Canadian Security Intelligence Service

Intelligence Assessment

TOP SECRET/

CSIS IA 2011-12/83
2011 11 21

Cyber Threats and Security: An Overview

Summary

The Canadian public and private sectors are dependent on their computer-based systems and associated network connections (including those to the Internet), which contain vulnerabilities that can be compromised by those with the necessary knowledge, tools and techniques.

Stuxnet has been described as a watershed or a tipping point in the realm of cyber. The Stuxnet worm acts as a proof-of-concept, illustrating that attacks once thought to be hypothetically possible but improbable can be mounted against a target if necessary knowledge, resources and assets are dedicated to the operation.

Cyber tools provide insiders and other threat actors with the opportunity of removing information from targeted sites while making it difficult for security and intelligence organizations to attribute such action since threat actors can be located in one legal jurisdiction and operate out of one or more elsewhere.

Even though system vulnerabilities have been exploited by a variety of threat actors, the computer/network user is the weak point in the system. Users have been the target of social engineering operations
to compromise their computer and exploit the enterprise

New cyber attack tools and techniques will be developed in efforts to compromise Canadian public- and private-sector systems.

CSIS IA 2011-12/83
2011 11 21

Head, IAB

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

Introduction

1. We live in an era where almost every tool (automobiles, smart phones and other devices) used in daily life incorporates a computer, an Internet connection and some kind of wireless communication capability. Technological innovation has been the basis of Canada's economic development, prosperity and security, especially as the Canadian economy becomes increasingly knowledge-based. A number of actors have identified this reliance on technology as a vulnerability and have sought to exploit it. stealing our industrial secrets, our personal identities, and penetrating our critical infrastructure networks, actors undermine our continued economic prosperity and peace, order and good government.

2. The Canadian public and private sectors depend on their computer-based systems and associated network connections (including those to the Internet) to conduct their day-to-day operations, and these systems and networks underpin all aspects of the national critical infrastructure (including water treatment, and hydro and nuclear power plants). Such networks

consist of four principal elements: hardware, software, the interconnection with communication and other networks, and the user. While computer-based networks provide greater functionality to daily operations within various sectors of activity, they contain vulnerabilities

3. The configuration of the devices, the default settings for their various capabilities, the speed with which they are brought to market, the bundling of functions within a single product are not necessarily created with security in mind. Even though these vulnerabilites have been exploited by a variety of threat actors
the computer/network user is the weak point in the system. In recent computer-related incidents, the user has been the target

to compromise their computer and exploit the enterprise where the person works

Vulnerabilities

4. The software and hardware that comprise computer-based networks normally possess some form of vulnerability. Many of these are known and their details can be found via the Internet. Threat actors use a variety of software applications to observe these networks for information relating to system configuration, and software and hardware components which comprise them, in order to develop the means to compromise specific systems, networks and users. Some of these efforts are automated, combining the probing – to see what systems and defences the target is running - and compromise function. While some of these efforts are opportunistic, looking for any vulnerable systems, others are more targeted, seeking to compromise the systems used by specific government departments/branches, businesses, and military and academic institutions.

5. Previously, system resources only could be used within the public or private-sector enterprise. Security was designed to protect the periphery of the enterprise to prevent access to

computer and other assets. Once these computer-based systems were networked and connected to the Internet, it became difficult to define what constituted an enterprise's periphery. Employees can conduct enterprise operations using desktops, laptops, smartphones, tablets and other handheld devices wherever they are located around the globe, and have the ability to move data from one device to another using a variety of removable media (thumb drives, discs, and in the memory of various handheld devices) and "cloud computing"2.

6. Early adopters acquire and use new products for reasons of functionality rather than with security in mind, creating new vulnerabilities within their enterprises. Threat actors no longer require direct access to a targeted system to effect a compromise. They can achieve remote access using a variety of tools and techniques. They can provide themselves with authorised access to the targeted system manipulate its operation, create backdoors into the system, use system resources to mount compromise efforts on other networks, and steal, erase or alter the information resident on or accessible via the system.

7. The system user is a weakpoint within an enterprise as he/she generally uses technology without understanding it. Their use of the technology determines the security of the enterprise, The user possesses or has access to information and the networked nature of computer-based systems makes this data more accessible to threat actors.

8. At the level of the individual user (both at home and work), they can be a target for identity theft. The private sector is a target because of its proprietary information, The public sector possesses information relating relating to political, social and economic issues, both domestically and abroad.

2 Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data.

Compromise/Exploit Tools

11. The focus of system security, stated simply, is to ensure access to the resources when required, integrity of the data available via the system, and the identity of the system's users. Threat actors use a variety of tools and techniques, which vary from the fairly simple to very complex, to compromise and exploit the systems they target. The capabilities of threat actors are defined by the extent of these resources and assets. The following outline some of the types of tools that are most noted in the media

16. Advisories issued by the UK and the US in 2005 outlined aspects of the crafting, sending, and impacts of these emails. The attack campaigns, gathered information about topics of interest to government departments and the private sector, and about employees within them. This information was used to craft the emails, target the recipient of the message, give the appearance that the originator was a person or organization known to the addressee (spoofing the sender), to have the recipient of the message open the email,

23. In October 2011, some anti-virus firms issued assessments of Duqu, a Stuxnet-like variant that uses a Word Document zero-day vulnerability to compromise systems. It has been detected in systems in France, the Netherlands, Switzerland, Ukraine, India, Iran, Sudan and Vietnam, and is suspected of compromises in Austria, Hungary, Indonesia and the UK. Duqu is a remote access Trojan that shares code with the Stuxnet malware

Some describe its infection of systems as a possible precursor of future attacks.

New Tools

24. Media reporting has raised awareness of the potential utility of research projects and presentations at hacker conferences,

In one instance, a project illustrated how an unmanned aerial vehicle (UAV) could be loaded with hardware and software that would allow the UAV to overfly and compromise/exploit wireless networks.

25. Furthermore, efforts will be made to compromise and exploit the capabilities of handheld devices such as smartphones and tablets, as more and more individuals adopt them for business and personal use. Given that these devices can contain personal and proprietary information, they will serve as a gateway into enterprises.

Choice of Tools

26. Some of the attack tools and techniques that have been observed can be fairly simple,

Timing

28. The timing of attacks seems to fall into three categories: the normal day-to-day compromise and exploitation of systems found to be vulnerable through automated or directed operations online; more directed phishing and spear-phishing attacks against specific organizations/institutions
and those associated with special social and political events, and economic activities

Special Events

29. Criminals and other threat actors have attempted to exploit systems associated with sporting events, and international expositions for personal gain

30. Demonstrations opposing some aspect of government social, economic or foreign policy are usually accompanied by some form of online activity.

Regional Conflicts/Tensions

32. Every conflict or period of political tension is usually accompanied by some form of online campaign by one group targeting the other's online resources. In some cases, one or both sides have supporters who exploit vulnerable systems to alter Web page content to display a message that seeks to rationalize a particular political position or to achieve some political goal.

37. Government officials in the UK believe computer-based systems provide new opportunities for states to engage in new arenas to target critical infrastructure and steal information from the public and private sectors.

These concerns are echoed in the US where it has been stated that the financial sector has been targeted and exploited, US officials have voiced concerns regarding the activities of hacking collectives, such as Anonymous, to exploit vulnerable Web servers, Web sites, computer networks

Challenges

49.

some enterprises may not detect such intrusions into their systems or report them to the relevant authorities because of fears of loss of confidence among clients, partners and other users of their services. There is an ongoing contest between the development of attack tools and techniques by threat actors and counter measures by system administrators and defenders.

50. While there may be a variety of technical measures, and policies and procedures to secure IT systems, the weak point remains the system user. The questions that remain are: how to link security to the adoption of new technologies, how to incite users to be more secure in the use of technology,

Conclusion

51. The cyber threats posed by threat actors affect Canada's national and economic security. This has implications for its critical infrastructure, the operation of its public and private sectors, and its domestic and international interests.

53. Cyber tools provide insiders and other threat actors with the opportunity to remove information from targeted sites

Given the nature of the Internet and the existence of "mirror sites" (copies of the sites located on servers in other parts of the world), it is difficult to remove such data once it is posted. The same is true of the hurdles associated with trying to attribute the

action when threat actors can be located in one jurisdiction and operate out of one or more elsewhere.

54. New cyber attack tools and techniques will be developed in efforts to compromise Canadian public and private-sector systems.

The cyber-related threat environment will evolve and become more complex, creating ever greater challenges for Canada within the context of national security.