un processus ou une connexion réseau tout en étant très difficile à démasquer. Cependant cette méthode n'est pas très robuste. Les objets utilisés par le noyau ne sont pas forcément identiques entre chaque version de Windows. Elle demande beaucoup de temps et de travail à réaliser. Aussi, on ne peut modifier que ce qui est présent en mémoire : par exemple, il n'est pas possible de dissimuler un fichier alors que l'on peut masquer un processus.

## Détection

### Intégrité

Etant donné que les premiers rootkits modifiaient les binaires sur le disque dur, la première parade implémentée par les détecteurs de rootkits fut de développer des contrôleurs d'intégrité. Pour cela, il existe des outils utilisant des sommes de contrôle effectuées sur des binaires sains, pour détecter des modifications. Il suffit ensuite d'examiner les fichiers modifiés pour détecter si une intrusion a eu lieu. Bien que cette méthode fut très efficace sur les premiers rootkits, elle a perdu de cette efficacité contre les rootkits résidents en mémoire, et n'utilisant pas le disque dur.

Cependant des outils sont apparus, combinant une détection basée sur l'intégrité avec une heuristique statistique. Par exemple, prenons un flux d'exécution des binaires à analyser, comparons le, avec des méthodes statistiques au flux d'exécution de binaires sains. Si un rootkit détourne le flux d'exécution, des modifications vont

apparaître et permettre de détecter que quelque chose modifie le flux d'exécution "normal". Un autre principe est de comparer le code des binaires sur le disque dur à celui présent en mémoire. Si un rootkit a modifié un binaire dans la mémoire, on détectera une différence. Néanmoins, ces outils deviennent inefficaces face à des rootkits utilisant des techniques comme DKOM car ils ne vérifient que les modifications sur le code alors que DKOM va jusqu'à modifier les données.

### Signatures

Méthode relativement inefficace contre les rootkits. En effet, ils peuvent désactiver le logiciel de protection avant de s'installer. Si le logiciel est lancé après le rootkit, celui-ci peut très bien cacher ses données et échapper à la détection. Cependant, la détection par signature donne de bons résultats pour trouver les rootkits dans la mémoire. En effet les rootkits actuels utilisent très rarement des techniques pour échapper aux signatures (ex : chiffrement et polymorphisme). Bien sûr, cela suppose qu'une signature du rootkit recherché existe...

### Détection des hooks

Les hooks peuvent être détectés grâce à la SSDT (*System Service Dispatch Table*). La méthode consiste à comparer chaque entrée de la SSDT avec la SSDT présente dans ntoskrnl.exe (processus lancé au démarrage de Windows) Les différences indiquent les hooks.

Pour détecter les hooks utilisant les IRP (*I/O Request Packets*) des pilotes de périphériques, on peut regarder si les fonctions chargées de gérer les IRP ont leur adresse dans l'espace d'adressage du pilote. Si ce n'est pas le cas, cela indique un hook.

Les hooks effectués en mode utilisateur sont plus facilement détectables que ceux effectués en mode noyau. On peut vérifier que les adresses dans l'IAT pointe bien dans l'espace d'adressage de la bibliothèque. Une méthode simple pour trouver les fonctions patchées est de regarder si les premières instructions

sont un saut. La solution idéale serait de scanner toute la fonction pour détecter les sauts au delà du code de l'application ou de la bibliothèque, mais cela n'est pas évident à réaliser. VICE (*Virtual Intruder Capture Engine*) écrit par Jamie Butler, est un outil qui permet de détecter les hooks. Trouver des hooks ne signifie pas forcément la présence d'un rootkit. Il existe de nombreux outils qui utilisent cette technique à des fins légitimes. Le plus difficile, lorsqu'on utilise les logiciels de détection, est donc de cerner les faux positifs.

### Comparaisons croisées

Elle consiste simplement à demander la même information de deux sources différentes et d'en comparer les résultats. Une divergence implique un probable rootkit. (ex : énumérer les fichiers sur le disque en utilisant l'API haut-niveau de Windows et avec les fonctions bas-niveau du noyau Windows). Cette technique ne va cependant pas détecter des rootkits qui utilisent DKOM car les données qui se situent derrière sont les mêmes. Pour détecter les rootkits utilisant DKOM, il faut utiliser le fait que des structures du noyau sont référencées à plusieurs endroits. Par exemple, les processus du système sont stockés dans une liste doublement chaînée. Il est donc possible pour un rootkit d'enlever un processus de cette liste ce qui aura pour effet de dissimuler le processus. Cependant il existe une autre liste doublement chaînée qui indique les *handles* ouverts sur le système, et ces *handles* détiennent une référence vers les processus les contenant. En parcourant cette liste, on obtient une liste des processus peut-être différente de la première. Si le rootkit ne s'est pas dissimulé dans les deux listes, il sera détecté.

Il existe plusieurs outils qui combinent toutes les méthodes de détection de rootkits. On peut citer par exemple BlackLight de F-Secure, IceSword, Gmer ou RAIDE (*Rootkit Analysis Identification Elimination*) présentés à la BlackHat Europe en 2006 par Peter Silberman et Jamie Butler.

Comme nous venons de voir, les technologies utilisées par les rootkits sont diverses. Elles sont issues du bras de fer permanent entre les créateurs de rootkits et les créateurs de logiciels anti-rootkit. Nous savons maintenant qu'il peut être difficile de détecter certains rootkits qui prendraient en compte les techniques les plus pointues.

## Références :

- [1] <http://invisiblethings.org/papers/malware-taxonomy.pdf> [Taxonomie]
- [2] <http://it.rkuster.com/articles/winspy.htm> [Injection processus]
- [3] <http://www.intel.com/products/processor/manuals/index.htm> [Manuels Intel]
- [4] <http://www.f-secure.com/blacklight/> [BlackLight]
- [5] <http://mail.ustc.edu.cn/~jfan/> [IceSword]
- [6] <http://www.gmer.net/index.php> [Gmer]
- [7] [http://www.rootkit.com/vault/petersilberman/RAIDE\\_BETA\\_1.zip](http://www.rootkit.com/vault/petersilberman/RAIDE_BETA_1.zip) [RAIDE]
- [8] Rootkits: Subverting the Windows Kernel - James Butler, Greg Hoglund - 2005



## ZOOM

**V**ulnérabilités des réseaux informatiques industriels

Les réseaux informatiques industriels sont largement utilisés dans les activités de la vie économique. Pour la plupart, ces réseaux sont organisés autour de systèmes dits **SCADA**, acronyme qui signifie « **S**upervisory **C**ontrol and **D**ata **A**cquisition » et qui représente une famille de protocoles utilisés pour exploiter et administrer des équipements impliqués dans un grand nombre d'activités industrielles comme la génération et le transport d'énergie électrique, les systèmes de transport et autres infrastructures critiques que nous utilisons chaque jour.

La sécurité de ces systèmes est évidemment importante, mais qu'en est-il exactement des sécurités à mettre en place et quelles sont les menaces ? Cet article présente les challenges qui s'imposent pour assurer la sécurité de tels systèmes.

### Présentation des systèmes SCADA

Les systèmes SCADA sont utilisés par un grand nombre de processus qui nécessitent surveillance, reporting ou contrôle depuis des ordinateurs. Ces systèmes sont mis en œuvre pour gérer des infrastructures opérationnelles critiques comme la distribution d'énergie électrique, la pression dans les flux de pipelines gaziers, la surveillance et la gestion des réseaux d'eau, les systèmes de transport,.... Notre vie dépend grandement de ces infrastructures, de leur bon fonctionnement et de leur résistance en cas de problème ou de dysfonctionnement.

### Un peu d'histoire

Pour bien comprendre les vulnérabilités, menaces et challenges pesant sur les systèmes SCADA aujourd'hui, il est important de regarder leur histoire et d'examiner comment ils ont été impactés dans le temps.

À l'origine, les systèmes SCADA étaient des systèmes « stand alone », entités quasiment isolées et organisées autour de plateformes matérielles et logicielles propriétaires, assumant des fonctions bien spécifiques. Les capacités de ces systèmes étaient limitées aux seules fonctions nécessaires avec très peu de possibilités supplémentaires pour faire tourner d'autres programmes. Des protocoles de communication propriétaires ont été développés pour permettre aux données et aux informations de commande et de contrôle d'être transmises aux ordinateurs distants dans des temps bien déterminés. Ces systèmes de contrôle ont été à l'origine conçus avant l'émergence d'Internet et réalisés pour être isolés dans des environnements non connectés, donc sans fonction de sécurité comme les antivirus, les pare-feu, etc. Cela constitue un vrai challenge pour la sécurité globale des systèmes SCADA car beaucoup de ces systèmes sont encore utilisés de nos jours.

De même, les possibilités techniques des réseaux et des systèmes informatiques s'améliorant, les managers poussent sans cesse pour disposer d'une

connaissance en temps réel des processus industriels dans les sites de production. Cela conduit à interconnecter différents systèmes SCADA et d'intégrer ces réseaux au réseau *corporate*. Pour répondre au mieux aux besoins des managers, les entreprises ont également incorporé des plateformes matérielles et logicielles standard dans des réseaux SCADA. Il en résulte un mélange détonnant de plateformes anciennes et propriétaires et de systèmes standard basés sur Windows et Unix interconnectées en réseau. Ainsi la sécurité intrinsèque aux systèmes isolés et aux matériels et logiciels propriétaires n'est aujourd'hui pas évidente d'où des vulnérabilités potentielles nouvelles menaçant les systèmes SCADA.

Partant de ce constat, plusieurs challenges sont à relever pour sécuriser ces systèmes. Certains sont techniques, d'autres culturels ou politiques, mais tous sont importants et doivent être pris en compte.

### Challenge technique

Les défis techniques principaux ont trait aux limitations de ce qui peut être installé et configuré sur les systèmes SCADA et les limitations techniques d'autres composants dans un environnement de type SCADA. En outre, quels tests peuvent être exécutés sur ces systèmes pour détecter la présence de vulnérabilités ? Ces informations sont nécessaires pour comprendre les vrais risques de cet environnement particulier.

À la différence des réseaux d'entreprise et des systèmes classiques que nous utilisons, les systèmes SCADA ont beaucoup de difficulté pour supporter les dispositifs de sécurité de base tels que pare-feu, IDS, antivirus ou système de chiffrement. Essayer de configurer des mots de passe complexes, ou même utiliser des mots de passe est un vrai challenge dans certaines situations, en raison de l'impact que cela pourrait avoir sur la disponibilité des systèmes, voire la sécurité des personnels.

Les efforts de mise en place d'antivirus et de management de patches de sécurité, fonctions de sécurité nécessaires et fondamentales pour tout environnement informatique, exige une évaluation

soigneuse pour réduire au minimum les effets négatifs qu'ils pourraient provoquer sur la disponibilité des ressources. Puisque ces systèmes doivent fonctionner dans un environnement déterministe, tout changement pourrait ralentir leur fonctionnement, induire des délais dans les communications, ou les mettre hors ligne, toutes choses inadmissibles.

Pour compliquer encore l'affaire, beaucoup de professionnels n'ont pas encore les idées claires concernant ce qu'ils essaient de protéger sur ces réseaux. Beaucoup de systèmes SCADA sont très sensibles aux scans de vulnérabilités, il est donc risqué de les exécuter sur de tels environnements car on n'a pas une compréhension totale des conséquences provoquées. Par exemple, un simple scan, source de risque minimal sur un réseau *corporate*, peut provoquer des dégâts importants sur un réseau SCADA, causant des dysfonctionnements allant jusqu'à stopper des processus industriels critiques.

### Challenge culturel

Les défis techniques sont accentués par les différences culturelles existant entre les ingénieurs SCADA et les spécialistes IT. La convergence des réseaux SCADA et *corporate* a porté ces deux mondes sur un même sujet, chacun parlant un langage sécuritaire différent.

Pour les spécialistes IT, la sécurité a pour but de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes d'information. Dans un contexte SCADA, le but est d'assurer en premier lieu la disponibilité des systèmes, la confidentialité et l'intégrité étant considérées comme secondaires.

Les ingénieurs et SCADA doivent prendre en compte que le paradigme « la sécurité via l'obscurité » n'est plus valable. Il y a quelques années, lorsque les systèmes SCADA étaient isolés, ce raisonnement était valable mais les avancées et convergences technologiques ont définitivement changé la donne.



Où est la divergence culturelle entre les deux mondes ? Elle existe des deux côtés. D'un côté, les professionnels de l'IT doivent prendre en compte que les systèmes SCADA, bien que vulnérables dans beaucoup de secteurs, ne peuvent pas intégrer de manière simple les mesures implémentées facilement sur un réseau *corporate*. Les systèmes sont conçus différemment et les enjeux sont plus importants en cas d'indisponibilité de ces systèmes.

A l'opposé, les ingénieurs SCADA doivent comprendre qu'il existent des principes fondamentaux de sécurité qui doivent être mis en œuvre pour réduire les risques d'intrusion, d'attaque de virus, ou toute chose capable de faire tomber leurs systèmes.

Le but ultime de ces deux mondes est d'assurer la disponibilité des systèmes et ils doivent collaborer de manière entière et efficace pour définir quelle sécurité doit être mise en œuvre pour assurer le bon fonctionnement des systèmes et réduire les risques attaque.

### Challenge politique

Les défis techniques et culturels sont conséquents, mais les défis politiques sont encore d'une autre dimension. Sous la pression de contraintes business, les décisions politiques sont souvent prises sans consulter les personnes responsables de la sûreté et sécurité des systèmes SCADA. Quand de telles décisions sont prises pour acquiescer ou fusionner des entreprises, il faut prendre en compte les risques que cela implique.

Adresser ces questions après que les contrats aient été signés peut s'avérer trop tardif. Si des entités externes ont donné l'accès à vos réseaux, en particulier à vos réseaux SCADA, vous devez assumer le risque additionnel imposé par les connexions de ces nouveaux partenaires car le niveau de sécurité des deux réseaux correspond alors à celui du plus faible.

### Exemples d'incident

Selon le FBI, environ 70% des incidents de cybercriminalité, accidentel ou intentionnel, provenaient de sources internes durant la période allant 1982 à 2000. Depuis, le modèle s'inverse et beaucoup d'incidents ont lieu depuis l'externe. Pourquoi ce changement et en quoi cela affecte-t-il les réseaux SCADA ?

En fait, ce changement est partiellement dû au fait que de plus en plus de systèmes sont reliés à Internet et donc potentiellement vulnérables depuis n'importe quelle partie du monde. La prolifération des outils d'attaque fait que même un hacker novice peut représenter une menace potentielle pour tous réseaux sur la planète.

En quelques minutes, un hacker peut lancer une multitude d'attaques et mettre à genoux les réseaux d'une entreprise. Lorsque réseau *corporate* et réseau SCADA sont connectés, ces attaques peuvent affecter des composants d'architecture informatique industrielle. Ainsi des *malwares* pénétrant sur des réseaux *corporate* peuvent migrer dans des environnements SCADA et causer des dysfonctionnements importants sur ces systèmes.

Pour avoir une idée de la manière dont ces attaques peuvent survenir, regardons certaines qui se sont produites dans le passé. Ainsi, en Australie, un ex-employé parti en mauvais terme avec une entreprise prit le contrôle à distance d'un service de traitement des eaux d'égout et libéra plus de 260.000 gallons d'eaux usées dans les réseaux d'approvisionnement en eau potables, voisins.

En 2003, le vers MS SQL Slammer mis hors service un système de contrôle de sécurité dans une centrale nucléaire de production d'électricité, dans l'Ohio aux USA, pendant plus de 5 heures.

Ces types d'incident apparus dans le passé sur les systèmes SCADA prouvent que la compromission de composants critiques peut avoir de profonds effets sur l'économie d'une nation ou la sécurité de sa population. Pour ces raisons, les terroristes sont fortement intéressés pour en savoir plus sur ces systèmes de contrôle. Leur intérêt fut mis en évidence en 2001 quand les militaires américains découvrirent des documents SCADA dans des caches d'Al Qaeda en Afghanistan. John Hamre, adjoint au secrétaire à La Défense US, indiqua que des laptops d'Al Qaeda avaient servi à consulter des sites Web traitant de « programmation de systèmes de contrôle et de supervision pour des compagnies spécialisées dans la production d'énergie électrique ». Cet article insistait notamment sur l'importance pour les terroristes d'apprendre et de connaître ces systèmes SCADA contrôlant les réseaux de distribution d'eau, les barrages, les pipelines de gaz et de pétrole et les centrales nucléaires.

De nos jours, les vulnérabilités des systèmes SCADA ne sont plus un secret et les informations techniques sur leur conception sont aisément disponibles. Le déploiement de tels systèmes vulnérables dans des réseaux industriels a pour conséquence d'engendrer des risques d'attaque importants sur ces infrastructures critiques. Les barrières culturelles existant entre les mondes des ingénieurs IT et des spécialistes SCADA doivent être abaissées et des pas importants doivent être faits de chaque côté pour détecter et prévenir les attaques que les terroristes et hackers imaginent à travers des scénarii d'attaques toujours plus perfectionnés.



**Inscription à la Newsletter :** [newsletter-subscribe@esec.fr.sogeti.com](mailto:newsletter-subscribe@esec.fr.sogeti.com)  
**Désinscription :** [newsletter-unsubscribe@esec.fr.sogeti.com](mailto:newsletter-unsubscribe@esec.fr.sogeti.com)

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.

Cette Newsletter a été réalisée par les consultants sécurité de l'agence ESEC - SOGETI.