Anatomy of a Breach
China + Cyber

A CASE STUDY

An Incursion Into a Canadian Company

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE

C/DIG CSCSS / DEFENCE INTELLIGENCE GROU

Case Study

Anatomy of a Breach

This case study reports on a cyber-attack on a Canadian Business, and contains supplementary analysis.

“a series of unusual incidents”

The attack information was volunteered by multiple sources. Identification data has been removed to protect the sources as well as the companies involved. This incursion is NOT public knowledge. The analysis is based on computer security analysis that has been released into that industry's trade journals and publications. It is also based on Open Source Media and unclassified government sources.

EXECUTIVE SUMMARY

In November 2011, a number of personnel from ***(Targeted Company) (location removed)*** publicly vented their frustrations with a series of unusual incidents in the company. There was a series of issues with a particular project. Some incidents centered around the company computer network, others around a crash of the company telephone network, followed by a crash of the network file server. Detailed non-technical[1] descriptions were provided by multiple sources. The descriptions and subsequent data suggests that ***(Targeted Company)*** received a targeted cyber-attack, most probably from the People's Republic of China (PRC).

OBSERVATIONS

In November 2011 a number of ***(Targeted Company)*** personnel expressed frustration over the large number of changes being made to ***(a sub-contracted project)*** being designed for ***(Contracting Company)***. As the project neared its production deadline, changes were required from Engineering and the Sales / Marketing groups. From the context, the number of changes was abnormally high. Further, some of the changes were made by the client at a late stage i project design.

During the week of November 28th – December 2nd 2011, IT personnel noticed a reduction in workstation and network performance over several days[1]. On the third day of significant computer incidents, while experiencing a dramati reduction in both workstation and network service IT personnel removed hard drives from three workstations “in order to safeguard the data on the hard drives”. The personnel operating the workstations were working on a project designing for ***(Contracting Company)***.

“attacked because of lax security”

On Thursday December 1st there was a complete failure of the ***(Targeted Company)*** telephone exchange, a VOIP[1] system which operates on the computer network[1]. On Friday December 2nd, staff was informed that the failure of the telephone system was due to ~~a~~ network cables being cut[1].

COMMENT: *Network failure was almost certainly NOT due to a cut cable. If telephone or network cables were cut, there would be no requirement to remove hard drives. Further, cut cables do not result in the described effects..*

During the week starting December 12th, a general improvement in the performance of ***(Targeted Company)'s*** computer network was observed. IT staff stated they were upgrading the operating system on Windows workstations. On Thursday December 15th the network login database crashed. Only personnel already logged into the server with programs running before the crash had any network access.

COMMENT: *In any computer network the login database is designed to be one of the most robust components. It is literally the keys to accessing the network. It is an extraordinarily unusual event for a login database to crash on its own.*

Strategic Linkage. ***(Targeted Company)*** is a sub-contractor working for ***(Contracting Company)***. ***(Contracting Company)*** has a number of contracts with PRC companies.

(Targeted Company) has not admitted to having being attacked or nor having any incursion on their network. Cyber-incursion / cyber-attack is a non-topic. Senior staff explained the loss of telephone service as a cut cable. No explanation was given for the removal of the hard drives. The ***(Targeted Company)*** computer network had been stable and reliable. No explanations were provided for the changes in network performance.

COMMENT: *This does not match previous information on **(Targeted Company)** processes, nor their internal messaging..*

ALTERNATIVE EXPLAINATIONS
(Other ECOA)

There are a number of possible alternatives to a PRC cyber-attack. They include:

A. Commercial / Industrial attack;
B. Protest group attack;
C. Random / Amateurs attack; and,
D. Other nation / other national interests.

The ***(Targeted Company)*** is not a logical target for a commercial attack. There is no significant intellectual property. Their company orientation is design and logistics support. The company makes money from its business processes. It should be noted that the attack was designed to capture documentation on ***(removed)*** being designed for, and provided to, a third party company supplying strategic resources to the PRC .

Protest groups advertise their successes. It is one method they use to raise funds and gather support. Their claims are distinctive and usually follow patterns.

ASSESSMENT: *The lack of any claim by protest organizations is therefore a significant indicator that protest groups did NOT attack the company. It is ASSESSED as HIGHLY UNLIKELY that protest groups generated the attack.*

Random attack / Amateur attacker. No attack is entirely random. There is usually focus on money personal data, intellectual property or some other attractive item. At the very least, companies are attacked because of lax security procedures. In essence, the organizations are attacked because the attacker can penetrate their security. Methodology tends to be sloppy. There also tends to be some sort of electronic graffiti to enable the hacker to demonstrate their superiority. Lastly, the favorite target of random and amateur attacks are company web sites. The ***(company name removed)*** web site was not defaced or visibly modified.

“the objective is to gain wider access”

ASSESSMENT: *It is ASSESSED that the lack of electronic graffiti combined with the focus on a specific project indicates the attack was PROBABLY NOT random or conducted by amateurs*

Other Nation / Other National Interests: Nations and major organizations do not readily invest time and money in efforts that can embarrass them – unless they have some sort of vested interest. In this case, ***(Targeted Company)*** was designing ***(removed)*** for projects near ***(geographic location removed)***. The United States had posed no significant objections to the process or the proposed business. Neither Russia nor Europe have an interest in these projects. Overall the project was not far enough along to draw attention from international interests[1].

PATTERNS IN CHINESE (PRC) Cyber-Attacks

The following pattern has been published by a variety of Internet Security companies and validated by SME in both Computer Security[1] and China[1]. The components involved are:

A. One element of the hack is traceable to the Third Directorate, People's Liberation Army;

B. There are usually several Chinese companies involved. These companies operate legitimate businesses. They will also have strong ties to some element of People's Republic of China (PRC) Strategic Policy; and,

C. The third group participating / conducting the attack will be identified as “hackers”.

COMMENT: *Given the PRC control of the Internet within China, the number of people required, the high degree of skill required, the high degree of technical co-ordination required and the costs of sustaining these attacks over time, they are not hackers in the Western sense. This is a funded, sustained, long-term effort.*

One documented methodology of PRC cyber-attacks on commercial / industrial targets is[1]:

A. E-mail from a “legitimate company” arrives at the target organization. The e-mail is targeted, meaning it is tailored for one person and appears entirely legitimate[1]. Within the e-mail is a link to a piece of “malware” (attack software). The purpose of the malware is to bypass security measures, opening the target's / victim's compute to the intruder;

B. Once the intruders have access to the target organization's computer system, the objective is t gain wider access to the target's computer network. One method to do this involves remotely generating e-mails on a compromised workstatior and sending them to other personnel inside the target organization. This e-mail will instruct them to provide passwords or provide greater access t the target network. The effort to gain broad network access will continue until the target data is identified;

C. Additional software will be installed to provide hidden access point into the target system. This provides long term access to the target system, regardless of the success or failure of the current operation;

D. Data will be copied off the target system and sent to a “Command and Control Server”. This may be a one time event, target a specific project or incident, or in some cases can be a multi-year operation designed to provide on-going intelligence; and,

E. If detected or the effort is ended, logs on the target network are wiped of any data documentin the incursion. Command and Control servers are also “wiped” to deny tracking information.

NOTE: Access points are usually left in place. This permits the attacker to re-enter the target system.

Strategic Context. A key question is: Does the PRC have a reason (from their perspective) to engage in this? To quote LCol Hagestad:

“The prime mover is the Communist Party of China (CPC). If they mandate that a particular state owned enterprise (SOE) within China needs the proprietary information OR if the resource involved is identified as a strategic requirement, then they have a vested interest in tracking the resource.”

The LCol's analysis states that the PRC would monitor its supply of strategic resources. ASSESSMENT: Given China's strategic requirements in oil, gas, natural gas, and aluminum, there is ample justification, from the PRC / CPC perspective, to ensure critical supply chains are going into place. It is ASSESSED that this company's work does constitute a link in the PRC's strategic requirements and that it is HIGHLY LIKELY that the PRC would track its progress.

ASSESSMENT

General: Given the descriptions of computer and network failures, it is ASSESSED as HIGHLY PROBABLE that ***(Targeted Company)*** received a targeted cyber-attack. Given the removal of the hard-drives of personnel working on the ***(project)***, it is ASSESSED that the attack intention was exploitation and project monitoring.

Attack Methodology:

A. Given the “unusual number of project changes”, both internally and from the contractor, it is ASSESSED as LIKELY that the intrusion commenced through e-mail;

B. Given the surge in changes and the decrease in network performance, it is estimated that the initial incursion lasted between three and seven days;

C. The removal of the hard drives is seen as an extraordinary action. This would not occur unless there was direct evidence, visible on ***(Targeted Company)*** network equipment, of an incursion in progress;

D. The crash of the ***(Targeted Company)*** telephone system is ASSESSED as attributable to high network load and POSSIBLY hacking of the file server (DNS[1]) during the incursion; and,

E. It is ASSESSED as HIGHLY LIKELY that the crash of the network file server and the login database was part of an effort to remove all traces of the incursion.

Given the descriptions before, during and after the crash of the telephone system, it is ASSESSED that the methods used in this attack are used by, and normally attributed to, hackers based in the People's Republic of China.

The following assessment is based on the business linkages published in Open Source Media that identify:

A. Resources identified by the PRC as strategic requirements;

B. State and privately owned companies operating in and on behalf of the PRC;

C. ***(Contracting Company)*** operating in the acquisition of, and sale of, resources to the PRC; and,

D. ***(Targeted Company)*** is designing and supervising the construction of ***(deleted)*** to supply these resources.

It is ASSESSED that from the PRC / CPC perspective, they have a vested interest in the planning and processes of ***(Targeted Company)***. This would include the ***(Targeted Company)*** designed infrastructure. Monitoring and tracking the company fits the tactics, techniques and procedures used by the PRC.

It is ASSESSED as HIGHLY PROBABLE the PRC will continue to monitor ***(Targeted Company)*** as a source of data on the development and delivery of strategic resources. This includes the ability to access the company computer network when the PRC desires access.

It is ASSESSED as HIGHLY PROBABLE that ***(Targeted Company)*** will:

A. Deny they were attacked;

B. Be uncooperative with any effort to query them on this incident and/or their computer security; and,

C. Deny any investigative access to their network.

One documented methodology of PRC cyber-attacks on commercial / industrial targets is[1]:

A. E-mail from a "legitimate company" arrives at the target organization. The e-mail is targeted, meaning it is tailored for one person and appears entirely legitimate[1]. Within the e-mail is a link to a piece of "malware" (attack software). The purpose of the malware is to bypass security measures, opening the target's / victim's computer to the intruder;

B. Once the intruders have access to the target organization's computer system, the objective is t gain wider access to the target's computer network. One method to do this involves remotely generating e-mails on a compromised workstatior and sending them to other personnel inside the target organization. This e-mail will instruct them to provide passwords or provide greater access t the target network. The effort to gain broad network access will continue until the target data is identified;

C. Additional software will be installed to provide hidden access point into the target system. This provides long term access to the target system, regardless of the success or failure of the current operation;

D. Data will be copied off the target system and sent to a "Command and Control Server". This may be a one time event, target a specific project or incident, or in some cases can be a multi-year operation designed to provide on-going intelligence; and,

E. If detected or the effort is ended, logs on the target network are wiped of any data documentin the incursion. Command and Control servers are also "wiped" to deny tracking information.

NOTE: Access points are usually left in place. This permits the attacker to re-enter the target system.

"permits the attacker to re-enter the target"

D. ***(Targeted Company)*** is designing and supervising the construction of ***(deleted)*** to supply these resources.

It is ASSESSED that from the PRC / CPC perspective, they have a vested interest in the planning and processes of ***(Targeted Company)***. This would include the ***(Targeted Company)*** designed infrastructure. Monitoring and tracking the company fits the tactics, techniques and procedures used by the PRC. It is ASSESSED as HIGHLY PROBABLE the PRC will continue to monitor ***(Targeted Company)*** as a source of data on the development and delivery of strategic resources. This includes the ability to access the company computer network when the PRC desires access.

It is ASSESSED as HIGHLY PROBABLE that ***(Targeted Company)*** will:

A. Deny they were attacked;

B. Be uncooperative with any effort to query them on this incident and/or their computer security; and,

C. Deny any investigative access to their network.

SUMMARY

Given the nature of cyber-warfare there is no equivalent to a "smoking gun" nor the precision of "CSI" style forensic analysis. Without access to ***(Targeted Company)*** files, servers, routers and network information, it would be highly difficult to verify the data in this report. What is available is an overwhelming amount of circumstantial evidence. Based on this data it is ASSESSED that ***(Targeted Company)*** was targeted by a cyber-attack based from the PRC. It is HIGHLY PROBABLE that the attack was successful and that the PRC will continue to access company files in order to track the development and delivery of strategic resources

“targeted by a cyber-attack based from the PRC”

Keynotes of This Case Study

1 Personnel had no training in Computer Security and could not provide computer forensic data.
2 Source has ***(Targeted Company)*** network access and is ASSESSED as having reliability rating of A2. Reason for rating is source is not IT trained.
3 VOIP: Voice Over Internet Protocol. The telephone system runs on the company computer network.
4 ***(Targeted Company)*** uses an IP based telephone system. It operated on the same wiring as the computer network and requires the network to be functional and 'reasonably healthy' in order to work correctly.
5 Incident information RATED as A1. Although a cable may have been cut on the ***(company name removed)*** property,

6 The project had not yet attracted interest from North American based protest organizations who track the subject. It is HIGHLY UNLIKELY to have attracted interest from any party that did not have a vested interest in the project.

7 One of the best documented Chinese cyber-attacks on Canada is the effort to track the BHP bid for the Saskatchewan Potash Corporation. Daniel Tobok of Digital Wyzdom are credited in Open Source Media for the detection and analysis.

David Swan CD.
Senior Vice President and leads the CSCSS Defence Intelligence Group (C/DIG)

David Swan is a CSCSS Executive Vice President and leads the CSCSS Defence Intelligence Group (C/DIG) which focuses on transnational / International threats against nations including infrastructure and strategic industries. C/DIG includes Intelligence analysis outside conventional computer security, looking to identify targets and threats before countries (or organizations) are attacked. David is a contributor to CSCSS articles and blog, contributing information on: security threats, case studies and security awareness.

David's working career spans a dynamic technical background and service in the Canadian Military Reserve. A partner in an early Internet Service Provider, David started in Customer Service: specializing in e-mail and troubleshooting. He progressed through network administration, and network engineering to systems design. Twice employed as a Chief Technical Officer (CTO), David developed RFID technology on Linux platforms, improving performance and security. As CTO of **DBiTS** (Database Information Technology Services Inc), he became familiar with Advanced Persistent Threats (APT) and cyber-espionage from attempts to penetrate the development network and acquire company Intellectual Property (IP). Since 2009 he has operated **David Swan Consulting**, providing computer support to businesses in Southern Alberta and specializing in Computer Security Services.

David joined the Canadian Naval Reserve in High School. He has enjoyed success as: a Naval Communicator, a Naval Officer and an Army Intelligence Officer. All three military careers have reflected experience in Command Support and Operational roles. In 1987 He was part of the implementation of a computer-based headquarters: as a user, user group leader, and instructor. He was part of the command operations team during Gulf War I. During 1997-99 He was a project manager responsible for the implementation of an integrated computer command and control (C2) system and subsequently its first deployments. In additional to project manager David's roles with the system included: policy, planning, training, operational deployment, operational procedures and maintenance. David was employed as a SME on the system until 2005. In 2003 David was recruited into the Canadian Army Reserve Intelligence Branch, qualifying as an Intelligence Officer (Land) in 2004. He continued to enjoy an active career supporting both Regular Force and Reserve units as well as numerous other tasks. He works in a command support role as the Intelligence Officer for 41 Canadian Brigade Group.

A graduate of the Advanced Operations Course (AOC) David continues to contribute to the Army at the Unit, Brigade and Command levels. David's military career has included work with U.S. (Coast Guard, Navy and USMC), U.K. (Navy and Army) and NATO.

David resides in Vulcan, Alberta. Canada

CSCSS Defence Intelligence Group Briefing

For a dedicated briefing by the CSCSS Defense Intelligence Group on the issues and challenges regarding National entities and espionage please contact us

Contact Us
For more information on the Defence Intelligence Group or to find out how we can help you please contact us.

· Washington D.C + 571.451.0312
· London, United Kingdom +44 2035141784
· North America +877.436.6746
· Middle East +800.653.407
· Australia +61 2 8003 7553

Email: defintel@cscss.org
www.cscss.org/defence_intelligence.php

C/DIG CSCSS / DEFENCE INTELLIGENCE GROUP

The CSCSS Defence Intelligence Group through its CSCSS subsidiaries has aligned with defense, civilian and intelligence agencies providing specific defence intelligence support to mission-essential requirements at every stage of the program, product and business lifecycle. We deliver mission and technical expertise, delivery of intelligence products, and a commitment to client objectives and results at the strategic, operational and tactical Levels. We provide specialize defence intelligence expertise; services and solutions that help our clients address and achieve their missions, goals and objectives securely

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE

The Centre for Strategic Cyberspace + Security Science / CSCSS is a multilateral, international not-for-profit organization that conducts independent cyber-centric research, development, analysis, and training in the areas of cyberspace, defence intelligence, cyber security, and science while addressing the threats, trends, and opportunities shaping international security policies and national cyberspace cyber security initiatives.

CSCSS, as a strategic leader in cyberspace, works jointly with key partners to address, develop, and define cyber technologies, cyber defence force capabilities, information dominance, and concept operations. We deliver practical recommendations and innovative solutions and strategies to advance a secure