Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Our file: 117-2010-189

January 26, 2011

Dear

This refers to your *Access to Information Act* request of December 8, 2010, for **"For the period 2008 to present. Threat assessments produced by the Integrated Threat Assessment Centre relating to cyber security, cyber threats and cyber incidents including but not limited to malware, bots and other cyber attacks"**, received on December 16, 2010. A receipt for your $5.00 application fee is attached.

Enclosed please find a copy of the releasable material pertaining to the subject of your request. Portions of the material have been exempted from disclosure by virtue of sections 13(1), 15(1) (as it relates to the efforts of Canada towards detecting, preventing or suppressing subversive or hostile activities), and/or 19(1) of the *Act*.

Should you wish to obtain clarification concerning your request, please use the information at the bottom of this letter to either call or write us. Please provide the file number at the top of this letter for reference purposes.

Please be advised that you are entitled to complain to the Information Commissioner concerning the processing of your request within sixty days of the receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:
Information Commissioner of Canada
Tower "B", Place de Ville
112 Kent Street
Ottawa, Ontario
K1A 1H3

Yours truly,

Nicole Jalbert
Coordinator
Access to Information
and Privacy

Attachments

RA 2011-08-04

P.O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4
Tel: (613) 231-0107
(Ontario) K1G 4G4
1-877-995-9903
C.P. 9732, Succursale "T", Ottawa
Fax: (613)842-1271

Canada

08 / 09

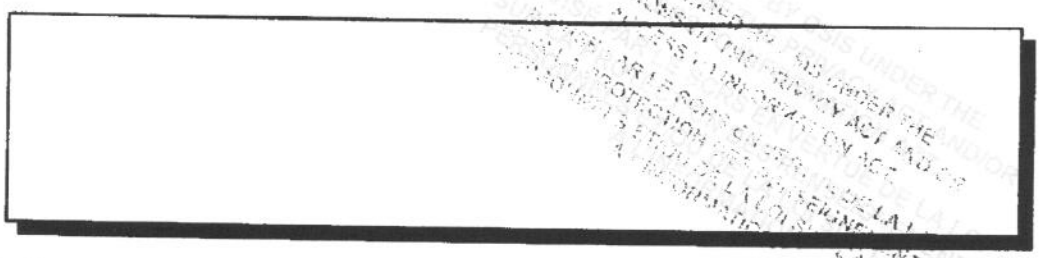
2008 02 08

CYBER TERRORISM; THREAT TO DIGITAL PROTECTION AND CONTROL EQUIPMENT

Key Points

- Digital protection and control (P&C) devices are used throughout modern critical infrastructure, including electrical power grids where they protect various high-value devices such as power lines, transformers, and generators.

contd...



Background

1. This assessment was produced at the request of the Canadian Electricity Association Security and Infrastructure Protection Committee and is the first in a series of assessments specifically addressing cyber terrorism threats.

2. ITAC has previously assessed the cyber threat to the North American power grid and supervisory control and data acquisition (SCADA) systems. Please see ITAC 07/66 for further information.

Introduction – Digital Protection and Control (P&C) Devices

3. Both digital P&C devices and SCADA systems acquire data and perform control actions. Typically, digital P&C devices automatically perform control actions based on preset conditions, while SCADA's control actions can be executed manually. Given this difference, threats to SCADA do not necessarily equate to specific threats against P&C devices.

4. Digital P&C devices are used in various industries to control processes, collect information, and monitor system status. In the electrical industry, one of the main functions of a digital P&C device is to monitor the operating state of a power distribution line or network. Digital P&C devices also protect various high-value devices that comprise many other parts of the electrical grid such as power lines, transformers, and generators. This function is integral to the continued operation of the electrical power grid.

5. As a result of the rapid advancement and popularization of Internet and intranet systems in recent years, digital and communication technologies are being employed in various industries to improve equipment performance and reduce labour costs. In order to realize these advantages, Canadian utilities are installing Internet Protocol (IP) digital protection relay devices. The risk of unauthorized remote access of these devices is dependent on each utility's network architecture and its effective use of protective measures, such as firewalls and passwords.

6. Some digital P&C devices are located in

7. In March 2007, the U.S. Department of Energy, U.S. Department of Homeland Security (DHS), and Idaho National Labs conducted a laboratory experiment dubbed "Aurora" that involved controlled hacking into a replica of a power plant's control system. Researchers, demonstrating the potential for physical damage from directed external hacking, were able to change the operating cycle of the generator, causing it to smoke and shake until if became non-functional. Industry experts claimed the experiment demonstrated the vulnerability of large electric systems in ways not previously indicated. However, DHS officials noted the difficulty associated with such an intrusion, stating that "several conditions have to be in place" in order to successfully execute an attack.

8. Digital P&C devices are installed world-wide, and basic information about these systems is available through various sources including the Internet.

The Insider Threat

10. The most serious potential threat to digital P&C devices is an insider with access to process control systems. Due to inherent knowledge, the insider would be better able to conceal his or her identity and activities.

ITAC Assessment

CYBERTERRORISME : MENACE QUI PÈSE SUR LES DISPOSITIFS NUMÉRIQUES DE PROTECTION ET DE CONTRÔLE

Faits saillants

- Les dispositifs numériques de protection et de contrôle qui sont utilisés dans l'infrastructure essentielle moderne, y compris les réseaux électriques, où ils servent à protéger les appareils de grande valeur faisant partie du réseau électrique comme les lignes électriques, les transformateurs et les génératrices.

Contexte

1. Rédigée à la demande du comité chargé de la sécurité et de la protection de l'infrastructure de l'Association canadienne de l'électricité, la présente évaluation est la première d'une série portant sur le cyberterrorisme.

2. Le CIEM a déjà évalué la cybermenace qui pèse sur le réseau électrique de l'Amérique du Nord et les systèmes d'acquisition et de contrôle des données (SCADA). Veuillez consulter le rapport du CIEM n° 07/66 pour de plus amples informations.

Introduction – Dispositifs numériques de protection et de contrôle

3. Les dispositifs numériques de protection et de contrôle et les systèmes SCADA servent à recueillir des données et à effectuer des actions de contrôle. En général, les dispositifs numériques de protection et de contrôle effectuent automatiquement les actions de contrôle en fonction de conditions préétablies tandis les actions de contrôle des systèmes SCADA peuvent être exécutées manuellement. Vu cette différence, les menaces qui pèsent sur les systèmes SCADA ne sont pas nécessairement les mêmes que celles qui planent sur les dispositifs de protection et de contrôle.

4. Les dispositifs numériques de protection et de contrôle sont utilisés dans divers secteurs industriels pour contrôler les processus, recueillir des données et surveiller l'état des systèmes. Dans l'industrie électrique, ces dispositifs servent principalement à surveiller l'état de fonctionnement des lignes ou des réseaux de transport d'électricité. Ils protègent également certains appareils de grande valeur faisant partie du réseau électrique comme les lignes électriques, les transformateurs et les génératrices. Cette fonction est indispensable pour assurer le fonctionnement, sans interruption, du réseau électrique.

5. En raison des progrès rapides et de la popularité croissante d'Internet et des systèmes intranet ces dernières années, diverses industries ont adopté des technologies numériques et de communication pour améliorer la performance de l'équipement et réduire les coûts de main-d'œuvre. Pour profiter de ces avantages, les sociétés de service public canadiennes installent des dispositifs numériques de relais de protection sur IP (protocole Internet). Les risques d'accès à distance non autorisé à ces dispositifs dépendent de l'architecture du réseau des sociétés et de l'efficacité de leurs mesures de protection comme les pare-feu et les mots de passe.

6. Certains dispositifs numériques de protection et de contrôle se trouvent

7. En mars 2007, le ministère américain de l'Énergie, le Département de la sécurité intérieure des États-Unis et les laboratoires Idaho National Labs ont effectué une expérience en laboratoire appelée « Aurora » qui portait sur le piratage contrôlé d'une réplique du système de contrôle d'une centrale électrique. Désireux de prouver les dommages matériels que peut causer le piratage externe, les chercheurs ont réussi à modifier le cycle de fonctionnement de la génératrice, la faisant surchauffer et vibrer jusqu'à ce qu'elle cesse de fonctionner. Selon les experts de l'industrie, cette expérience illustre les vulnérabilités des vastes réseaux électriques qui n'avaient jamais encore été démontrées. Les représentants du Département de la sécurité intérieure des États-Unis ont toutefois souligné les difficultés associées à une telle intrusion, affirmant que « plusieurs conditions devaient être réunies » pour qu'une telle attaque réussisse.

8. Les dispositifs numériques de protection et de contrôle sont utilisés partout dans le monde et il est facile d'obtenir des informations générales sur leur fonctionnement auprès de différentes sources, dont Internet.

Menace que représentent les initiés

10. Un initié ayant accès à des systèmes de contrôle représente la menace la plus grave pour les dispositifs numériques de protection et de contrôle et serait difficile à repérer. Les connaissances dont il dispose sur les systèmes visés lui permettraient de mener ses activités clandestinement.

Évaluation du CIEM

08 / 10

2008 02 11

CYBER TERRORISM: THREAT TO DIGITAL PROTECTION AND CONTROL EQUIPMENT

Key Points

- Digital protection and control (P&C) devices are used throughout modern critical infrastructure, including electrical power grids where they protect various high-value devices such as power lines, transformers, and generators.

Background

1. This assessment was produced at the request of the Canadian Electricity Association Security and Infrastructure Protection Committee and is the first in a series of assessments specifically addressing cyber terrorism threats.

Introduction – Digital Protection and Control (P&C) Devices

2. Both digital P&C devices and SCADA systems acquire data and perform control actions. Typically, digital P&C devices automatically perform control actions based on preset conditions, while SCADA's control actions can be executed manually. Given this difference, threats to SCADA do not necessarily equate to specific threats against P&C devices.

3. Digital P&C devices are used in various industries to control processes, collect information, and monitor system status. In the electrical industry, one of the main functions of a digital P&C device is to monitor the operating state of a power distribution line or network. Digital P&C devices also protect various high-value devices that comprise many other parts of the electrical grid such as power lines, transformers, and generators. This function is integral to the continued operation of the electrical power grid.

4. As a result of the rapid advancement and popularization of Internet and intranet systems in recent years, digital and communication technologies are being employed in various industries to improve equipment performance and reduce labour costs. In order to realize these advantages, Canadian utilities are installing Internet Protocol (IP) digital protection relay devices. The risk of unauthorized remote access of these devices is dependent on each utility's network architecture and its effective use of protective measures, such as firewalls and passwords.

5. Some digital P&C devices are located in remote locations; these areas are difficult to protect, making them easier to infiltrate. Gaining physical access to these facilities could provide direct access to digital P&C devices as well as a network access point to execute a cyber attack, though external network access is not possible through the digital P&C device itself.

6. In March 2007, the U.S. Department of Energy, U.S. Department of Homeland Security (DHS), and Idaho National Labs conducted a laboratory experiment dubbed "Aurora" that involved controlled hacking into a replica of a power plant's control system. Researchers, demonstrating the potential for physical damage from directed external hacking, were able to change the operating cycle of the generator, causing it to smoke and shake until it became non-functional. Industry experts claimed the experiment demonstrated the vulnerability of large

electric systems in ways not previously indicated. However, DHS officials noted the difficulty associated with such an intrusion, stating that "several conditions have to be in place" in order to successfully execute an attack.

7. Digital P&C devices are installed world-wide, and basic information about these systems is available through various sources including the Internet.

CYBERTERRORISME : MENACE QUI PÈSE SUR LES DISPOSITIFS NUMÉRIQUES DE PROTECTION ET DE CONTRÔLE

Faits saillants

- Les dispositifs numériques de protection et de contrôle qui sont utilisés dans l'infrastructure essentielle moderne, y compris les réseaux électriques, où ils servent à protéger les appareils de grande valeur faisant partie du réseau électrique comme les lignes électriques, les transformateurs et les génératrices.

Contexte

1. Rédigée à la demande du comité chargé de la sécurité et de la protection de l'infrastructure de l'Association canadienne de l'électricité, la présente évaluation est la première d'une série portant sur le cyberterrorisme.

Introduction – Dispositifs numériques de protection et de contrôle

2. Les dispositifs numériques de protection et de contrôle et les systèmes SCADA servent à recueillir des données et à effectuer des actions de contrôle. En général, les dispositifs numériques de protection et de contrôle effectuent automatiquement les actions de contrôle en fonction de conditions préétablies tandis les actions de contrôle des systèmes SCADA peuvent être exécutées manuellement. Vu cette différence, les menaces qui pèsent sur les systèmes SCADA ne sont pas nécessairement les mêmes que celles qui planent sur les dispositifs de protection et de contrôle.

3. Les dispositifs numériques de protection et de contrôle sont utilisés dans divers secteurs industriels pour contrôler les processus, recueillir des données et surveiller l'état des systèmes. Dans l'industrie électrique, ces dispositifs servent principalement à surveiller l'état de fonctionnement des lignes ou des réseaux de transport d'électricité. Ils protègent également certains appareils de grande valeur faisant partie du réseau électrique comme les lignes électriques, les transformateurs et les génératrices. Cette fonction est indispensable pour assurer le fonctionnement, sans interruption, du réseau électrique.

4. En raison des progrès rapides et de la popularité croissante d'Internet et des systèmes intranet ces dernières années, diverses industries ont adopté des technologies numériques et de communication pour améliorer la performance de l'équipement et réduire les coûts de main-d'œuvre. Pour profiter de ces avantages, les sociétés de service public canadiennes installent des dispositifs numériques de relais de protection sur IP (protocole Internet). Les risques d'accès à distance non autorisé à ces dispositifs dépendent de l'architecture du réseau des sociétés et de l'efficacité de leurs mesures de protection comme les pare-feu et les mots de passe.

5. Certains dispositifs numériques de protection et de contrôle se trouvent dans des installations isolées. Ces endroits sont difficiles à protéger, ce qui les rend plus facile à infiltrer. Un malfaiteur qui pénétrerait dans ces installations aurait directement accès aux dispositifs numériques de protection et de contrôle et un point d'accès au réseau qui lui permettrait de mener un cyberattaque. Il est toutefois impossible d'avoir accès au réseau depuis l'extérieur, par l'intermédiaire du dispositif numérique de protection et de contrôle.

6. En mars 2007, le ministère américain de l'Énergie, le Département de la sécurité intérieure des États-Unis et les laboratoires Idaho National Labs ont effectué une expérience en laboratoire appelée « Aurora » qui portait sur le piratage contrôlé d'une réplique du système de contrôle d'une centrale électrique. Désireux de prouver les dommages matériels que peut causer le piratage externe, les chercheurs ont réussi à modifier le cycle de fonctionnement de la génératrice, la faisant surchauffer et vibrer jusqu'à ce qu'elle cesse de fonctionner. Selon les experts de l'industrie, cette expérience illustre les vulnérabilités des vastes réseaux électriques qui n'avaient jamais encore été démontrées. Les représentants du Département de la sécurité intérieure des États-Unis ont toutefois souligné les difficultés associées à une telle intrusion, affirmant que « plusieurs conditions devaient être réunies » pour qu'une telle attaque réussisse.

7. Les dispositifs numériques de protection et de contrôle sont utilisés partout dans le monde et il est facile d'obtenir des informations générales sur leur fonctionnement auprès de différentes sources, dont Internet.

INTEGRATED THREAT ASSESSMENT CENTRE | CENTRE INTEGRE D'ÉVALUATION DES MENACES

INTELLIGENCE ASSESSMENT | ÉVALUATION DE RENSEIGNEMENTS

08 / 19 2008 03 20

CYBER TERRORISM: THREAT TO CANADIAN COMMUNICATIONS INFRASTRUCTURE

- Al Qaeda (AQ) has promoted the concept of "E-Jihad",

Introduction

1. This assessment on the terrorist cyber threat to Canadian communications infrastructure is part of an ongoing series of threat assessments specifically addressing cyber terrorism.

Definitions and Background

2. Communications infrastructure forms the backbone of the modern economy and includes telecommunications (e.g. phone, fax, cable, satellites) and broadcasting systems, as well as computer hardware, software, and networks.

3. "Convergence" refers to the combination of multiple communicative technologies into one form, and requires consideration of the Canadian communications infrastructure as a whole, when examining the cyber terrorism threats. The best known form of convergence is called "triple play" convergence, referring to the digital transmission of television, Internet, and other communications data over the same medium via Internet Protocol (IP). Beyond triple play convergence, "transparent" convergence addresses the movement of communications and control systems to IP from formerly proprietary and stand-alone networks. Convergence has been ongoing since the late 1990s and reached mass-market proportions as of 2005.

4. Canada's national critical infrastructure and emergency response is dependent upon the integrity of communications systems. For example, in the financial sector, the availability of communications infrastructure is essential to electronic transactions, the operation of domestic and world markets, and other business processes.

5. For the purposes of this assessment, cyber terrorism is defined as a computer-generated attack against other computers or computer-controlled systems via a communications network. This can include the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructures. Examples of cyber terrorism include computer hacking, introducing viruses to vulnerable networks, web site defacing, denial of service (DoS), and distributed denial of service (DDoS) attacks.

6. A DoS attack is an attempt by a malicious user, process, or system to prevent legitimate users from accessing a resource (usually a network service) by exploiting a weakness or design limitation in an information system. Examples of DoS attacks include flooding network connections, filling disk storage, disabling ports, or removing power.

7. A "botnet" or robot network is the name given to a large number of compromised computers that are used to create and send spam, viruses, or flood a network with messages during a DDoS attack. Generally, a computer is compromised by malicious software (malware) and then remotely controlled by the person administering the botnet.

8. Cyber attacks often take the form of DDoS attacks, which are designed to degrade or terminate the operation of a network by flooding it with useless traffic originating from multiple compromised systems. This is different from a DoS attack, in which a single host or compromised computer is used to mount the attack.

9. Although cyber attacks have caused billions of dollars in damage and affected the lives of millions, few if any can be characterized as acts of terrorism. Instead, most cyber attacks tend to be acts of fraud, theft, sabotage, vandalism, and extortion.

Recent Cyber Attacks Against Communications Infrastructure

10. It is generally accepted that nearly all internet sites and associated information infrastructures are under constant cyber probes and attacks.

11. The recent "cyber war" between Estonia and Russia is perhaps the best-known example of a major cyber attack. The event that sparked the conflict was the relocation of a statue commemorating Soviet war dead in the Estonian capital Tallinn. The cyber attacks, began on 2007 04 27 within hours of the war memorial's relocation. The botnet of compromised computers used during the attack involved about 1 million computers worldwide and was used to launch a large DDoS attack. The Estonian government responded by blocking Internet traffic – first from Russia and eventually from the rest of the world. On 2007 05 09, a new wave of attacks began at midnight Moscow time, and within a day forced Estonia's largest bank to shut down online services for all customers for half an hour.

12. The May 2007 cyber attacks on Estonia illustrate the widespread impact these types of attacks can have. During these attacks, access to the electronic infrastructure of the Estonian government, including media, communications, financial institutions, and emergency services, were disrupted. The attacks also show the ease with which botnets can be repurposed for political ends. Typically, the botnets involved in the attacks would be rented by their owners for criminal purposes. However, in the case of the Estonia cyber attacks, various botnet owners allowed their networks to be used free of charge.

The Global Threat Environment

13. AQ has promoted the concept of "E-Jihad",

14.

groups such as AQ actively recruit computer-savvy individuals,

15.

16. As societies become increasingly dependent on computer networks that cross national borders, the potential damage of a cyber attack increases. The U.S. Department of Homeland Security (DHS) has warned that U.S. networks should be secured against AQ hackers.

Cyber Threat Environment in Canada

18. The Quebec provincial police recently arrested the members of a 17-person hacking network, calling the group's operations "the largest hacking scam in Canadian history." Police claim the group planted malicious software on personal, corporate, and governmental computers allowing the suspects to control tens of thousands of computers without the knowledge of their legitimate users. The majority of computers attacked by the group were in Poland, Brazil, and Mexico; however, 3,383 computers in Canada were affected. The group acted mainly for profit and did not attack Canadian communications infrastructure, but used Canadian communications infrastructure as a tool for its hacking activities.

ITAC Assessment

CYBERTERRORISME : MENACE QUI PÈSE SUR L'INFRASTRUCTURE CANADIENNE DES COMMUNICATIONS

Faits saillants

- al-Qaïda fait l'apologie du « jihad électronique »,

Introduction

1. La présente évaluation sur la cybermenace terroriste qui pèse sur l'infrastructure canadienne des communications fait partie d'une série d'évaluations portant expressément sur le cyberterrorisme.

Définitions et contexte

2. L'infrastructure des communications est la cheville ouvrière de l'économie moderne. Elle comprend les systèmes de télécommunication (p. ex., la téléphonie, la télécopie, la câblodistribution et les satellites) et de radiotélédiffusion, ainsi que le matériel, les logiciels et les réseaux informatiques.

3. La « convergence » désigne le regroupement de nombreuses technologies des communications et nous oblige à tenir compte de l'ensemble de l'infrastructure canadienne des communications dans le contexte de l'examen de la menace que représente le cyberterrorisme. La convergence dite « service triple » est la mieux connue; elle désigne l'intégration des services de télévision, d'Internet et d'autres services de communication numériques sur un seul réseau IP (protocole Internet). Il y a aussi la convergence dite « transparente », c'est-à-dire la migration de systèmes de communication et de commande vers un réseau IP à partir de réseaux exclusifs et autonomes. Le phénomène de la convergence a débuté à la fin des années 1990 et, depuis 2005, a connu une expansion commerciale fulgurante.

4. L'intégrité des systèmes de communication est d'une importance primordiale pour l'infrastructure essentielle du Canada et les mesures d'intervention d'urgence. Par exemple, dans le secteur financier, les transactions électroniques et les activités sur les marchés intérieurs et mondiaux et autres activités commerciales dépendent de la disponibilité de l'infrastructure des communications.

5. Aux fins de la présente évaluation, le cyberterrorisme désigne une attaque informatique contre des ordinateurs ou des systèmes commandés par ordinateur au moyen d'un réseau de communication. Il peut comprendre le recours à la technologie de l'information pour monter et exécuter des attaques contre des réseaux, des systèmes informatiques et des infrastructures de télécommunications. Le piratage informatique, l'introduction de virus dans des réseaux vulnérables, la défiguration de sites Web, les dénis de service et les dénis de service distribués constituent des exemples de cyberterrorisme.

6. On qualifie d'attaque par déni de service une tentative, que ce soit par un utilisateur hostile ou au moyen d'un procédé ou d'un système malveillant, pour empêcher des utilisateurs légitimes d'avoir accès à une ressource (habituellement un réseau), en exploitant les failles d'un système d'information ou une faiblesse de conception. Les attaques par déni de service peuvent prendre diverses formes : inondation de réseaux, saturation de la mémoire d'un ordinateur, désactivation de ports ou coupure de l'alimentation en électricité.

7. Un réseau de zombies est un grand réseau d'ordinateurs compromis qui sont utilisés pour créer ou envoyer du pourriel, propager des virus ou inonder un réseau de messages pendant une attaque par déni de service distribué. En règle générale, on utilise un programme malveillant (maliciel) pour compromettre un ordinateur, ce dernier pouvant ensuite être commandé à distance par la personne qui administre le réseau de zombies.

8. Les cyberattaques prennent souvent la forme d'attaques par déni de service distribué, qui visent à altérer ou à interrompre le fonctionnement d'un réseau en l'inondant de messages inutiles en provenance de nombreux systèmes compromis. Le déni de service distribué est différent du déni de service en ce que, dans ce dernier cas, un seul ordinateur hôte ou compromis est utilisé pour monter l'attaque.

9. Même si les cyberattaques commises jusqu'à maintenant ont causé des milliards de dollars en dommages et ont touché des millions de personnes, peu d'entre elles, sinon aucune, peuvent être qualifiées d'actes de terrorisme. Dans la plupart des cas, il s'agit plutôt d'actes de fraude, de vol, de sabotage, de vandalisme et d'extorsion.

Cyberattaques récentes contre l'infrastructure des communications

10. Il est généralement reconnu que presque tous les sites Internet et infrastructures d'information connexes sont la cible constante de tentatives d'exploration et d'attaques.

11. La récente « cyberguerre » entre l'Estonie et la Russie constitue peut-être l'exemple le mieux connu d'une importante cyberattaque. Le conflit a été déclenché lorsqu'une statue commémorant les Soviétiques morts à la guerre a été déménagée dans la capitale estonienne de Tallinn. Les cyberattaques ont débuté le 2007 04 27, quelques heures seulement après le déplacement du monument en question. Le réseau de zombies utilisé pour l'attaque comptait environ un million d'ordinateurs partout dans le monde et a servi à lancer une vaste attaque par déni de service distribué. Le gouvernement estonien a réagi en bloquant le trafic Internet, d'abord en provenance de la Russie, puis du reste du monde. Le 2007 05 09, une nouvelle vague d'attaques a été lancée à minuit (heure de Moscou), laquelle a forcé, au bout

d'une journée, la plus importante banque d'Estonie à interrompre pendant une demi-heure l'accès aux services en direct pour tous ses clients.

12. Les cyberattaques perpétrées en mai 2007 contre l'Estonie illustrent les vastes retombées qu'un tel phénomène peut avoir. Au cours de ces attaques, l'accès à l'infrastructure électronique du gouvernement estonien, y compris les médias, les communications, les institutions financières et les services d'urgence, a été perturbé. Les attaques montrent également comment des réseaux de zombies peuvent facilement être adaptés en vue d'une utilisation à des fins politiques. En temps normal, les réseaux de zombies sont loués par leurs propriétaires à des fins criminelles. Toutefois, dans le cas des cyberattaques en Estonie, divers propriétaires de réseaux de zombies ont autorisé leur utilisation sans frais.

Contexte mondial de la menace

13. al-Qaïda fait l'apologie du « jihad électronique »,

14.

des groupes comme al-Qaïda recrutent activement des personnes qui s'y connaissent en informatique,

15.

16. La dépendance accrue des sociétés modernes envers des réseaux informatiques qui transcendent les frontières fait augmenter les dommages pouvant être causés par une cyberattaque. Le Département de la sécurité intérieure américain a d'ailleurs prévenu que les réseaux américains devaient être protégés contre les pirates informatiques d'al-Qaïda.

Cybermenace au Canada

18. La Sûreté du Québec a récemment arrêté les 17 membres d'un réseau de piratage et a qualifié les activités du groupe de plus importante fraude informatique de l'histoire du Canada. La police prétend que les suspects ont installé des logiciels malveillants dans les ordinateurs de personnes, d'entreprises et d'institutions gouvernementales de manière à pouvoir contrôler des dizaines de milliers d'ordinateurs à l'insu de leurs utilisateurs légitimes. La plupart des ordinateurs se trouvaient en Pologne, au Brésil et au Mexique, mais 3 383 ordinateurs au Canada ont été touchés. Motivé surtout par l'appât du gain, le groupe n'a pas attaqué l'infrastructure canadienne des communications, mais s'est servi de cette dernière comme outil pour ses activités de piratage.

Évaluation du CIEM

INTEGRATED THREAT ASSESSMENT CENTRE | CENTRE INTEGRE D'EVALUATION DES MENACES

INTELLIGENCE ASSESSMENT | EVALUATION DE RENSEIGNEMENTS

09 / 07

2009 01 22

CYBER TERRORISM: THE EMERGENCE OF ISLAMIST EXTREMIST

Key Points

- Most cyber attacks are website defacements, denial of service (DoS) attacks, or the dissemination of malicious software such as worms or viruses. Sophisticated attacks can include the use of BotNets.

Background

1) For the purposes of this assessment, cyber terrorism is defined as a computer-generated attack against other computers or computer-controlled systems by a communications network. This can include the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructures. A list of terms is provided in the Annex.

2) Over the last decade, the Internet has become a global platform for terrorist and extremist support activities such as spreading propaganda, recruitment, training, reconnaissance, attack planning, financing, and communications.

3) In addition, the Internet provides an alternative platform to engage in terrorist attacks on-line.

Islamist Extremist Cyber Attack Capabilities

Al Qaeda-Core

4) For several years, AQ-Core has shown an intent to develop and use cyber capability in its struggle against its "infidel" and "apostate" enemies.

5) In 2002, data found on the hard drives of laptops recovered in Afghanistan indicated that AQ researched the possibility of a cyber attack against Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are used extensively for electric power, water, gas and other utility companies to monitor and manage distribution facilities.

Islamist Extremist Hacker Groups

8) There are a number of Islamist extremist hacker groups which are capable of DoS attacks and website defacements.

9) Examples of Islamist extremist hacker attacks include the following:

- In 1999 and 2000, the Pakistan Hackerz Club repeatedly defaced sites belonging to the US Air Force and the US Department of Energy. However, there was no additional disruption to the functioning of the websites.
- In 2000, pro-Palestinian hackers disrupted and defaced sites belonging to the Israeli Parliament, the Israeli Defence Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and other sites. While there were no long-term effects or physical damage, some financial transactions were temporarily disrupted.
- In 2006, thousands of Danish websites (mainly media, government, and business sites) were disabled by DoS attacks and defaced in retaliation for the publication of the Prophet Mohammed cartoons. Over a one-month period, 2,817 websites were defaced.

Types of Cyber Attacks

11) Most cyber attacks are website defacements, DoS attacks, or the dissemination of malicious software such as worms or viruses. However, more sophisticated attacks can include the use of

BotNets. A BotNet, or robot network, is the name given to a large number of compromised computers that are used in concert to create and send spam, viruses, or flood a network with messages during a distributed denial of service (DDoS) attack. Generally, computers are compromised by malicious software (malware) and then remotely controlled by the administering BotNet.

Annex

Address: There are three types of addresses in common use within the Internet: I) email address; ii) Internet Protocol (IP) address; iii) hardware (manufacture) address.

Backdoor: A means of access to a computer and or program that bypasses security mechanisms. A programmer may install a backdoor so that the program can be accessed for means of troubleshooting or other purposes, but an attacker may exploit or use a backdoor to gain unauthorized access to information or install spyware.

Botnet: A term describing a collection of software robots or 'bots' that run autonomously and automatically. The term is often associated with malicious software but can also refer to a network of computers using distributed computing software.

Denial of Service (DoS)/Distributed Denial of Service (DDoS): A DoS or DDoS attack is an attempt to make a computer resource unavailable to its intended user(s). Although targets, motives, and *modus operandi* of a DoS attack may vary, it generally consists of the concerted effort of a person or persons to temporarily or indefinitely prevent an Internet site or service to function efficiently.

Host: A computer that allows users to communicate with other host computers on a network.

Internet Protocol address: The IP address, usually represented in dotted decimal notation, is assigned to devices involved in a network.

Internet Relay Chats (IRC): A world-wide "party line" protocol that allows an individual to converse with others in real time. IRC is structured as a network of servers, each of which accepts connections from client programs (one per user).

Network: A data communications system which interconnects computer systems at various different sites.

Programming Script: A sequence of instructions carried out by another program rather than by the computer processor (which would be referred to as a compiled script).

SPAM: Unwanted instant messages or mail.

Trojan Horse: A computer program that carries within itself a means to allow the creator of the program access to the system using it. See also: Virus, Worm.

Virus: A program that replicates on computer systems by incorporating itself in other programs which are shared among computer systems. See also: Trojan Horse, Worm.

Worm: A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. See also: Trojan Horse, Virus.

CYBERTERRORISME : ÉMERGENCE DE GROUPES EXTRÉMISTES ISLAMISTES

Faits saillants

- La défiguration de sites Web, les dénis de service et la propagation de logiciels malveillants tels que des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies.

Contexte

1) Aux fins de la présente évaluation, le terme cyberterrorisme désigne une attaque informatique contre des ordinateurs ou des systèmes commandés par ordinateur menée au moyen d'un réseau de communication. Cela peut comprendre le recours à des technologies de l'information pour monter et exécuter des attaques contre des réseaux, des systèmes informatiques et des infrastructures de télécommunications. Certains termes employés dans la présente évaluation sont définis à l'annexe.

2) Depuis une dizaine d'années, Internet est devenu un outil dont se servent les terroristes et les extrémistes partout dans le monde pour mener leurs activités, c'est-à-dire pour diffuser de la propagande, faire du recrutement, donner de la formation, réaliser des opérations de reconnaissance, planifier des attaques, recueillir des fonds et communiquer.

3) Internet sert aussi à la perpétration d'attaques terroristes en ligne.

Capacité des extrémistes islamistes de perpétrer des cyberattaques

Noyau d'al-Qaïda

4) Dans le cadre de sa lutte contre ses ennemis « infidèles » et « apostats », le noyau d'al-Qaïda manifeste depuis plusieurs années son intention de se doter des moyens de perpétrer des cyberattaques.

5) En 2002, des données trouvées sur les lecteurs de disque dur d'ordinateurs portatifs récupérés en Afghanistan ont révélé qu'al-Qaïda avait envisagé de perpétrer une cyberattaque contre des systèmes d'acquisition et de contrôle des données (SCADA). Les systèmes SCADA sont utilisés sur une vaste échelle par les entreprises d'approvisionnement en électricité, en eau et en gaz et autres entreprises de services publics pour assurer la surveillance et la gestion des installations de distribution.

Groupes de pirates informatiques chez les extrémistes islamistes

8) Il existe chez les extrémistes islamistes de nombreux groupes de pirates informatiques capables de défigurer des sites Web et de perpétrer des attaques par déni de service.

9) Voici des exemples d'actes de piratage commis par des extrémistes islamistes.

- En 1999 et 2000, le Pakistan Hackerz Club a défiguré à plusieurs reprises des sites Web appartenant à l'Armée de l'air américaine et au département américain de l'Énergie. Il n'a toutefois pas réussi à perturber le fonctionnement de ces sites.

- En 2000, des pirates pro-palestiniens ont procédé à la défiguration de sites appartenant notamment au Parlement israélien, aux Forces de défense israéliennes, au ministère des Affaires étrangères, à la Banque d'Israël et à la Bourse de Tel-Aviv, et perturbé leur fonctionnement. Bien que ces actes n'aient pas eu d'effets à long terme ou causé des dommages matériels, certaines transactions financières ont été interrompues temporairement.

- En 2006, des milliers de sites Web danois (surtout les sites d'organes médiatiques, du gouvernement et d'entreprises) ont été rendus inutilisables à la suite d'attaques par déni de service et défigurés en représailles à la publication de caricatures du prophète Mahomet. En fait, sur une période d'un mois, 2 817 sites Web ont été défigurés.

Types de cyberattaques

11) La défiguration de sites Web, les dénis de service et la propagation de logiciels malveillants comme des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies. Un réseau de zombies est un grand réseau d'ordinateurs compromis qui sont utilisés pour créer ou envoyer du pourriel, propager des virus ou inonder un réseau de messages pendant une attaque par saturation. En règle générale, on utilise un logiciel malveillant (maliciel) pour compromettre un ordinateur, ce dernier pouvant ensuite être commandé à distance par la personne qui administre le réseau de zombies.

Annexe

Adresse : Trois types d'adresses sont utilisées couramment sur Internet : i) l'adresse électronique; ii) l'adresse IP; iii) l'adresse matérielle (du fabricant).

Adresse IP : Adresse, habituellement formée de nombres séparés par des points, attribuée aux appareils branchés à un réseau.

Cheval de Troie : Programme informatique doté d'un moyen de permettre au créateur d'avoir accès au système qui l'utilise. Voir aussi : virus informatique, ver informatique.

Déni de service / Attaque par saturation : Attaques qui visent à rendre une ressource informatique inaccessible à l'utilisateur autorisé. Bien que les cibles et les motifs de telles attaques et les méthodes employées puissent varier, elles visent toutes à empêcher le fonctionnement efficace d'un site ou d'un service Internet pour une période temporaire ou indéfinie.

Hôte : Ordinateur qui permet aux utilisateurs de communiquer avec d'autres ordinateurs hôtes sur un réseau.

Porte dérobée : Porte d'accès à un ordinateur ou à un programme qui permet de contourner les mécanismes de sécurité. Un programmeur peut installer une porte dérobée pour avoir accès au programme à des fins de dépannage notamment, mais un pirate peut aussi l'exploiter pour obtenir l'accès non autorisé à des informations ou pour installer un logiciel espion.

Pourriel : Messages instantanés importuns.

Réseau : Système de communication de données qui relie des systèmes informatiques se trouvant à divers endroits.

Réseau de zombies : Terme qui décrit un ensemble de robots virtuels ou « zombies » qui fonctionnent de façon autonome et automatique. Le terme est souvent associé aux logiciels malveillants, mais peut également désigner un réseau d'ordinateurs qui utilisent un logiciel d'informatique distribuée.

Script de programmation : Série d'instructions accomplies par un autre programme plutôt que par le processeur (dans ce dernier cas, on parlerait de script de compilation).

Service de bavardage Internet : Protocole mondial qui permet aux internautes de communiquer entre eux en temps réel. Il s'agit d'un réseau de serveurs, dont chacun accepte les connexions des internautes dotés d'un logiciel client approprié (un par utilisateur).

Ver informatique : Programme informatique qui se reproduit et se propage par lui-même. Les vers informatiques, par opposition aux virus, sont conçus de manière à se reproduire dans les réseaux. Voir aussi : cheval de Troie, virus informatique.

Virus informatique : Programme qui se reproduit sur des systèmes informatiques en s'introduisant dans d'autres programmes que partagent ces systèmes. Voir aussi : cheval de Troie, ver informatique.

ITAC CIEM
INTEGRATED THREAT ASSESSMENT CENTRE | CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

INTELLIGENCE ASSESSMENT | ÉVALUATION DE RENSEIGNEMENTS

09 / 17 2009 03 16

CYBER TERRORISM: THE EMERGENCE OF ISLAMIST EXTREMIST

Key Points

- Most cyber attacks are website defacements, denial of service (DoS) attacks, or the dissemination of malicious software such as worms or viruses. Sophisticated attacks can include the use of BotNets.

Background

1)
For the purposes of this assessment, cyber terrorism is defined as a computer-generated attack against other computers or computer-controlled systems by a communications network. This can include the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructures. A list of terms is provided in the Annex.

2) Over the last decade, the Internet has become a global platform for terrorist and extremist support activities such as spreading propaganda, recruitment, training, reconnaissance, attack planning, financing, and communications.

3) In addition, the Internet provides an alternative platform to engage in terrorist attacks on-line.

Islamist Extremist Cyber Attack Capabilities

Al Qaeda-Core

4) For several years, AQ-Core has shown an intent to develop and use cyber capability in its struggle against its "infidel" and "apostate" enemies.

5) In 2002, data found on the hard drives of laptops recovered in Afghanistan indicated that AQ researched the possibility of a cyber attack against Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are used extensively for electric power, water, gas and other utility companies to monitor and manage distribution facilities.

Islamist Extremist Hacker Groups

7) There are a number of Islamist extremist hacker groups which are capable of DoS attacks and website defacements.

8) Examples of Islamist extremist hacker attacks include the following:

- In 1999 and 2000, the Pakistan Hackerz Club repeatedly defaced sites belonging to the US Air Force and the US Department of Energy. However, there was no additional disruption to the functioning of the websites.

- In 2000, pro-Palestinian hackers disrupted and defaced sites belonging to the Israeli Parliament, the Israeli Defence Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and other sites. While there were no long-term effects or physical damage, some financial transactions were temporarily disrupted.

- In 2006, thousands of Danish websites (mainly media, government, and business sites) were disabled by DoS attacks and defaced in retaliation for the publication of the Prophet Mohammed cartoons. Over a one-month period, 2,817 websites were defaced.

Types of Cyber Attacks

9) Most cyber attacks are website defacements, DoS attacks, or the dissemination of malicious software such as worms or viruses. However, more sophisticated attacks can include the use of BotNets. A BotNet, or robot network, is the name given to a large number of compromised computers that are used in concert to create and send spam, viruses, or flood a network with messages during a distributed denial of service (DDoS) attack. Generally, computers are compromised by malicious software (malware) and then remotely controlled by the administering BotNet.

Annex

Address: There are three types of addresses in common use within the Internet: I) email address; ii) Internet Protocol (IP) address; iii) hardware (manufacture) address.

Backdoor: A means of access to a computer and or program that bypasses security mechanisms. A programmer may install a backdoor so that the program can be accessed for means of troubleshooting or other purposes, but an attacker may exploit or use a backdoor to gain unauthorized access to information or install spyware.

Botnet: A term describing a collection of software robots or 'bots' that run autonomously and automatically. The term is often associated with malicious software but can also refer to a network of computers using distributed computing software.

Denial of Service (DoS)/Distributed Denial of Service (DDoS): A DoS or DDoS attack is an attempt to make a computer resource unavailable to its intended user(s). Although targets, motives, and *modus operandi* of a DoS attack may vary, it generally consists of the concerted effort of a person or persons to temporarily or indefinitely prevent an Internet site or service to function efficiently.

Host: A computer that allows users to communicate with other host computers on a network.

Internet Protocol address: The IP address, usually represented in dotted decimal notation, is assigned to devices involved in a network.

Internet Relay Chats (IRC): A world-wide "party line" protocol that allows an individual to converse with others in real time. IRC is structured as a network of servers, each of which accepts connections from client programs (one per user).

Network: A data communications system which interconnects computer systems at various different sites.

Programming Script: A sequence of instructions carried out by another program rather than by the computer processor (which would be referred to as a compiled script).

SPAM: Unwanted instant messages or mail.

Trojan Horse: A computer program that carries within itself a means to allow the creator of the program access to the system using it. See also: Virus, Worm.

Virus: A program that replicates on computer systems by incorporating itself in other programs which are shared among computer systems. See also: Trojan Horse, Worm.

Worm: A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. See also: Trojan Horse, Virus.

CYBERTERRORISME : ÉMERGENCE DE GROUPES EXTRÉMISTES ISLAMISTES

Faits saillants

- La défiguration de sites Web, les dénis de service et la propagation de logiciels malveillants tels que des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies.

Contexte

1) Aux fins de la présente évaluation, le terme cyberterrorisme désigne une attaque informatique contre des ordinateurs ou des systèmes commandés par ordinateur menée au moyen d'un réseau de communication. Cela peut comprendre le recours à des technologies de l'information pour monter et exécuter des attaques contre des réseaux, des systèmes informatiques et des infrastructures de télécommunications. Certains termes employés dans la présente évaluation sont définis à l'annexe.

2) Depuis une dizaine d'années, Internet est devenu un outil dont se servent les terroristes et les extrémistes partout dans le monde pour mener leurs activités, c'est-à-dire pour diffuser de la propagande, faire du recrutement, donner de la formation, réaliser des opérations de reconnaissance, planifier des attaques, recueillir des fonds et communiquer.

3) Internet sert aussi à la perpétration d'attaques terroristes en ligne.

Capacité des extrémistes islamistes de perpétrer des cyberattaques

Noyau d'al-Qaïda

4) Dans le cadre de sa lutte contre ses ennemis « infidèles » et « apostats », le noyau d'al-Qaïda manifeste depuis plusieurs années son intention de se doter des moyens de perpétrer des cyberattaques.

5) En 2002, des données trouvées sur les lecteurs de disque dur d'ordinateurs portatifs récupérés en Afghanistan ont révélé qu'al-Qaïda avait envisagé de perpétrer une cyberattaque contre des systèmes d'acquisition et de contrôle des données (SCADA). Les systèmes SCADA sont utilisés sur une vaste échelle par les entreprises d'approvisionnement en électricité, en eau et en gaz et autres entreprises de services publics pour assurer la surveillance et la gestion des installations de distribution.

Groupes de pirates informatiques chez les extrémistes islamistes

7) Il existe chez les extrémistes islamistes de nombreux groupes de pirates informatiques capables de défigurer des sites Web et de perpétrer des attaques par déni de service.

8) Voici des exemples d'actes de piratage commis par des extrémistes islamistes.

- En 1999 et 2000, le Pakistan Hackerz Club a défiguré à plusieurs reprises des sites Web appartenant à l'Armée de l'air américaine et au département américain de l'Énergie. Il n'a toutefois pas réussi à perturber le fonctionnement de ces sites.
- En 2000, des pirates pro-palestiniens ont procédé à la défiguration de sites appartenant notamment au Parlement israélien, aux Forces de défense israéliennes, au ministère des Affaires étrangères, à la Banque d'Israël et à la Bourse de Tel-Aviv, et perturbé leur fonctionnement. Bien que ces actes n'aient pas eu d'effets à long terme ou causé des dommages matériels, certaines transactions financières ont été interrompues temporairement.
- En 2006, des milliers de sites Web danois (surtout les sites d'organes médiatiques, du gouvernement et d'entreprises) ont été rendus inutilisables à la suite d'attaques par déni de service et défigurés en représailles à la publication de caricatures du prophète Mahomet. En fait, sur une période d'un mois, 2 817 sites Web ont été défigurés.

Types de cyberattaques

9) La défiguration de sites Web, les dénis de service et la propagation de logiciels malveillants comme des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies. Un réseau de zombies est un grand réseau d'ordinateurs compromis qui sont utilisés pour créer ou envoyer du pourriel, propager des virus ou inonder un réseau de messages pendant une attaque par saturation. En règle générale, on utilise un logiciel malveillant (maliciel) pour compromettre un ordinateur, ce dernier pouvant ensuite être commandé à distance par la personne qui administre le réseau de zombies.

Annexe

Adresse : Trois types d'adresses sont utilisées couramment sur Internet : i) l'adresse électronique; ii) l'adresse IP; iii) l'adresse matérielle (du fabricant).

Adresse IP : Adresse, habituellement formée de nombres séparés par des points, attribuée aux appareils branchés à un réseau.

Cheval de Troie : Programme informatique doté d'un moyen de permettre au créateur d'avoir accès au système qui l'utilise. Voir aussi : virus informatique, ver informatique.

Déni de service / Attaque par saturation : Attaques qui visent à rendre une ressource informatique inaccessible à l'utilisateur autorisé. Bien que les cibles et les motifs de telles attaques et les méthodes employées puissent varier, elles visent toutes à empêcher le fonctionnement efficace d'un site ou d'un service Internet pour une période temporaire ou indéfinie.

Hôte : Ordinateur qui permet aux utilisateurs de communiquer avec d'autres ordinateurs hôtes sur un réseau.

Porte dérobée : Porte d'accès à un ordinateur ou à un programme qui permet de contourner les mécanismes de sécurité. Un programmeur peut installer une porte dérobée pour avoir accès au programme à des fins de dépannage notamment, mais un pirate peut aussi l'exploiter pour obtenir l'accès non autorisé à des informations ou pour installer un logiciel espion.

Pourriel : Messages instantanés importuns.

Réseau : Système de communication de données qui relie des systèmes informatiques se trouvant à divers endroits.

Réseau de zombies : Terme qui décrit un ensemble de robots virtuels ou « zombies » qui fonctionnent de façon autonome et automatique. Le terme est souvent associé aux logiciels malveillants, mais peut également désigner un réseau d'ordinateurs qui utilisent un logiciel d'informatique distribuée.

Script de programmation : Série d'instructions accomplies par un autre programme plutôt que par le processeur (dans ce dernier cas, on parlerait de script de compilation).

Service de bavardage Internet : Protocole mondial qui permet aux internautes de communiquer entre eux en temps réel. Il s'agit d'un réseau de serveurs, dont chacun accepte les connexions des internautes dotés d'un logiciel client approprié (un par utilisateur).

Ver informatique : Programme informatique qui se reproduit et se propage par lui-même. Les vers informatiques, par opposition aux virus, sont conçus de manière à se reproduire dans les réseaux. Voir aussi : cheval de Troie, virus informatique.

Virus informatique : Programme qui se reproduit sur des systèmes informatiques en s'introduisant dans d'autres programmes que partagent ces systèmes. Voir aussi : cheval de Troie, ver informatique.

INTEGRATED THREAT ASSESSMENT CENTRE | CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

INTELLIGENCE ASSESSMENT | ÉVALUATION DE RENSEIGNEMENTS

09 / 22

2009 03 26

CYBER TERRORISM: THE EMERGENCE OF ISLAMIST EXTREMIST

Key Points

- Most cyber attacks are website defacements, denial of service (DoS) attacks, or the dissemination of malicious software such as worms or viruses. Sophisticated attacks can include the use of BotNets.

Background

1) For the purposes of this assessment, cyber terrorism is defined as a computer-generated attack against other computers or computer-controlled systems by a communications network. This can include the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructures. A list of terms is provided in the Annex.

2) Over the last decade, the Internet has become a global platform for terrorist and extremist support activities such as spreading propaganda, recruitment, training, reconnaissance, attack planning, financing, and communications.

3) In addition, the Internet provides an alternative platform to engage in terrorist attacks on-line.

Islamist Extremist Cyber Attack Capabilities

Al Qaeda-Core

4) In 2002, data found on the hard drives of laptops recovered in Afghanistan indicated that AQ researched the possibility of a cyber attack against Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are used extensively for electric power, water, gas and other utility companies to monitor and manage distribution facilities.

Islamist Extremist Hacker Groups

6) Examples of Islamist extremist hacker attacks include the following:

- In 1999 and 2000, the Pakistan Hackerz Club repeatedly defaced sites belonging to the US Air Force and the US Department of Energy. However, there was no additional disruption to the functioning of the websites.

- In 2000, pro-Palestinian hackers disrupted and defaced sites belonging to the Israeli Parliament, the Israeli Defence Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and other sites. While there were no long-term effects or physical damage, some financial transactions were temporarily disrupted.

- In 2006, thousands of Danish websites (mainly media, government, and business sites) were disabled by DoS attacks and defaced in retaliation for the publication of the Prophet Mohammed cartoons. Over a one-month period, 2,817 websites were defaced.

Types of Cyber Attacks

7) Most cyber attacks are website defacements, DoS attacks, or the dissemination of malicious software such as worms or viruses. However, more sophisticated attacks can include the use of BotNets. A BotNet, or robot network, is the name given to a large number of compromised computers that are used in concert to create and send spam, viruses, or flood a network with messages during a distributed denial of service (DDoS) attack. Generally, computers are compromised by malicious software (malware) and then remotely controlled by the administering BotNet.

Annex

Address: There are three types of addresses in common use within the Internet: i) e-mail address; ii) Internet Protocol (IP) address; iii) hardware (manufacture) address.

Backdoor: A means of access to a computer and or program that bypasses security mechanisms. A programmer may install a backdoor so that the program can be accessed for means of troubleshooting or other purposes, but an attacker may exploit or use a backdoor to gain unauthorized access to information or install spyware.

Botnet: A term describing a collection of software robots or 'bots' that run autonomously and automatically. The term is often associated with malicious software but can also refer to a network of computers using distributed computing software.

Denial of Service (DoS)/Distributed Denial of Service (DDoS): A DoS or DDoS attack is an attempt to make a computer resource unavailable to its intended user(s). Although targets, motives, and *modus operandi* of a DoS attack may vary, it generally consists of the concerted effort of a person or persons to temporarily or indefinitely prevent an Internet site or service to function efficiently.

Host: A computer that allows users to communicate with other host computers on a network.

Internet Protocol address: The IP address, usually represented in dotted decimal notation, is assigned to devices involved in a network.

Internet Relay Chats (IRC): A world-wide "party line" protocol that allows an individual to converse with others in real time. IRC is structured as a network of servers, each of which accepts connections from client programs (one per user).

Network: A data communications system which interconnects computer systems at various different sites.

Programming Script: A sequence of instructions carried out by another program rather than by the computer processor (which would be referred to as a compiled script).

SPAM: Unwanted instant messages or mail.

Trojan Horse: A computer program that carries within itself a means to allow the creator of the program access to the system using it. See also: Virus, Worm.

Virus: A program that replicates on computer systems by incorporating itself in other programs which are shared among computer systems. See also: Trojan Horse, Worm.

Worm: A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. See also: Trojan Horse, Virus.

CYBERTERRORISME : ÉMERGENCE DE GROUPES EXTRÉMISTES ISLAMISTES

Faits saillants

- La défiguration de sites Web, les dénis de service et la propagation de logiciels malveillants tels que des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies.

Contexte

1) Aux fins de la présente évaluation, le terme cyberterrorisme désigne une attaque informatique contre des ordinateurs ou des systèmes commandés par ordinateur menée au moyen d'un réseau de communication. Cela peut comprendre le recours à des technologies de l'information pour monter et exécuter des attaques contre des réseaux, des systèmes informatiques et des infrastructures de télécommunications. Certains termes employés dans la présente évaluation sont définis à l'annexe.

2) Depuis une dizaine d'années, Internet est devenu un outil dont se servent les terroristes et les extrémistes partout dans le monde pour mener leurs activités, c'est-à-dire pour diffuser de la propagande, faire du recrutement, donner de la formation, réaliser des opérations de reconnaissance, planifier des attaques, recueillir des fonds et communiquer.

3) Internet sert aussi à la perpétration d'attaques terroristes en ligne.

Capacité des extrémistes islamistes de perpétrer des cyberattaques

Noyau d'al-Qaïda

4) En 2002, des données trouvées sur les lecteurs de disque dur d'ordinateurs portatifs récupérés en Afghanistan ont révélé qu'al-Qaïda avait envisagé de perpétrer une cyberattaque contre des systèmes d'acquisition et de contrôle des données (SCADA). Les systèmes SCADA sont utilisés sur une vaste échelle par les entreprises d'approvisionnement en électricité, en eau et en gaz et autres entreprises de services publics pour assurer la surveillance et la gestion des installations de distribution.

Groupes de pirates informatiques chez les extrémistes islamistes

6) Voici des exemples d'actes de piratage commis par des extrémistes islamistes.

- En 1999 et 2000, le Pakistan Hackerz Club a défiguré à plusieurs reprises des sites Web appartenant à l'Armée de l'air américaine et au département américain de l'Énergie. Il n'a toutefois pas réussi à perturber le fonctionnement de ces sites.

- En 2000, des pirates pro-palestiniens ont procédé à la défiguration de sites appartenant notamment au Parlement israélien, aux Forces de défense israéliennes, au ministère des Affaires étrangères, à la Banque d'Israël et à la Bourse de Tel-Aviv, et perturbé leur fonctionnement. Bien que ces actes n'aient pas eu d'effets à long terme ou causé des dommages matériels, certaines transactions financières ont été interrompues temporairement.

- En 2006, des milliers de sites Web danois (surtout les sites d'organes médiatiques, du gouvernement et d'entreprises) ont été rendus inutilisables à la suite d'attaques par déni de service et défigurés en représailles à la publication de caricatures du prophète Mahomet. En fait, sur une période d'un mois, 2 817 sites Web ont été défigurés.

Types de cyberattaques

7) La défiguration de sites Web, les déni de service et la propagation de logiciels malveillants comme des vers ou des virus informatiques constituent les principales techniques employées dans les cyberattaques. Dans le cas d'attaques plus sophistiquées, on peut aussi faire appel à des réseaux de zombies. Un réseau de zombies est un grand réseau d'ordinateurs compromis qui sont utilisés pour créer ou envoyer du pourriel, propager des virus ou inonder un réseau de messages pendant une attaque par saturation. En règle générale, on utilise un logiciel malveillant (maliciel) pour compromettre un ordinateur, ce dernier pouvant ensuite être commandé à distance par la personne qui administre le réseau de zombies.

Annexe

Adresse : Trois types d'adresses sont utilisées couramment sur Internet : i) l'adresse électronique; ii) l'adresse IP; iii) l'adresse matérielle (du fabricant).

Adresse IP : Adresse, habituellement formée de nombres séparés par des points, attribuée aux appareils branchés à un réseau.

Cheval de Troie : Programme informatique doté d'un moyen de permettre au créateur d'avoir accès au système qui l'utilise. Voir aussi : virus informatique, ver informatique.

Déni de service / Attaque par saturation : Attaques qui visent à rendre une ressource informatique inaccessible à l'utilisateur autorisé. Bien que les cibles et les motifs de telles attaques et les méthodes employées puissent varier, elles visent toutes à empêcher le fonctionnement efficace d'un site ou d'un service Internet pour une période temporaire ou indéfinie.

Hôte : Ordinateur qui permet aux utilisateurs de communiquer avec d'autres ordinateurs hôtes sur un réseau.

Porte dérobée : Porte d'accès à un ordinateur ou à un programme qui permet de contourner les mécanismes de sécurité. Un programmeur peut installer une porte dérobée pour avoir accès au programme à des fins de dépannage notamment, mais un pirate peut aussi l'exploiter pour obtenir l'accès non autorisé à des informations ou pour installer un logiciel espion.

Pourriel : Messages instantanés importuns.

Réseau : Système de communication de données qui relie des systèmes informatiques se trouvant à divers endroits.

Réseau de zombies : Terme qui décrit un ensemble de robots virtuels ou « zombies » qui fonctionnent de façon autonome et automatique. Le terme est souvent associé aux logiciels malveillants, mais peut également désigner un réseau d'ordinateurs qui utilisent un logiciel d'informatique distribuée.

Script de programmation : Série d'instructions accomplies par un autre programme plutôt que par le processeur (dans ce dernier cas, on parlerait de script de compilation).

Service de bavardage Internet : Protocole mondial qui permet aux internautes de communiquer entre eux en temps réel. Il s'agit d'un réseau de serveurs, dont chacun accepte les connexions des internautes dotés d'un logiciel client approprié (un par utilisateur).

Ver informatique : Programme informatique qui se reproduit et se propage par lui-même. Les vers informatiques, par opposition aux virus, sont conçus de manière à se reproduire dans les réseaux. Voir aussi : cheval de Troie, virus informatique.

Virus informatique : Programme qui se reproduit sur des systèmes informatiques en s'introduisant dans d'autres programmes que partagent ces systèmes. Voir aussi : cheval de Troie, ver informatique.

LASER

ITAC Threat Assessment / Évaluation de la menace CIEM

UNCLASSIFIED - For Official Use Only **2009 09 21**
NON-CLASSIFIÉ - Réservé à des fins officielles seulement
09/241

Unknown *Jihadi* Internet user threatens the US economy
Un internaute jihadiste inconnu menace l' économie américaine

KEY POINTS

- On 2009 09 16, a private security company in the United States (US) calling itself the TARGETED ACTIONABLE MONITORING CENTER (TAM - C) INSTITUTE OF TERRORISM RESEARCH AND RESPONSE (ITRR) issued an online alert, revealing that they have identified two recent *jihadi* communications indicating the imminent launch of an attack that will affect the US economy by targeting electronics. The subject of the communications identifies himself as "Rakan bin WILLIAMS".

- According to the SITE INTELLIGENCE GROUP (SIG), WILLIAMS, also known as "a secret soldier of al-Qaeda", is a character portrayed in GLOBAL ISLAMIC MEDIA FRONT (GIMF) publications as a Western member of AL QAEDA (AQ).

ANALYSIS

1) On 2009 09 16, a private security company in the United States (US) calling itself the TARGETED ACTIONABLE MONITORING CENTER (TAM- C) INSTITUTE OF TERRORISM RESEARCH AND RESPONSE (ITRR) issued an online alert, revealing that they have identified two recent *jihadi* communications indicating the imminent launch of an attack that will affect the US economy by targeting electronics. The subject of the communications identifies himself as "Rakan bin WILLIAMS".

2) The TAM-C alert goes on to give background information on WILLIAMS, who appears be an American convert originating from Europe. TAM-C assesses that the means of attack suggested by WILLIAMS is beyond his operational capability, and could take the form of a cyber attack by adversarial computer hackers against an US asset that can have an effect on a large portion of the population. No more information is available on the means, the target or the timing of the potential attack. However, WILLIAMS is known to have made specific reference to Arizona in previous *jihadi* communications.

3) According to the SITE INTELLIGENCE GROUP (SIG), WILLIAMS, also known as "a secret soldier of al-Qaeda", is a character portrayed in GLOBAL ISLAMIC MEDIA FRONT (GIMF) publications as a Western member of AL QAEDA (AQ). He first appeared online in November 2005 assessing the security situation in Europe and threatening new attacks to come by a group of Western converts to Islam. His latest message, dated 2009 09 11 and coming after three years of silence, is titled, "Obama, What's Up." WILLIAMS calls Obama the "grandson of Kunta Kinte," in reference to the novel, "Roots: The Saga of an American Family," written by author Alex Haley, and slavery. (

4) According to the UNITED STATES SENATE, the GIMF produces and distributes violent Islamist material designed to inform, inspire, and recruit followers into the global violent Islamist movement. GIMF tries to reach as wide an audience as possible by disseminating material in different languages and by tailoring its content to appeal to a range of nationalities, educational backgrounds, and age groups. Original content produced by GIMF may include religious, military, or ideological texts, online magazines, and videos of speeches and military operations.

6) ITAC will continue to monitor the situation and will provide updates as necessary.

FAITS SAILLANTS

- Le 2009 09 16, une entreprise de sécurité privée aux États - Unis, TARGETED ACTIONABLE MONITORING CENTER (TAM - C) de l' INSTITUTE OF TERRORISM RESEARCH AND RESPONSE (ITRR) a diffusé en ligne un avertissement dans lequel elle indiquait avoir repéré deux récentes communications jihadistes annonçant l' imminence d' une attaque contre des appareils électroniques qui aurait un impact sur L' économie des États - Unis. L' auteur des communications est un certain « Rakan bin WILLIAMS »
- Selon le SITE INTELLIGENCE GROUP (SIG), WILLIAMS, aussi appelé « un soldat secret d' al - Qaïda », est décrit dans les publications du FRONT ISLAMIQUE MONDIAL DE L' INFORMATION (FIMI) comme un membre occidental d' AL - QAÏDA.

ANALYSE

1) Le 2009 09 16, une entreprise de sécurité privée aux États - Unis, TARGETED ACTIONABLE MONITORING CENTER (TAM - C) de l' INSTITUTE OF TERRORISM

RESEARCH AND RESPONSE (ITRR) a diffusé en ligne un avertissement dans lequel elle indiquait avoir repéré deux récentes communications jihadistes annonçant l' imminence d' une attaque contre des appareils électroniques qui aurait un impact sur l' économie des États - Unis. L' auteur des communications est un certain « Rakan bin WILLIAMS ».

2) Dans son avertissement, TAM - C donne des informations générales sur WILLIAMS, qui semble être un Américain d' origine européenne converti. TAM - C croit que le type d' attaque mentionné par WILLIAMS dépasse ses moyens opérationnels et que l' attentat pourrait prendre la forme d' une cyberattaque par des pirates informatiques hostiles contre une cible américaine qui pourrait toucher une grande partie de la population. Aucune autre information n' est fournie sur les méthodes, la cible ou la date de l' attaque éventuelle, mais WILLIAMS a déjà mentionné précisément l' Arizona dans des communications jihadistes précédentes.

3) Selon le SITE INTELLIGENCE GROUP (SIG), WILLIAMS, aussi appelé « un soldat secret d' al - Qaïda », est décrit dans les publications du FRONT ISLAMIQUE MONDIAL DE L' INFORMATION (FIMI) comme un membre occidental d' AL - QAÏDA. WILLIAMS a été aperçu en ligne pour la première fois en novembre 2005, lorsqu' il a fait une évaluation de la situation sécuritaire de l' Europe et annoncé qu' un groupe d' Occidentaux convertis à l' islam allait commettre de nouvelles attaques. Dans son dernier message intitulé « Obama, What' s Up », publié le 2009 09 11 après trois ans de silence, WILLIAMS qualifie Obama de « petit - fils de Kunta Kinte », une allusion au roman *Roots: The Saga of an American Family* d' Alex Haley et à l' esclavage.

4) D' après le SÉNAT DES ÉTATS - UNIS, le FIMI produit et diffuse de la documentation islamiste à caractère violent qui vise à informer, à inspirer et à recruter des adeptes du mouvement islamiste violent mondial. Le FIMI tente de joindre le plus grand nombre de personnes possible en diffusant sa documentation dans plusieurs langues et en l' adaptant à diverses nationalités, à divers niveaux d' instruction et à divers groupes d' âge. La documentation produite par le FIMI comprend des textes religieux, militaires et idéologiques, des revues en ligne, ainsi que des discours et des opérations militaires enregistrés sur vidéo.

6) Le CIEM continue de surveiller la situation et fera le point au besoin.

LASER

ITAC Threat Assessment / Évaluation de la menace CIEM

UNCLASSIFIED - For Official Use Only **2010 10 08**
NON-CLASSIFIÉ - Réservé à des fins officielles seulement
10/177

STUXNET worm poses potential threat

Menace que pourrait faire peser le ver STUXNET

KEY POINTS

- In June 2010 the STUXNET worm was detected when a Belarusian company identified a sample obtained from an Iranian client. By 2010 09 30, Symantec, the largest maker of security software for personal computers, had reported almost 100,000 infected hosts in over a dozen different countries. The majority of hosts infected (over half of those reported) were found in Iran, in proximity to the Bushehr nuclear plant.
- The STUXNET worm is designed to reside in and potentially attack critical control systems, specifically SCADA systems. It operates only on Siemens Simatic software.
- ITAC is providing this report to its readership for awareness purposes.

ANALYSIS

1) In June 2010 the STUXNET worm was detected when a Belarusian company identified a sample obtained from an Iranian client.

2) STUXNET appears to be designed to attack Microsoft operating systems, as detailed in MS security bulletins such as MS10-046, MS10-061, MS08-067 and two privileged escalation vulnerabilities -- keyboard layout and task scheduler. STUXNET spreads over Universal Serial Bus (USB) devices and shared drives. The worm is written in C/C++ coding to spread and install *via* Microsoft Windows. After installation, it makes Internet connections to Universal Resource Locator (URL) mypremierfutbol.com and todaysfutbol.com, then searches for Supervisory Control And Data Acquisition (SCADA) system WinCC/Step 7 software. Once the software has been identified, STUXNET tests for SCADA to ensure it is a valid target. Once identified as a target, it installs itself as a rootkit (stealth) and hides within its own modified library .dll file. The worm is then capable of reprogramming the Programmable Logic Controllers (PLC) and hide any changes that may have occurred. If STUXNET cannot locate Step 7 software or identify a valid Siemens Simatic target, it does nothing but propagate.

3) STUXNET has been coded to stop propagating on 2012 06 24. By 2010 09 30, Symantec, the largest maker of security software for personal computers, had reported almost 100,000 infected hosts in over a dozen different countries. The majority of hosts infected (over half of those reported) were found in Iran. By geographically mapping the location of infected IP addresses, Symantec was able to determine that the majority of infections in Iran occurred in Bushehr, home of the Bushehr nuclear plant. This discovery led experts to allege that Iranian nuclear systems were the intended target of the STUXNET worm. Given the complexity of STUXNET's design, it is very difficult for experts to trace with certainty the worm's ultimate origins.

4) The STUXNET worm is designed to attack critical control systems, specifically SCADA systems. It only operates on Siemens Simatic software.

5) Siemens Simatic software is used extensively around the world, including in Canada, in industrial control systems.

6) ITAC is providing this report to its readership for awareness purposes.

FAITS SAILLANTS

- En juin 2010, une société bélarussienne a découvert le ver informatique STUXNET en examinant un échantillon fourni par un client iranien. Au 2010 09 30, Symantec, le premier fabriquant de logiciels de protection pour ordinateurs personnels, avait recensé près de 100 000 ordinateurs infectés par le ver dans plus d'une dizaine de pays. La majorité de ces ordinateurs (plus de la moitié) étaient situés en Iran, près de la centrale nucléaire de Bouchehr.
- Le ver STUXNET s'installe dans des systèmes de contrôle critiques, plus précisément les systèmes SCADA, et peut s'y attaquer. Il s'exécute uniquement au moyen du logiciel Siemens Simatic.
- Le présent document vous est fourni à titre informatif.

ANALYSE

1) En juin 2010, une société bélarussienne a découvert le ver informatique STUXNET en examinant un échantillon fourni par un client iranien.

2) Le ver STUXNET semble être conçu pour attaquer les systèmes d'exploitation de Microsoft, comme il est expliqué dans les bulletins sur la sécurité n^{os} MS10-046, MS10-061 et MS08-067 de Microsoft, grâce à deux vulnérabilités d'élévation de privilèges – la fonction de disposition du clavier et le planificateur de tâches. Il se propage par les clés USB et les disques partagés. Programmé en langage C/C++, le ver STUXNET *utilise* Microsoft Windows pour se répandre et s'installer. Il se connecte ensuite aux adresses URL mypremierfutbol.com et todaysfutbol.com, puis cherche le logiciel WinCC/Step 7 dans le système SCADA (Supervisory Control And Data Acquisition). Lorsqu'il trouve le logiciel, il vérifie si le système SCADA est une cible valide. Dans l'affirmative, il s'installe furtivement dans sa propre bibliothèque de liens dynamiques modifiée (fichier .dll). De là, il peut reprogrammer les automates programmables et dissimuler les changements apportés. S'il ne trouve pas de logiciel Step 7 ou de cible valide, il ne fait que se propager.

3) Le ver STUXNET est programmé pour cesse de se répandre le 2012 06 24. Au 2010 09 30, Symantec, le premier fabriquant de logiciels de protection pour ordinateurs personnels, avait recensé près de 100 000 ordinateurs infectés par le ver dans plus d'une dizaine de pays. La majorité de ces ordinateurs (plus de la moitié) étaient situés en Iran. En déterminant l'emplacement géographique de leurs adresses IP, Symantec a découvert que la plupart étaient situés à Bouchehr, en Iran, où se trouve une centrale nucléaire. Des experts en ont conclu que les attaques du ver STUXNET visaient les centrales nucléaires iraniennes. L'ingéniosité et de la complexité du ver, laquelle empêche les experts d'en retracer l'origine aisément.

4) Le ver STUXNET attaque des systèmes de contrôle critiques, plus précisément les systèmes SCADA. Il s'exécute uniquement au moyen du logiciel Siemens Simatic.

5) Le logiciel Siemens Simatic est un logiciel très courant utilisé partout dans le monde, y compris au Canada, dans les systèmes de contrôle industriels.

6) Le présent document vous est fourni à titre informatif.

LASER