

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

Q2 2013

ID: CDR-2P-Q213-02

IRID File # 1348849

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

Canada
CDR-2P-Q213-02

TABLE OF CONTENTS

INTRODUCTION	2
SUMMARY	3
CYBER THREAT ACTORS.....	ERROR! BOOKMARK NOT DEFINED.
SEVERITY OF INCIDENTS.....	ERROR! BOOKMARK NOT DEFINED.
COMMONLY DETECTED THREAT VECTORS.....	5
CYBER-SECURITY HIGHLIGHTS	6
ACTIVITIES OFTEN RELATED TO CRIMINAL INTENT	7
CYBER THREAT ACTOR TRADECRAFT.....	ERROR! BOOKMARK NOT DEFINED.
IMPLANTS & MALWARE	9
ANNEX 1	10
ANNEX 2	13
ANNEX 3	14
DISTRIBUTION	15

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, and is therefore intended for Canadian Government use only.

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 Q2 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)

Q3 2013



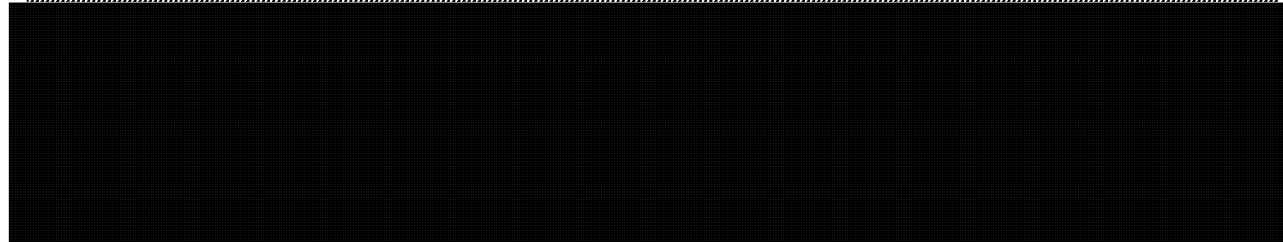
Actors

Incident Severity

Methods

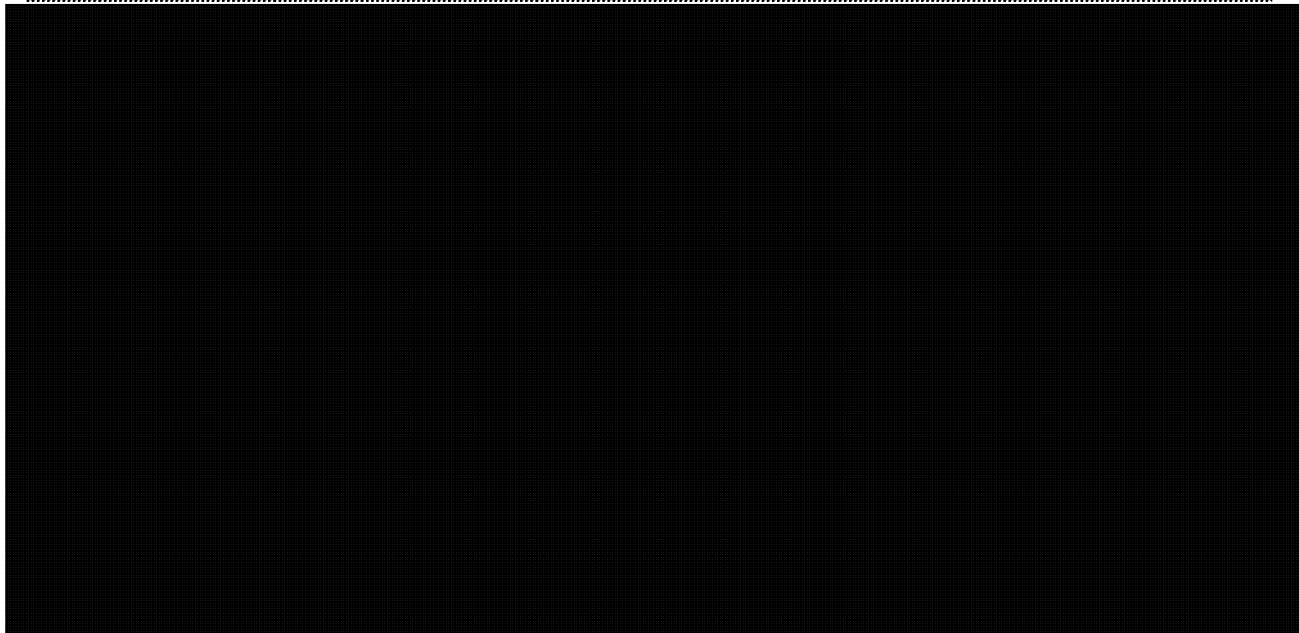
Figure 1: Q3 2013 Overview

Overview



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

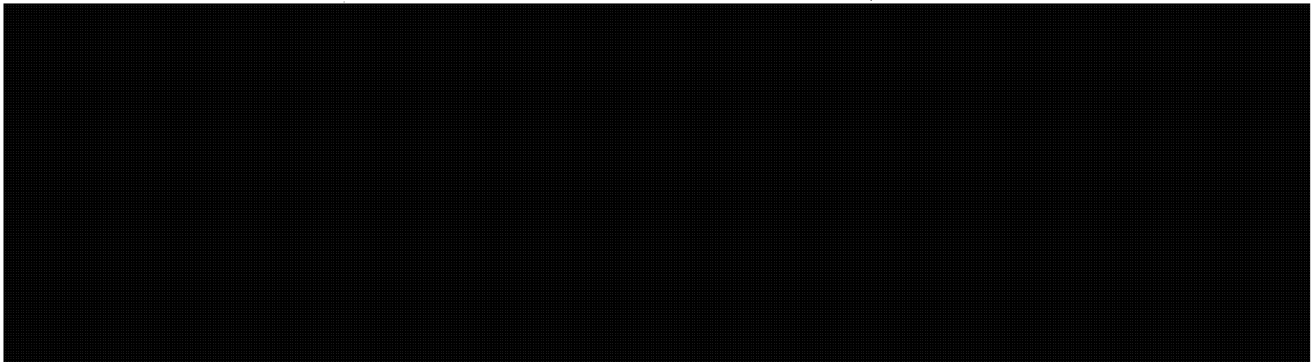
Year-to-Date



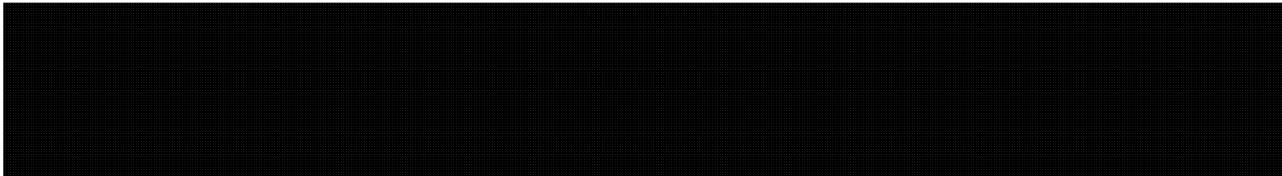
Actors

Incident Severity

Methods



Overview



COMMONLY DETECTED THREAT VECTORS

(U) Q3 2013

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

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

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

(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.

Figure 3: Commonly Detected Threat Vectors – Q3 2013

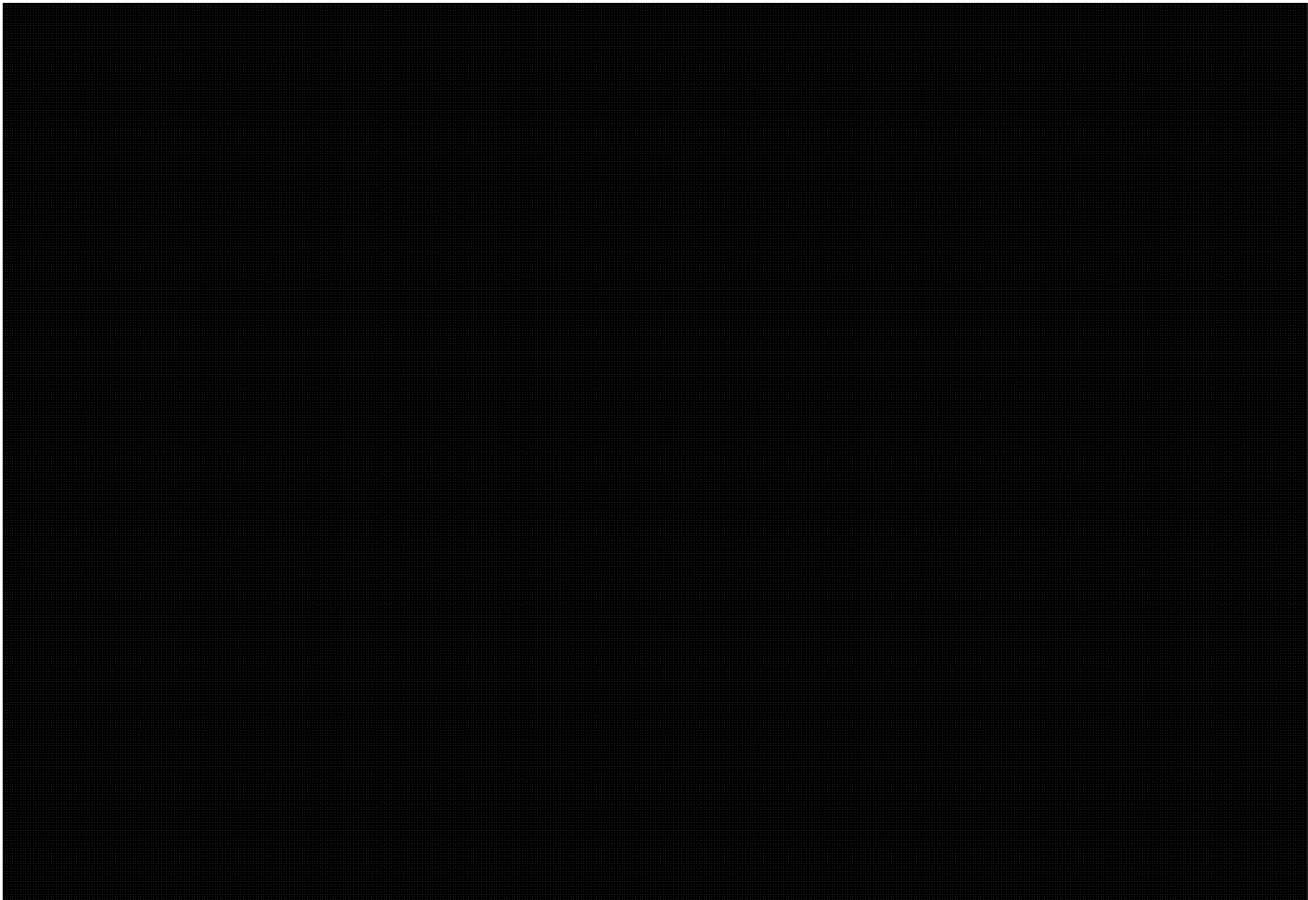
SECRET//REL TO CAN, AUS, GBR, NZL and USA

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

CTEC CYBER THREAT
EVALUATION CENTRE

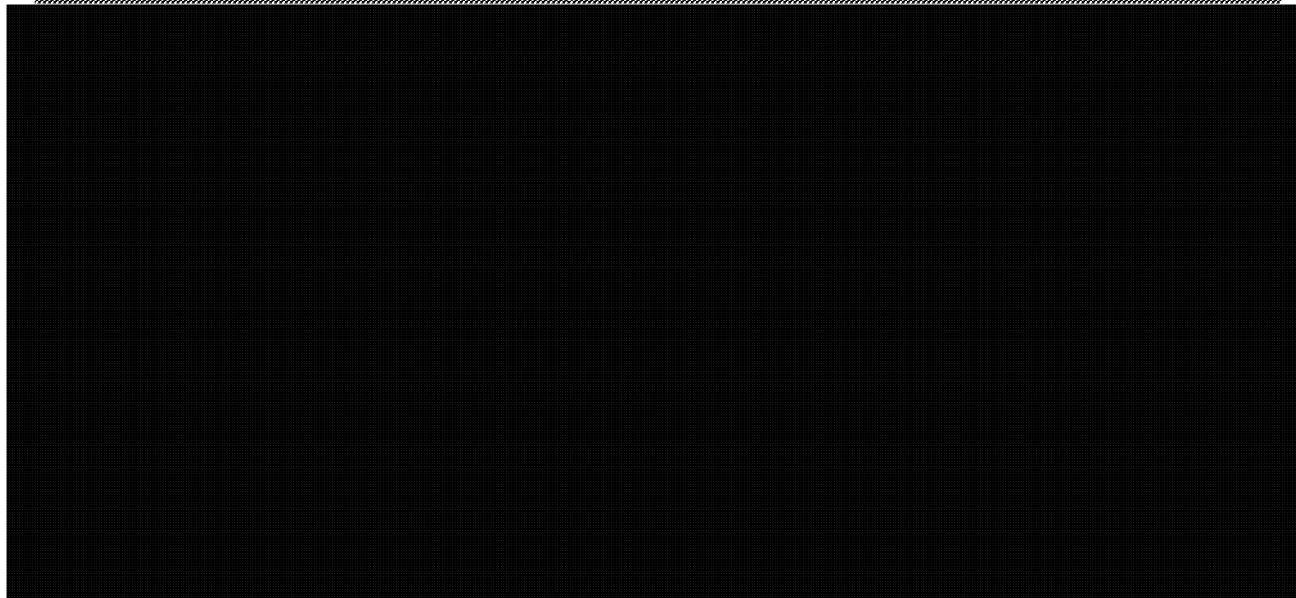
CYBER-SECURITY HIGHLIGHTS

(U) Q3 2013



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

Please note that 'cybercrime' activity is tracked and reported separately from foreign state-sponsored activity. The number of 'cybercrime' incidents being reported continues to rise as detection tradecraft improves.

'Cybercrime'

Exploit Kits
& Botnets

Number of Affected Departments/Sector

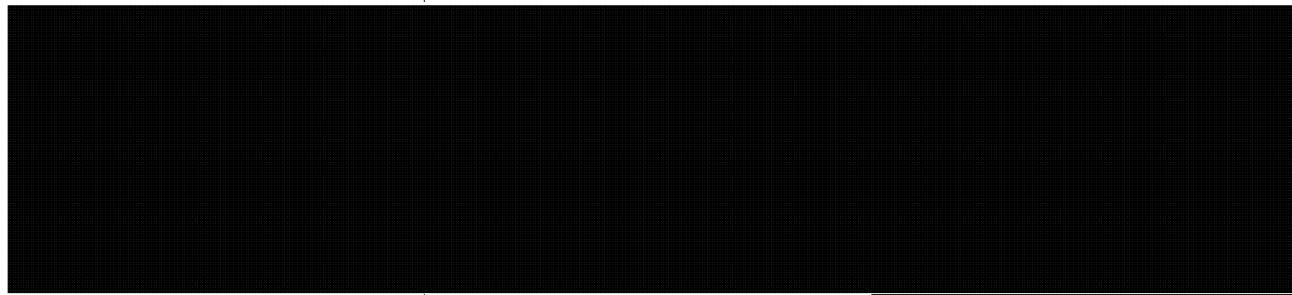


Figure 4: Q3 'Cybercrime' Overview

Overview

Cyber activity often related to criminal intent resulted in [REDACTED] this quarter. The majority of related 'cybercrime' tools (generally exploit kits and botnets) exploit known vulnerabilities, indicating that timely patching of GC systems may aid 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 are continuously effective against GC systems because of their constantly evolving nature. They take advantage of common

vulnerabilities, allow for customizable implants, and are often inexpensive, making them appealing to a variety of threat actors.

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

EXPLOIT KIT ACTIVITY HIGHLIGHT

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

(S//Rel to CAN, AUS, GBR, NZL, USA) Shared Services Canada (SSC)¹

¹ Shared Services Canada (SSC) was created to centralize GC IT infrastructure. SSC is "mandated to deliver email, data centre and telecommunication services to 43 federal departments and agencies." (www.ssc-spc.gc.ca/pages/mndt-eng.html)

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


COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

CTEC CYBER THREAT
EVALUATION CENTRE

IMPLANTS & MALWARE

(U) Q3 2013

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



GC Sectors Affected:

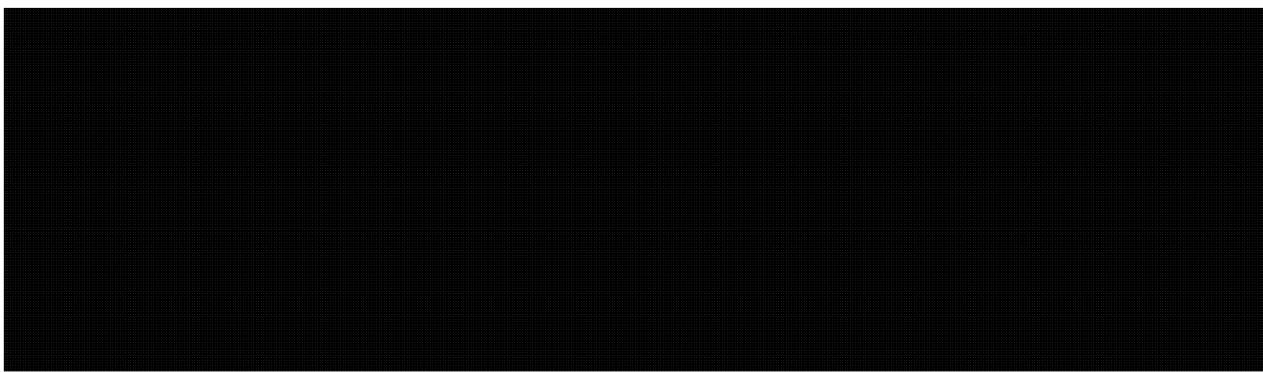
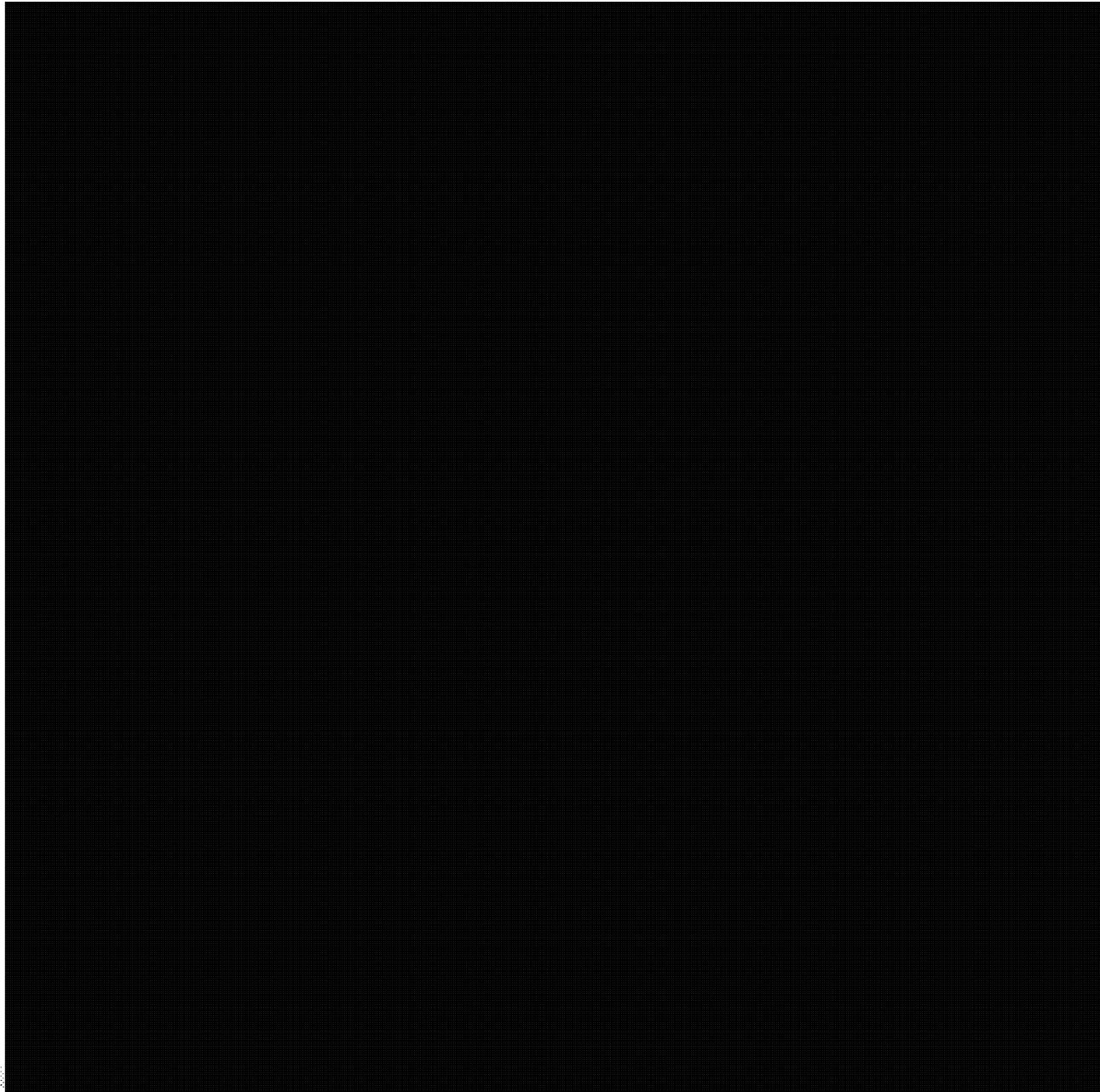


Figure 5: Implants Detected in Cyber Threat Incidents – Q3 2013

ANNEX 1

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

(S//Rel to CAN, AUS, GBR, NZL, USA) Q3 2013



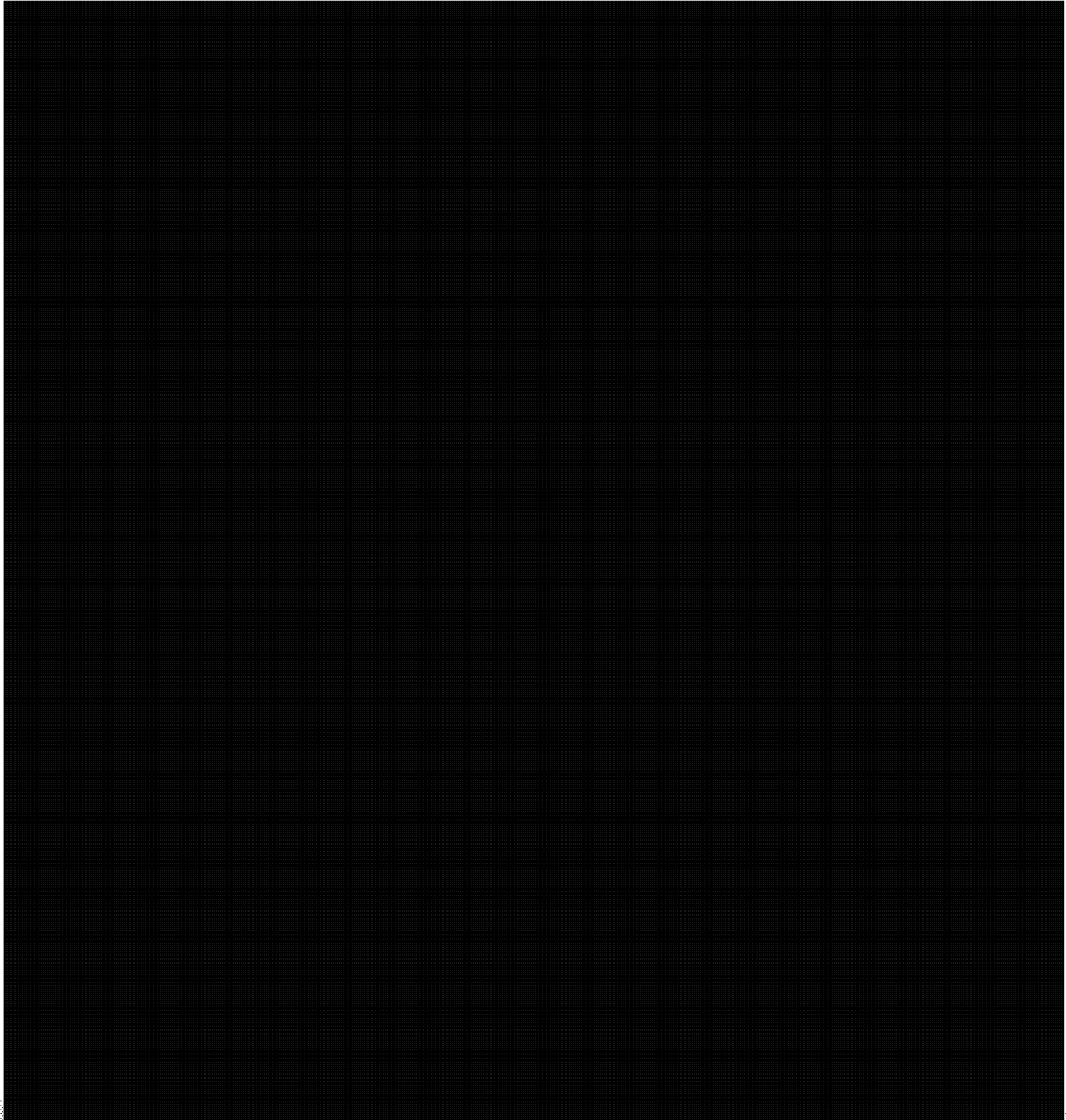
SECRET//REL TO CAN, AUS, GBR, NZL and USA

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

CTEC CYBER THREAT
EVALUATION CENTRE

ANNEX 1 (CONTINUED)

(S//Rel to CAN, AUS, GBR, NZL, USA) Q3 2013



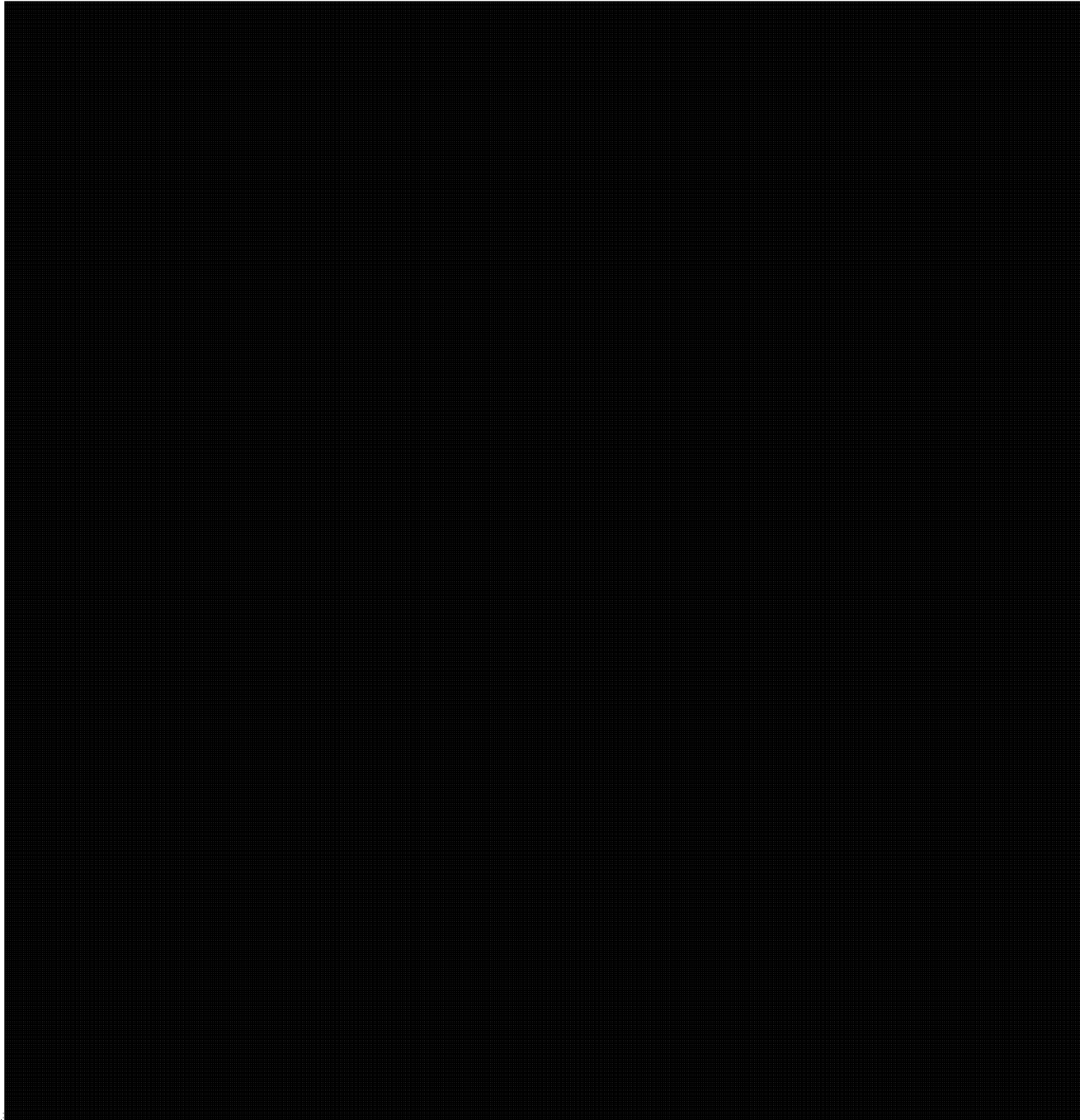
SECRET//REL TO CAN, AUS, GBR, NZL and USA

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

CTEC CYBER THREAT
EVALUATION CENTRE

ANNEX 1 (CONTINUED)

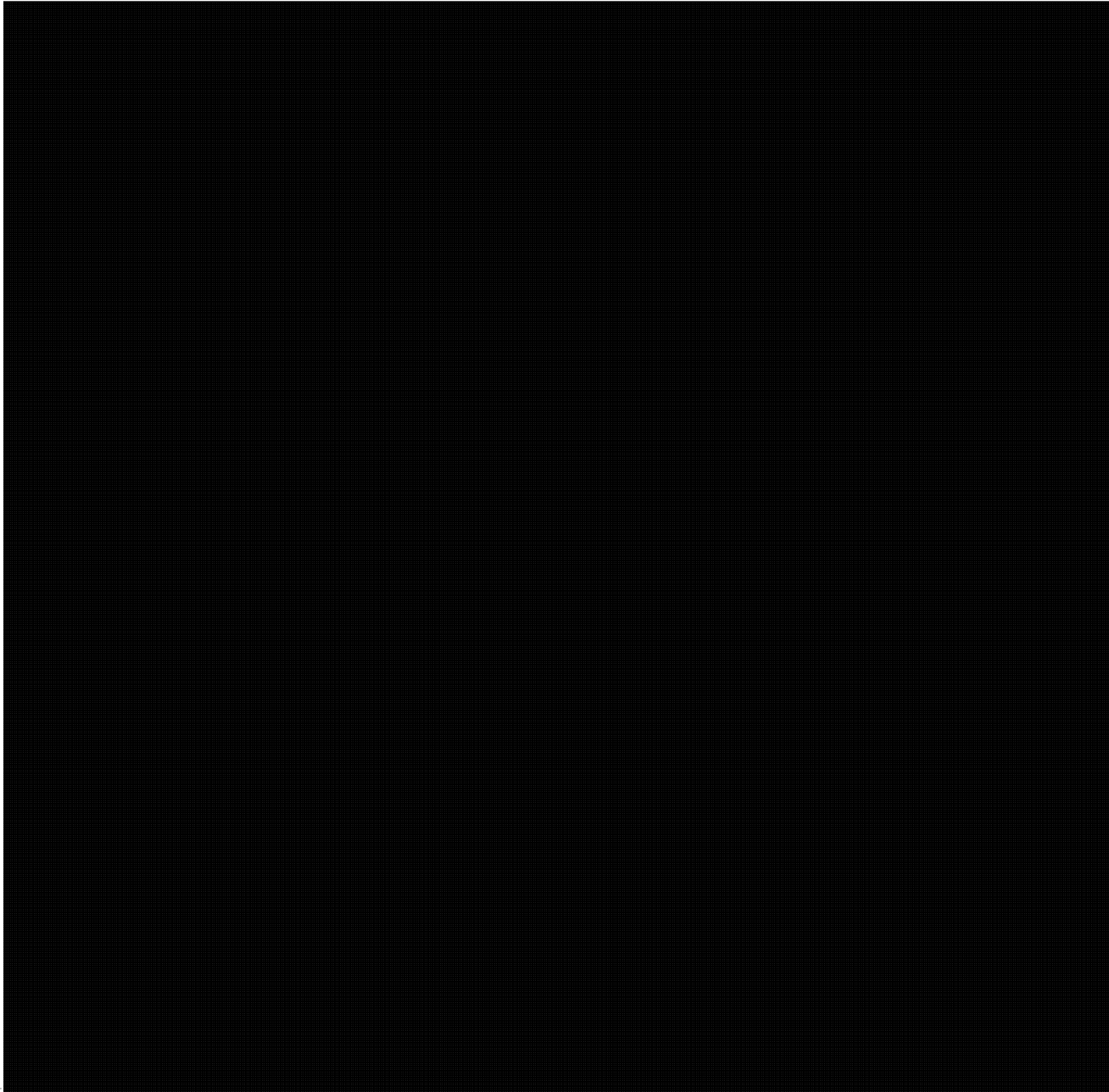
(S//Rel to CAN, AUS, GBR, NZL, USA) Q3 2013



ANNEX 2

COMMON VULNERABILITIES & EXPOSURES (CVE) REFERENCE

(S//Rel to CAN, AUS, GBR, NZL, USA) Q3 2013



**ANNEX 3
REFERENCE MATERIAL**

(S//Rel to CAN, AUS, GBR, NZL, USA) Q3 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]
[REDACTED]

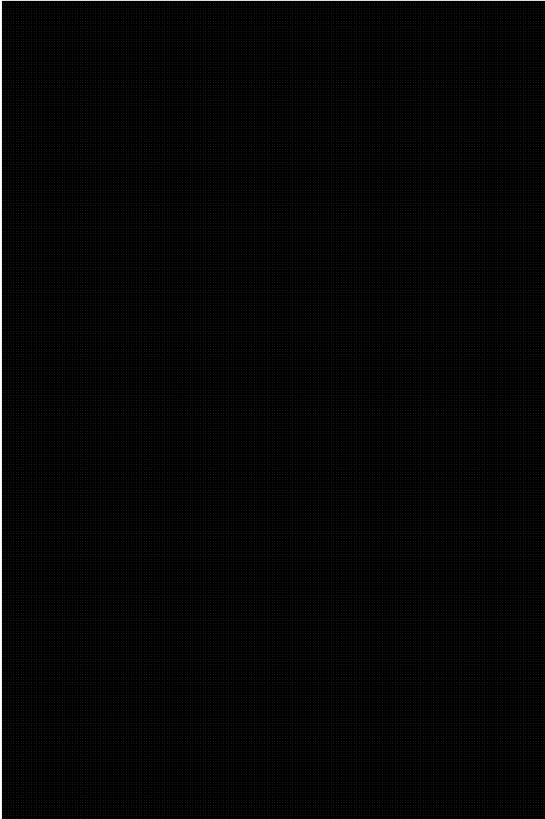
SECRET//REL TO CAN, AUS, GBR, NZL and USA

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

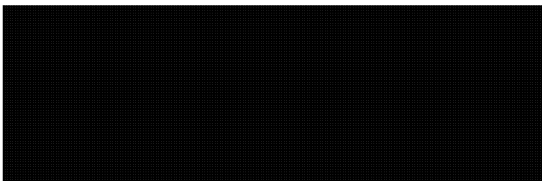
CTEC CYBER THREAT
EVALUATION CENTRE

DISTRIBUTION

NSA



GCHQ



15

CERRID File # 1348849

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

CDR-2P-Q213-02

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

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

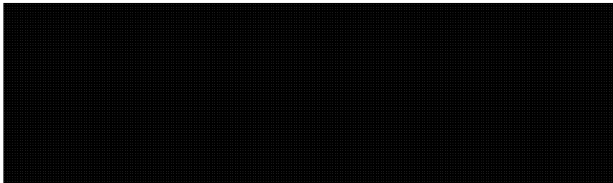
CTEC CYBER THREAT
EVALUATION CENTRE

DISTRIBUTION (CONTINUED)

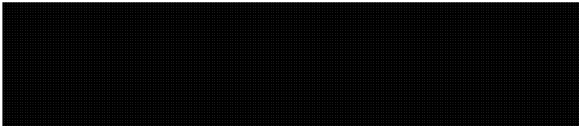
GCSB



DSD



CSIS



CSEC

John Forster, Chief CSEC,

