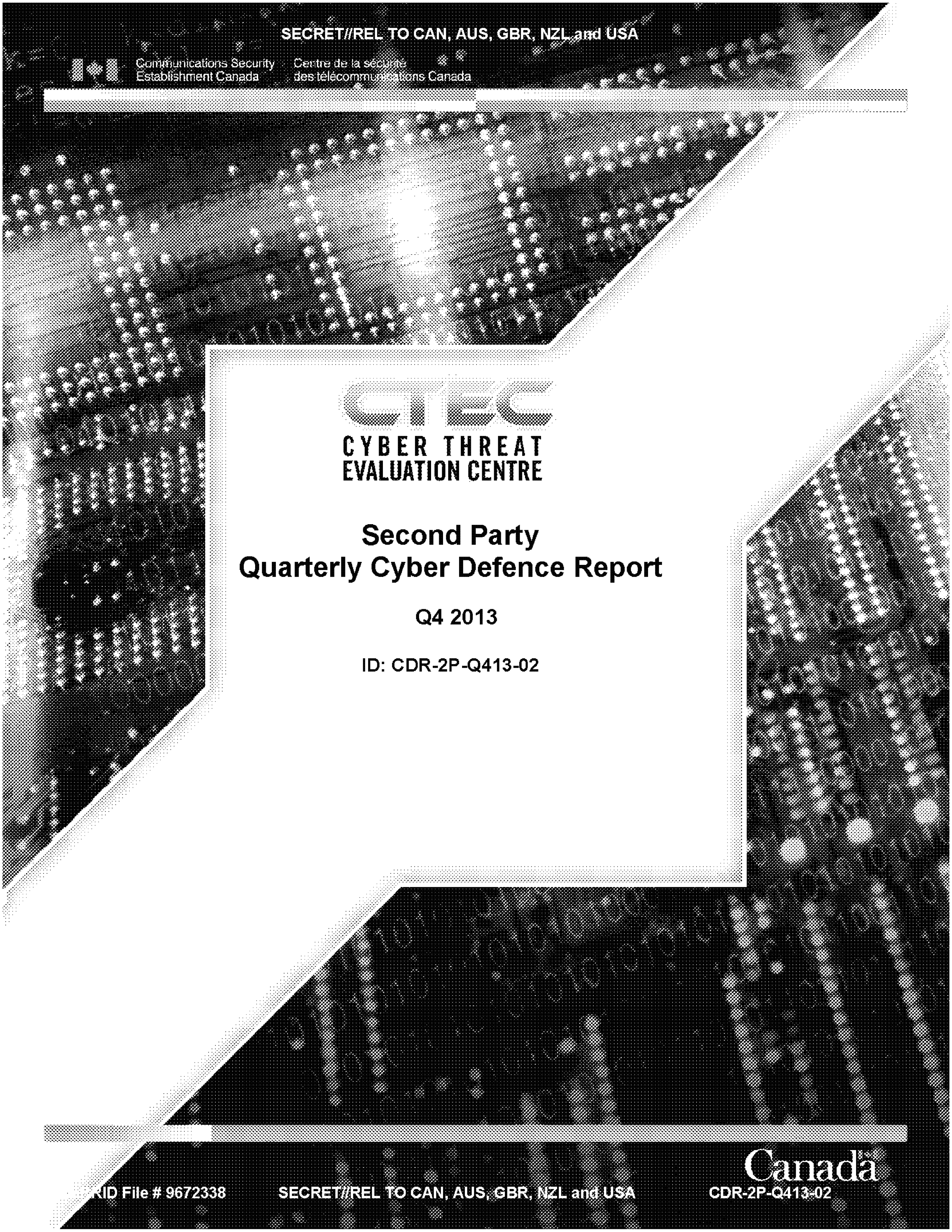
SECRET//REL TO CAN, AUS, GBR, NZL and USA

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



CTEC
CYBER THREAT EVALUATION CENTRE

Second Party Quarterly Cyber Defence Report

Q4 2013

ID: CDR-2P-Q413-02

Canada

RID File # 9672338 SECRET//REL TO CAN, AUS, GBR, NZL and USA CDR-2P-Q413-02

TABLE OF CONTENTS

This report is the property of the Communications Security Establishment Canada (CSEC). The report must be:

- *Securely stored according to the security classification,*
- *Subject to access control, and*
- *Used in a manner which will protect sources or methods.*

Information contained in this report may only be shared with staff responsible for network defence or cyber threat analysis within your department or organization and must be accompanied by a statement of those restrictions. Any actions based on the information contained in this report, other than those prescribed in the report's contents, must be pre-approved by the Operational Policy section at the Communications Security Establishment Canada.

This report contains information from recognized private communications. The report is provided to the recipient on the understanding that the report is essential to identify, isolate, or prevent harm to Government of Canada computer systems or networks.

INTRODUCTION

(U) This is a report on cyber-security threats to Government of Canada (GC) systems, produced by the Cyber Threat Evaluation Centre (CTEC). The report highlights the key cyber threat incidents detected for Q4 2013.

(U) This report is based on confirmed malicious threats affecting Government of Canada systems. Other suspicious activities may have taken place but are not included in this report. Should further analysis determine that the observed suspicious activity is malicious, details will be reported at that time.

(U) Information included in this report is based on current knowledge and available data from CSEC operations. CSEC leverages a variety of data sources on unclassified networks [redacted] As such, care should be exercised in making comparisons between data points.

(U) Contact Information:

ctec@cse-cst.gc.ca

SUMMARY *(S//REL TO CAN, AUS, GBR, NZL, USA)*

Foreign State-Sponsored Activity - Q4 2013

[redacted]

Actors	Incident Severity	Methods
[redacted]	[redacted]	[redacted]

Figure 1: Q4 2013 Overview

Overview

[redacted]

COMMONLY DETECTED THREAT VECTORS

(U) Q4 2013

(S//Rel to CAN, AUS, GBR, NZL, USA) The most common threat vector this quarter was spear-phishing email [redacted]

(S//Rel to CAN, AUS, GBR, NZL, USA) The threat vector used [redacted]

(S//Rel to CAN, AUS, GBR, NZL, USA) Please see Annex 2 for Common Vulnerabilities and Exposures (CVE) information relevant to the incidents reported this quarter.

[redacted]

Figure 2: Commonly Detected Threat Vectors – Q4 2013[1]

[1] [redacted]

SUMMARY *(S//REL TO CAN, AUS, GBR, NZL, USA)*

Foreign State-Sponsored Activity - 2013

[redacted]

Actors Incident Severity Methods

[redacted]

Figure 3: 2013 Overview

Overview

[redacted]

STATE-SPONSORED CYBER-SECURITY HIGHLIGHTS
(U) Q4 2013

[redacted]

Increase in Cyber Threat Activity from [redacted]

(S//Rel to CAN, AUS, GBR, NZL, USA) An increase in cyber threat activity from [redacted]

[redacted]

DETAILS OF EXPLOIT KITS & BOTNETS *(S//REL TO CAN, AUS, GBR, NZL, USA)*

Please note that exploit kit and botnet activity is tracked and reported separately from foreign state-sponsored activity.

Exploit Kits & Botnets - Q4

[redacted]

Exploit Kits & Botnets	Number of Affected Departments/Sector
[redacted]	

Figure 4: Q4 Exploit Kit & Botnet Overview

Overview

Exploit kit and botnet activity resulted in [redacted] this quarter. The majority of these tools exploit known vulnerabilities, indicating that timely patching of GC systems is critical in decreasing the number of compromises. Possible consequences of compromise are: theft of login credentials, theft of protected data, and downloads of ransomware, malware, or trojans. Exploit kits take advantage of common vulnerabilities, allow for customizable implants, and are often inexpensive, making them appealing to a variety of threat actors. [redacted]

IMPLANTS & MALWARE

(U) Q4 2013

(S//Rel to CAN, AUS, GBR, NZL, USA) [redacted]

[redacted]

Figure 5: Implants Detected in Cyber Threat Incidents – Q4 2013

ANNEX 1
SUMMARY OF MALICIOUS DOMAIN NAMES, URLs, & IP ADDRESSES AFFECTING GC SYSTEMS

(S//Rel to CAN, AUS, GBR, NZL, USA) Q4 2013

[redacted]

ANNEX 1 (CONTINUED)

(S//Rel to CAN, AUS, GBR, NZL, USA) Q4 2013

[redacted]

ANNEX 1 (CONTINUED)

(S//Rel to CAN, AUS, GBR, NZL, USA) Q4 2013

[redacted]

ANNEX 2
COMMON VULNERABILITIES & EXPOSURES (CVE) REFERENCE

(S//Rel to CAN, AUS, GBR, NZL, USA) Q4 2013

[redacted]

ANNEX 3
REFERENCE MATERIAL

(S//Rel to CAN, AUS, GBR, NZL, USA) Q4 2013

The following reference materials can be found on CSEC's [redacted]

- Lexicon of terms used in this report:
  [redacted]
- Government of Canada Departments by Sector:
  [redacted]
- [redacted]

DISTRIBUTION

NSA

[redacted]

GCHQ

[redacted]

DISTRIBUTION (CONTINUED)

GCSB

[redacted]

DSD

[redacted]

CSIS

[redacted]

CSEC

John Forster, Chief CSEC, [redacted]

[redacted]