Responding to Cybercrime:
Preserving Crucial Evidence for Law Enforcement

RCMP “National” Division
Integrated Technological Crime Unit (ITCU)

Presented by:
Sgt. Stéphane Turgeon
Cpl. David Connors
Goals

1. Educate managers and IT personnel on what digital evidence and data must be preserved from their computer systems and networks, following a cybercrime, to enable law enforcement to pursue a criminal investigation.

2. Provide guidelines on reporting these cybercrime incidents to Canadian law enforcement agencies, such as the RCMP’s Technological Crime Units.

3. Familiarize you with the expectations law enforcement will have when they respond to a cybercrime incident.
Topics Covered

1. Introductions
2. Role and Mandates of the RCMP Integrated Technological Crime Units (ITCUs)
3. Define Critical Infrastructure & Cybercrime
4. Evidence Preservation Guidelines
5. Cybercrime Incident Response Steps & Guidelines
6. Law Enforcement Expectations
Speaker Introductions

• **Sgt. Stéphane Turgeon**
  - NCO i/c / Unit Commander of the RCMP National Division ITCU
  - 15 yrs in the RCMP
  - 9 yrs in Technological Crime as a Computer Forensic Investigator

• **Cpl. David Connors**
  - Team Leader / Supervisor – Computer Forensics and Investigation
  - 10 yrs in the RCMP
  - 7 yrs in Technological Crime as a Computer Forensic Investigator
RCMP Technological Crime Units

11 Regional Offices plus HQ Policy Centre
Approx. 150 employees (regular and civilian members)
Role and Mandate of Technological Crime Units

- Investigate “pure” computer crimes
  - Unauthorized use of computer, s. 342.1 CC
  - Possession of device to obtain computer service, s. 342.2 CC
  - Mischief in relation to data, s. 430 (1.1) CC

- Provide technological investigative services for all computer facilitated crimes (to both RCMP units and federal partners)
  - Search warrant preparation and execution
  - Analysis of computers / digital evidence processing
  - Provide expert advice as needed
National Division ITCU

RCMP
8 Regular Members
&
3 Civilian Members

CFNIS
(Canadian Forces National Investigation Services)
4 Military Police Officers

National Division - Ottawa
Role and Mandate of National Division ITCU

• Provide expertise and assistance to RCMP for:
  • National Security Investigations
  • “O” Division Ottawa Detachment Investigations
  • Sensitive and International Investigations

• Investigate breaches / compromises of:
  • Federal Government IT Infrastructure
  • Critical Infrastructure / Essential Public Services

* Any companies / entities that fall outside of the above mandates should contact their local law enforcement agency for assistance.
Role and Mandate of National Division ITCU

- Maintain partnerships with agencies such as Canadian Cyber Incident Response Centre (CCIRC), Cyber Threat Evaluation Centre (CTEC), Shared Services Canada (SSC), Government of Canada Computer Incident Response Team (GC-CIRT), and other federal agencies.
Areas of Responsibility for IT INCIDENTS

Provinces & Territories, International Partners, Industry, Critical Infrastructure

CCIRC (PS)
- National incident response coordination

Government of Canada

TBS
OVERSIGHT & DIRECTION
- Monitoring
- Coordination
- Post-incident analysis

IT Incidents

GC CIRT (SSC)
- Central coordination centre for GC IT incidents

Cyber Incidents

GC CTEC (CSEC)
(Cyber incident focused)
Critical Infrastructure

Critical infrastructure - refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.

1. Health
2. Food
3. Finance
4. Water
5. Information and Communication Technology
6. Safety
7. Energy and Utilities
8. Manufacturing
9. Government
10. Transportation

Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.
What is Cybercrime?

Cybercrime: “A criminal offence involving a computer; as the object of the crime, or the tool used to commit a material component of the offence.”

- Government of Canada

Computer as the Object of the Crime:
- Denial-of-Service (DoS)
  - phishing
  - “hacking”

Computer as the Tool to Commit:
- child pornography
  - hate crimes
  - fraud
Reporting Criminal Offences

1. Report the incident to your local law enforcement agency, at any time, if there is reasonable evidence of a crime under the Criminal Code (CC) of Canada.

2. Report the incident to the RCMP if the Criminal Code offence involves:
   - Federal Government IT Infrastructure
   - Critical Infrastructure / Essential Public Services

3. Report the incident to the Canadian Security Intelligence Service (CSIS) if the offence is a national security concern.
Evidence Preservation Guidelines for First Responders

1. Establish Standard Operating Procedures (SOPs) for the management and coordination of IT-related security incidents.

2. Document and record all activity during, and after, the incident.

3. Preserve, isolate, and secure any affected systems to prevent tampering or accidental access.

4. Use proper chain of custody procedures.
Evidence Preservation Guidelines for First Responders

5. Trained IT personnel only should be securing and preserving evidence.

6. Forensically trained IT personnel only should be imaging and analyzing the evidence.

7. Only use the “forensic image” for analysis.

8. Request guidance from CCRIC or GC-CIRT whenever needed.
Primary Areas of Interest for Digital Evidence

Most Volatile

- RAM
- Live Network Analysis
- Log Files
- Hard Drives / ESM

Least Volatile

- Backup Systems
Responding to a Cybercrime Incident

**Identification**
- Recognize and Identify the Threat
- Begin Documentation

**Preservation**
- Preserve, Isolate, & Secure the Affected System(s) & Log(s)
- Secure the Digital Evidence

**Collection**
- Record All Actions Related to the Handling of the Digital Evidence
- Provide All Reports, Diagrams & Incident Notes to Law Enforcement
Cyber Incident Scenario

You are the senior incident handler in a medium-sized agency/company with forensic and analysis capabilities. You detect multiple spear phishing incidents and suspect that files were ex-filtrated. You activate your incident response plan.
Guidelines

- Identify the nature and extent / impacts of the incident.
- Define and create tasks to handle the situation
- Assign personnel as needed.
- Contact CCRIC (if public agency) or GC-CIRT (if government agency) to provide preliminary notification.
• Ensure the infected machines are no longer accessible to non-authorized personnel.

• Ensure no attempts are made to explore or recover the content of the infected machines.

• Incident handlers must document:
  • When/where the incident was discovered
  • How the incident was discovered
  • Who discovered/reported the incident
Guidelines

• Ensure the infected machines remain in “Live” state for memory collection

• Record:
  • All processes running on the infected machines
  • All physical connections from the infected machines to all other devices
  • All IP addresses and wireless connections to and from the infected machines across the network

• Preserve all traffic logs (such as firewall, etc.) to and from the infected machines across the network.
Guidelines

- When disconnecting machines, carefully monitor to ensure the hard drive is not being erased. If you suspect any information is being deleted, immediately power the machine down.

- Image the hard drives (if trained/capable)

- Acquire RAM (if trained/capable)

- Follow chain of custody procedures to secure the evidence

- Contact CCRIC / GC-CIRT for guidance, as needed.

Preservation
Guidelines

• Record all actions relating to the collection, preservation, access, storage, and transfer of digital evidence

• Prepare a network diagram with the IP addresses of all the infected machines and all other relevant network nodes.

• Prepare, date and sign detailed notes on all actions taken during the course of the incident response.

• Communicate all observations made and actions taken to law enforcement investigators.
Guidelines

• Secure the evidence and track its custody

• Calculate Hash value (MD5) any digital evidence, logs, hard drive images, etc.

• Produce working copies of network/system logs, analysis, and digital evidence.

• Provide of copy of the digital evidence, logs, and analysis to law enforcement agency and CCRIC / GC-CIRT, if requested

• Infected machines can be put back into service with new hard drives restored to known-good states.
Law Enforcement Expectations

- Full cooperation from all stakeholders
  - Witness statements
  - Reports & notes
  - Availability of evidence

- Potential access to your computer systems and facilities

- Willingness to testify in a court of law

- Likelihood of successful prosecution

- Other aspects to take into consideration
  - Publicity (media)
  - Public awareness
Contacts

- RCMP National Operations Centre (NOC)
  - RE: Criminal Activity
  - 24/7 service: # 613-993-4460
    - Calls may be redirected to local law enforcement organizations as appropriate

- CSIS
  - RE: National Security / Terrorism
  - # 613-993-9620
Questions ???

Thank you!

References:
GC IT TIMP – Government of Canada
Public Safety – Canada’s Cyber Security Strategy
RCMP Website: www.rcmp.gc.ca – Technological Crime Page