UNCLASSIFIED

Briefing to Critical Infrastructure Sector Organizations on the Canadian Cyber Incident Response Centre (CCIRC)
Cyber in the News...

Spamhaus DDoS grows to Internet-threatening size
More than 300 Gb/s of traffic aimed at the anti-spam site's hosting.

The New York Times
Global Business

South Korea Hit Hard by Massive Cyber-Attack
Published April 1, 2013

Aramco Says Cyberattack Was Aimed at Production
By REUTERs
Published December 9, 2012

Bank DDoS Attacks Resume: Wells Fargo Confirms Disruptions

Anonymous targets Israel in another cyberattack
The hacktivist collective claims to have caused more than $3 billion in damage in protest against treatment of Palestinians, but officials say the attack has caused minimal disruption.
Tactics, Techniques and Procedures

These observed tactics, techniques and procedures have impacted the availability, confidentiality and integrity of critical infrastructure organizations’ networks:

- Distributed denial-of-service (DDoS) attacks
- Destructive malicious software (e.g. Shamoon)
- Compromise of unsecure external-facing websites;
- Compromising user credentials (e.g. phishing emails);
- SQL injection attempts; and
- Watering hole attacks.

**Attacks launched using the above tactics, techniques and procedures have proven to be successful.**
Recent Examples

- Distributed denial-of-service (DDoS) attacks:
  - Waves of DDoS attacks targeting financial institutions (“OpAbabil”);
  - Vulnerabilities in Content Management Systems leveraged to launch DDoS attacks; and
  - Domain Name System (DNS) amplification and reflection DDoS attacks.
- Unsecured Internet facing industrial control systems devices
- Malware infection in organizations’ industrial control systems environment
- Several organizations reporting compromise of user credentials through phishing and spear phishing attacks
- Organizations’ websites compromised through SQL injections and other common techniques
Earlier in 2013, CCIRC sent 221 victim notifications to public and private sector partners in the following sectors:
## Top Exploited Vulnerabilities

<table>
<thead>
<tr>
<th>CVE Reference</th>
<th>CCIRC Product(s)</th>
<th>Risk(s)</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE 2012-0158</td>
<td>• AV12-016</td>
<td>• Used in state-sponsored attacks</td>
<td>• Patch made available by Microsoft in April 2012 (<a href="#">AV12-016</a>)</td>
</tr>
<tr>
<td></td>
<td>• CF12-020</td>
<td>• Spear phishing emails</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CF13-013</td>
<td>• Used in exploit kits to deliver ransomware</td>
<td></td>
</tr>
<tr>
<td>CVE 2013-3163</td>
<td>• AV13-025</td>
<td>• Spear phishing emails</td>
<td>• Patch made available by Microsoft in July 2013 (<a href="#">AV13-025</a>)</td>
</tr>
<tr>
<td></td>
<td>• CF13-010</td>
<td>• Drive-by downloading</td>
<td></td>
</tr>
<tr>
<td>CVE 2013-2471</td>
<td>• AL13-503</td>
<td>• Integrated into several exploit kits to deliver ZeroAccess rootkit and ransomware</td>
<td>• Effective February 2013, Oracle no longer supports Java 6. Users are recommended to upgrade to a newer version, or consider disabling Java.</td>
</tr>
<tr>
<td>CVE 2013-2463</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE 2013-2465</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE 2013-3893</td>
<td>• AL13-003</td>
<td>• Zero-day vulnerabilities</td>
<td>• Patch made available by Microsoft in October 2013 (<a href="#">AV13-0036</a>)</td>
</tr>
<tr>
<td>CVE 2013-3897</td>
<td>• AL13-003 - Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AV13-0036</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specific Mitigation Products

- The following Cyber Flashes released by CCIRC in 2012 and 2013 should be reviewed by critical infrastructure organizations.
- CCIRC recommends that organizations review the mitigation steps included in these Cyber Flashes and consider their implementation in the context of their network environment:
  - CF12-014: Shamoon/DistTrack Malware
  - CF13-007: Internet Explorer 8 Zero Day Vulnerability Used in Watering Hole Type Attacks
  - CF13-008: Tactics and Tools of Emerging Cyber Threat Actors
  - CF13-013: Phishing campaign leveraging CVE-2012-0158 and targeting critical infrastructure
  - CF13-014: Java Based Remote Access Trojan (RAT) Indicators
Mitigation: Denial-of-Service (DDoS) Attacks

1. **Preparation**: Clear and complete procedures and guidelines should be established before an attack takes place.

2. **Identification**: Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process.

3. **Containment**: Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages.

4. **Recovery**: Dependent on the containment strategy employed and the sensitivity to its collateral impact, an organization may be under different pressure to recover.

5. **Lessons Learned**: Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed.

**CCIRC Technical Report: Mitigation Guidelines for Denial of Service Attacks**
Securing an Industrial Control Systems Environment

- Establish in-depth knowledge of control system(s) and of corporate network(s): apply defense-in-depth.
- Ensure corporate networks and control systems networks are physically separated.
- Eliminate default passwords: adhere to a strict password policy and access controls.
- Implement change and patch management programs

## Mitigation Strategies

Applying the four mitigation strategies below will prevent at least 85% of compromises, and closer to 100%, based on testing performed at the Australia Signals Directorate.

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Mitigation Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Undertake <strong>application whitelisting</strong> of permitted/trusted programs, to prevent execution of malicious or unapproved programs.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Patch applications</strong> such as Adobe PDF viewers and Flash Player, Microsoft Office and Java Runtime Environment. Patch or mitigate high risk vulnerabilities within two days.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Patch operating system</strong> vulnerabilities. Patch or mitigate high risk vulnerabilities within two days.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Minimise the number of users with domain or local administrative privileges</strong>. Such users should use a separate unprivileged account for email and web browsing.</td>
</tr>
</tbody>
</table>
CCIRC – Mandate

Canada’s national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events for vital systems outside of the Government of Canada.
Services: Advanced Technical Capabilities

- **Automated Malware Analysis**
  - Malware feeds
  - Malware repository

- **Artifact Analysis**

- **Industrial Control Systems**
  - Equipment for security testing and analysis in support of critical infrastructure sectors.

- **National Cyber Threat Notification System (NCTNS)**

- **Indicators of Compromise**
## Services: Community Portal

**CCIRC Cyber Community Portal**
Portail de la communauté cybernétique CCRIC

This document library contains the CCIRC documents for the community portal.

<table>
<thead>
<tr>
<th>Type</th>
<th>File Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>221 KB</td>
<td>CCIRC Situation Report 25 April 2013</td>
<td></td>
</tr>
<tr>
<td>156 KB</td>
<td>CCIRC Situation Report 24 April 2013</td>
<td></td>
</tr>
<tr>
<td>671 KB</td>
<td>Weekly_Technical_Report_24_April_2013</td>
<td></td>
</tr>
<tr>
<td>35 KB</td>
<td>av13-016_UP2_BIL</td>
<td></td>
</tr>
<tr>
<td>131 KB</td>
<td>CCIRC Situation Report 23 April 2013</td>
<td></td>
</tr>
<tr>
<td>134 KB</td>
<td>CCIRC Situation Report 22 April 2013</td>
<td></td>
</tr>
<tr>
<td>196 KB</td>
<td>CCIRC Situation Report 21 April 2013</td>
<td></td>
</tr>
<tr>
<td>154 KB</td>
<td>CCIRC Situation Report 19 April 2013</td>
<td></td>
</tr>
<tr>
<td>356 KB</td>
<td>JN13-003_Windows_XP_SP3_EOL_Bilingual</td>
<td></td>
</tr>
<tr>
<td>152 KB</td>
<td>CCIRC Situation Report 17 April 2013</td>
<td></td>
</tr>
<tr>
<td>175 KB</td>
<td>CF13-006 - Update Apache Darktrace Malware</td>
<td></td>
</tr>
<tr>
<td>634 KB</td>
<td>Weekly_Technical_Report_17_April_2013</td>
<td></td>
</tr>
<tr>
<td>167 KB</td>
<td>Rapport - Résumé cybernétique opérationnel du CCIRC - 17 au 30 mars 2013</td>
<td></td>
</tr>
<tr>
<td>747 KB</td>
<td>Rapport technique hebdomadaire_10_Apr_2013</td>
<td></td>
</tr>
<tr>
<td>193 KB</td>
<td>CCIRC - Mise à jour du bulletin cybernétique CF13-006</td>
<td></td>
</tr>
<tr>
<td>13 KB</td>
<td>AV13-018_BIL</td>
<td></td>
</tr>
</tbody>
</table>

**CCIRC Product**
- Ops - Daily Report
- Ops - Weekly Technical Report
- Ops - Weekly Technical Report
- Ops - Advisory
- Ops - Daily Report
- Ops - Daily Report
- Ops - Daily Report
- Ops - Daily Report
- Ops - Information note
- Ops - Daily Report
- Ops - Cyber Flash
- Ops - Weekly Technical Report
- SA - CCIRC Cyber Operational Summary
- SA - CCIRC Cyber Operational Summary
- Ops - Weekly Technical Report
- Ops - Cyber Flash

**Date Published**
- 4/25/2013
- 4/24/2013
- 4/24/2013
- 4/22/2013
- 4/21/2013
- 4/19/2013
- 4/19/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/17/2013
- 4/16/2013
Services: Community Portal

Electrical sub-sector membership
- 35 accounts
- 18 organisations
- Plenty of room for more
Suite of Technical Products

Regularly issued products that provide partners with time sensitive information related to specific cyber threats, including detection indicators, mitigation information, and best practices.

- Cyber flashes;
- Information notes;
- Technical reports;
- Alerts; and
- Advisories.
Suite of Executive Reports

Operational reports that provide information about cyber incidents seen by CCIRC to help support organizations' operational and security decision-making.

- Bi-weekly;
- Quarterly; and
- Annually.
Summary of Products and Services

July – September 2013
Summary: Types of Incidents

July – September 2013

- Malicious code / Compromise: 55%
- Phishing / Targeted emails: 28%
- Investigation / Research: 10%
- Scans / Probes / Attempted access: 1%
- Unauthorized access / Credential theft: 4%
- Denial of service: 2%
- Improper usage / Misconfig.: 0%

N = 460
Summary: Incidents by Sector

July – September 2013

- ICT: 36%
- Energy and Utilities: 23%
- Federal: 9%
- Provincial / Territorial: 3%
- Finance: 23%
- Transportation: 1%
- Manufacturing: 1%
- Food: 1%
- Safety: 1%
- Education: 3%
Cyber security is a shared responsibility and is underpinned by two-way information sharing.

<table>
<thead>
<tr>
<th>Sector</th>
<th>Incidents</th>
<th>Incidents Reported to CCIRC</th>
<th>Victim Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy and Utilities</td>
<td>9</td>
<td>1</td>
<td>3,932</td>
</tr>
<tr>
<td>Finance</td>
<td>79</td>
<td>32</td>
<td>345</td>
</tr>
<tr>
<td>Information and Communication Technology (ICT)</td>
<td>128</td>
<td>11</td>
<td>5,341,511</td>
</tr>
<tr>
<td>Government (F/P/T/M)</td>
<td>45</td>
<td>6</td>
<td>19,231</td>
</tr>
<tr>
<td>Health</td>
<td>0</td>
<td>0</td>
<td>5,072</td>
</tr>
<tr>
<td>Food</td>
<td>1</td>
<td>0</td>
<td>247</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>4</td>
<td>1</td>
<td>1,962</td>
</tr>
<tr>
<td>Water</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transportation</td>
<td>2</td>
<td>1</td>
<td>363</td>
</tr>
<tr>
<td>Safety</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>269</strong></td>
<td><strong>52</strong></td>
<td><strong>5,372,663</strong></td>
</tr>
</tbody>
</table>
Number of events specific to the Electricity sub-sector

- Events since June 2011
  - 2011 : 5
  - 2012 : 13
  - 2013 : 16

- Reporting of events in Electricity 25% higher than O&G

- We can only report on events that are reported to CCIRC
Number of events specific to the Electricity sub-sector (cont’d)

- Type events reported
  - (3) Generic phishing
  - (9) Spear phishing
  - (4) Site compromise
  - (1) Drive by infection
  - (2) Brute force attacks / Port scanning
  - (5) Malware targeting the sector
  - (2) Detection based on CCIRC IoCs
  - (13) Malcode submissions
2012 – 2013 A Year of Progress

- **Strengthened CCIRC’s legal, policy and process foundations**
  - Updated and focused mandate.
  - Approved CCIRC Privacy Impact Assessment.
  - Developed a comprehensive suite of Standard Operating Procedures.
  - Developed standardized reporting criteria, impact assessment guidelines, and information sharing protocols.

- **Expanded collaboration with internal and external partners**
  - Enhancing trust through partner Non-Disclosure Agreements – Memorandums of Understanding.
  - Secure collaboration via the CCIRC Community Portal.
  - Improve synchronization between CCIRC, the Government Operations Centre and PS Communications.
  - Validation through incident reporting trials with provinces including Ontario, Alberta and Manitoba.
  - Operations are 24/7, with staff now on-site 15 hours a day, seven days per week (15/7).

- **Enhanced analytic capability**
  - Acquisition and integration into its operations a world-class malware laboratory, enabling CCIRC to advance its understanding of Canada’s cyber threat landscape and consequently to improve the mitigation advice it can provide to help critical infrastructure operators defend their systems.
  - Extended expertise and credibility with the development and deployment of an Industrial Control Systems (ICS/SCADA) test bed, which complements the NRCan / RCMP / DRDC training centre.
  - Launch of the National Cyber Threat Notification System to notify Canadian Internet Protocol (IP) address operators of compromise.
What CCIRC is Working Towards

- **Enhancing engagement efforts**
  - Complete engagement efforts with current priority sectors:
    - Energy and utilities
    - Finance
    - Information and communication technology
    - Provincial, territorial and municipal government

- **Continuing to develop and operationalize CCIRC’s new technology and enhanced capabilities**
  - BEhavioural Analysis using Virtualization and Experimental Research (BEAVER) and Critical Infrastructure Indicator and Attack Notifications (CIIAN) have been undergoing interface change to better meet the needs of CCIRC Incident Handlers.
  - New malware feeds have been added to the automated malware analysis performed in the lab.
  - Standard Operating Procedures developed to facilitate the processing of ad-hoc malware submission. This process is soon to be automated.

- **Formally defining the objectives and service offerings of a Industrial Control Systems Program**

- **Finding new accommodations**
  - Supports overall move towards enhanced fusion within the cyber operations community
Contact Us

cyber-incident@ps-sp.gc.ca