

SECRET//CANADIAN EYES ONLY

s.15(1) - DEF
s.16(2)(c)

From:
Sent: June-20-16 11:30 AM
To:
Cc:
Subject: 1 email, several documents

Classification: SECRET//CANADIAN EYES ONLY

The presentations attached are not only about TOR. Not sure how we would handle them. Just use the pages referring to TOR? The three decks are almost the same. Just updates. There are discussions of a capabilities and the status of their which is fairly sensitive.

I will return the initialled form to _____ for further distribution?

Cheers,



Update_Present... CSE DG Bilat CSE Bilat Timelin...
March 16, 201... March 30, 2016....

=====
=====Email talking about
TOR=====

Hi
This hash will be sent to CTEC for inclusion in their

Cheers,

From:
Sent: April-25-16 9:10 AM
To:
Cc:
Subject: RE: TOR

Classification: SECRET//CANADIAN EYES ONLY

Many people are ops this morning felt this was significant and timely for the on-going discussion over TOR ... What is the outcome a report to _____ from CTEC?

SECRET//CANADIAN EYES ONLY

SECRET//CANADIAN EYES ONLY

s.15(1) - DEF

s.16(2)(c)

Director Cyber Defence Operations/
Directeur Opérations de Cyberdéfense
Rm
BLK
GRN

From:
Sent: April-25-16 8:38 AM
To:
Cc:
Subject: RE: TOR

Classification: *SECRET//CANADIAN EYES ONLY*

Yes, the old network.

Unfortunately even if

From:
Sent: April-25-16 7:33 AM
To:
Cc:
Subject: RE: TOR

Classification: *SECRET//CANADIAN EYES ONLY*

Very sweet indeed ... we will highlight this perhaps at the Chief's Ops call this morning. So this is the network I assume.

Director Cyber Defence Operations/
Directeur Opérations de Cyberdéfense
Rm
BLK
GRN

From:
Sent: April-25-16 6:16 AM
To:
Cc:
Subject: RE: TOR

Classification: *SECRET//CANADIAN EYES ONLY*

Nice!

From:
Sent: April-22-16 2:59 PM
To:
Cc:
Subject: FW: TOR

SECRET//CANADIAN EYES ONLY

SECRET//CANADIAN EYES ONLY

s.15(1) - DEF

s.16(2)(c)

Classification: SECRET//CANADIAN EYES ONLY

FYI, found some

TOR

It's out there. ☺

From:

Sent: April-22-16 2:24 PM

To:

Cc: CDO Staff

Subject: TOR

Classification: SECRET//CANADIAN EYES ONLY

Hey

For inclusion in the next

Director Cyber Defence Operations/
Directeur Opérations de Cyberdéfense

Rm

BLK

GRN

SECRET//CANADIAN EYES ONLY

PROTECTED B

s.15(1) - DEF

s.16(2)(c)

DESCRIPTION:

TOR TOR (The Onion Router) is an anonymous network for routing internet traffic where the Zeus malware family has evolved into.

TIMELINES:

1. Internal Meeting

2. Initial Meeting

3. Technical Meetings

1. Internal meeting

- Internal briefings conducted and timelines proposed: **DATE**

2. Initial Meeting with

TOR

3. Technical meetings

TOR.

4.

PROTECTED B

s.15(1) - DEF

s.16(2)(c)

5.

TOR

TOR

TOR

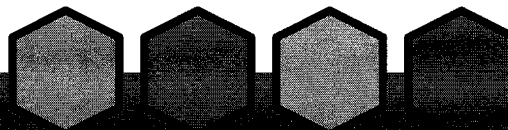
6.



s.15(1) - DEF



UPDATE



January 5th 2016

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Communications Security Establishment Centre de la sécurité des télécommunications

Canada

Agenda



s.15(1) - DEF
s.16(2)(c)

-
- Defending
- New
 -
 -
 -
- Future Bilat Topics
- Round Table

**Pages 8 to / à 9
are withheld pursuant to sections
sont retenues en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 10

**is withheld pursuant to sections
est retenue en vertu des articles**

16(2)(c), 15(1) - DEF, 15(1) - IA

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 11

**is withheld pursuant to sections
est retenue en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

TOR?



s.15(1) - DEF
s.16(2)(c)

Zeus Malware Goes 64 Bit, Includes Tor Connectivity

By Sean Michael Kerner | Posted 2013-12-12 Email Print



NEWS ANALYSIS: Zeus's new variant could be the next logical evolution of crimeware, security researchers say.

The Zeus malware family has been a common sight on the IT threat landscape for years, powering a banking fraud botnet of the same name that U.S. authorities have tried to shut down.

Zeus has now evolved.

The new version of Zeus also includes Tor connectivity, which is inseparable from the 64-bit version, Kaspersky Lab expert Dmitry Bestuzhev told *eWEEK*. Tor (The Onion Router) is an anonymous network for routing Internet traffic. "It connects to an onion domain, which means that the command and control server is well-hidden," Bestuzhev said. "Not all malware includes this functionality."

**Pages 13 to / à 14
are withheld pursuant to sections
sont retenues en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

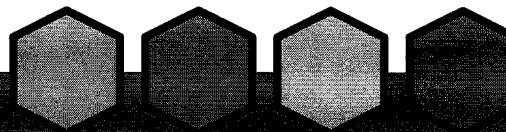
Questions





s.15(1) - DEF

CSE- [REDACTED] BILAT



March 15, 2016

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada

Agenda



s.15(1) - DEF
s.16(2)(c)

- Updates



Metrics

- Updates/Round table

Agenda



s.15(1) - DEF
s.16(2)(c)

- ◆ Updates



Metrics

- ◆ Updates/Round table

**Pages 19 to / à 21
are withheld pursuant to sections
sont retenues en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

Agenda



s.15(1) - DEF
s.16(2)(c)

- ◆ Updates



Metrics

- ◆ Updates/Round table



s.15(1) - DEF
s.16(2)(c)

TOR

- TOR (The Onion Router) is an anonymous network for routing internet traffic where the Zeus malware family has evolved into.

- CSE

GC departments
Onion Router(TOR)



Agenda



s.15(1) - DEF
s.16(2)(c)

- Updates



Metrics

- Updates/Round table

Agenda



s.15(1) - DEF
s.16(2)(c)

- Updates



Metrics

- Updates/Round table

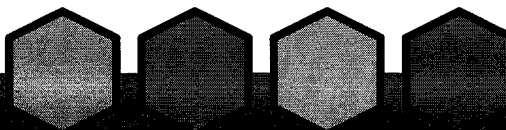
Questions





s.15(1) - DEF

CSE- [REDACTED] BILAT



2016-09-30-2016

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Communications Centre de la sécurité
Security Establishment des télécommunications

Canada

A-2016-00041-00027

Agenda



- Updates
-
-
-
- Updates/Round table

s.15(1) - DEF
s.16(2)(c)

Agenda



- Updates
-
-
-
- Updates/Round table

s.15(1) - DEF
s.16(2)(c)

**Pages 30 to / à 32
are withheld pursuant to sections
sont retenues en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

Agenda



s.15(1) - DEF
s.16(2)(c)

- ◆ Updates
- ◆
- ◆
- ◆
- ◆ Updates/Round table



s.15(1) - DEF
s.16(2)(c)

TOR

- TOR (The Onion Router) is an anonymous network for routing internet traffic where the Zeus malware family has evolved into.

● CSE

GC departments
Onion Router(TOR)

Agenda



s.15(1) - DEF
s.16(2)(c)

- Updates
-
-
-
- Updates/Round table

**Pages 36 to / à 37
are withheld pursuant to sections
sont retenues en vertu des articles**

16(2)(c), 15(1) - DEF

**of the Access to Information
de la Loi sur l'accès à l'information**

Agenda



- Updates
-
-
-
- Updates/Round table

s.15(1) - DEF
s.16(2)(c)

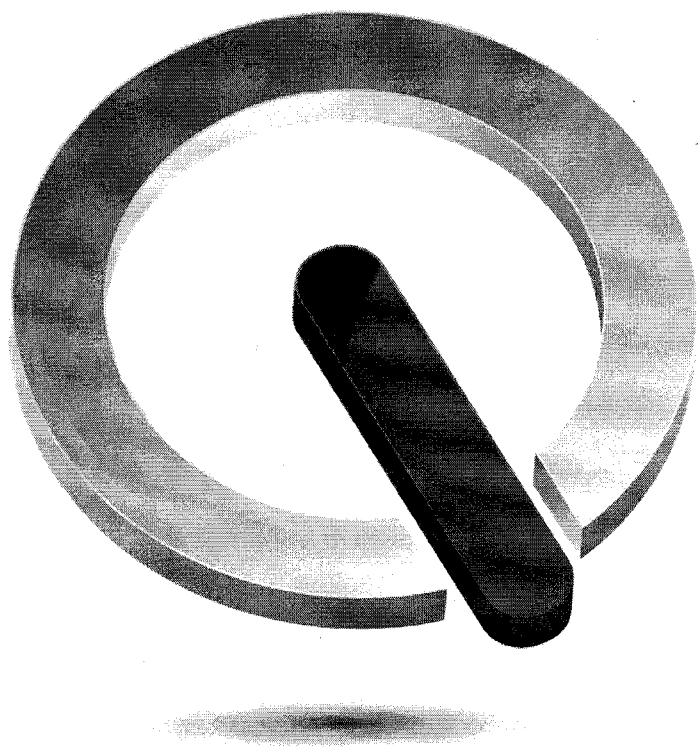
Agenda



- Updates
-
-
-
- Updates/Round table

s.15(1) - DEF
s.16(2)(c)

Questions



Communications Security Establishment Centre de la sécurité des télécommunications

Canada

TOP SECRET//SI//CANADIAN EYES ONLY

s.15(1) - DEF

s.15(1) - IA

From:
Sent: June-27-16 4:13 PM
To:
Subject: FW: Background on and

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

1st message with respect to Access to Information Act request # A-2016-00041.

From:
Sent: May-08-15 5:27 PM
To:
Cc:
Subject: Background on and

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

It's a bit more long winded than I would have liked but here is some background on under
and for

The main phenomena that was meant to address was radicalization and online extremism. It was an effort
meant to discover . It identified that could
be There were

to focus on The aim is always
displaying a combination of these

Using the Onion Router (TOR) to hide your tracks on the internet is an example.

An example where a

The information from the report was shared through a 2nd
party.

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

s.15(1) - DEF

s.15(1) - IA

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

A major concern is

Cheers,

s.15(1) - DEF

s.15(1) - IA

From:
Sent: November-19-15 10:57 AM
To:
Subject: FW: tech profiling

Classification: TOP SECRET//SI//REL TO CAN,

Do we have anything on technology?

From:
Sent: November-18-15 3:30 PM
To:
Cc:
Subject: tech profiling

Classification: TOP SECRET//SI//REL TO CAN,

Curious if we have any indicators about the type of technology used looking for the specific selectors but do we know they used

not

thanks

*Director General, | Directeur général de
Communications Security Establishment | Centre de la sécurité des télécommunications*

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

s.15(1) - DEF

s.15(1) - IA

From:
Sent: June-27-16 4:14 PM
To:
Subject: FW: tech profiing

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

2nd message with respect to Access to Information Act request # A-2016-00041.

From:
Sent: November-19-15 5:15 PM
To:
Cc:
Subject: RE: tech profiing

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

Many thanks for this... always searching for an opportunity
also establish some trends on use of technology.
Anything that you or the pick up is always welcome

where we can help . but

Tks

From:
Sent: November-19-15 3:35 PM
To:
Cc:
Subject: RE: tech profiing

Classification: TOP SECRET//SI//REL TO CAN,

Please see message below. He attended a VTC today with where provided some information on the comms usage of

Cheers,

From:

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

Sent: November-19-15 1:18 PM
To:
Subject: RE: tech profiling

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA

Classification: TOP SECRET//SI//REL TO CAN,

During the VTC mentioned was used to

From:
Sent: November-19-15 12:42 PM
To:
Cc:
Subject: RE: tech profiling

Classification: TOP SECRET//SI//REL TO CAN,

We have not seen specifics from below by the extended network (i.e. those

but has provided a summary of typical

Please let me know if you need any additional info.

From:
Sent: November-19-15 11:21 AM
To:
Subject: RE: tech profiling

Classification: TOP SECRET//SI//REL TO CAN,

On 21 October,

are used for
are by far the method of choice.

But nonetheless it illustrates that
however I believe that

Another known to be used in population;
but it's hard to assess because

although this is more among the

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

s.15(1) - DEF

s.15(1) - IA

s.21(1)(a)

From:
Sent: February-12-16 1:12 PM
To:
Cc:
Subject: RE: GCHQ-CSE Meeting (2016-02-12)

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

Howdy,

Firstly, well done team.

Second, this is a really awesome meeting summary, and I have passed it along to unchanged. So doublely well done

Cheers,

From:
Sent: February-12-16 10:36 AM
To:
Cc:
Subject: FW: GCHQ-CSE Meeting (2016-02-12)

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

I think last two paragraphs reflect the value of having such high quality analysts. I am very proud of our team right now.

"Overall, the GCHQ Leads were *very impressed* with what our team was doing, and how we were doing it

In my opinion, I believe

I think that they have seen

From:
Sent: February-12-16 10:28 AM
To:
Cc:
Subject: GCHQ-CSE Meeting (2016-02-12)

TOP SECRET//SI//CANADIAN EYES ONLY

TOP SECRET//SI//CANADIAN EYES ONLY

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA
s.19(1)

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

GCHQ-CSE Meeting (2016-02-12)

Attendees (GCHQ):

Attendees (CSE):
Just myself

Lay of the land:

headed the conversation for GCHQ...

Following a quick roundtable, the main focus/interest was heavily weighted on wanted to know about I kept having to jump back and forth with what we were doing (to answer his questions), and explaining things like the resources we have and the mandates / policies / teams / departments we work with. Operationally, I talked about

A whole section of talks revolved around and the report we released. On their end, they were are currently looking at

In regards to upcoming meetings:

Regarding

And in Canada, there was a just last week.]

Everyone was especially interested with the work we've been doing with They asked, and I provided, a detailed breakdown of what we know - how we

They

TOP SECRET//SI//CANADIAN EYES ONLY

also wanted to know what we don't know about

Because of NSA/GCHQ capabilities with [redacted] see my previous e-mail on updates), they said we can work together to provide

[redacted] and suggested that this would be a great way CSE can contribute to the community - And potentially highlight how our two organizations worked together, if we can

From our end, [redacted] wanted to know if we could assist them with some of their

[redacted] So long as they were relevant national security priorities for us. I also asked for a list of any other

Overall, the GCHQ Leads were *very impressed* with what our team was doing, and how we were doing it

In my opinion, I believe

[redacted] I think that they have seen

Cheers.

Communications Security Establishment

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA
s.19(1)
s.21(1)(a)

TOP SECRET//SI//CANADIAN EYES ONLY

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA

From:
Sent: February-12-16 1:02 PM
To:
Cc:
Subject:

Classification: TOP SECRET//SI//CANADIAN EYES ONLY

Hi

The following is a summary from what has been reported back to us from
for a workshop on
During one of his bilats, GCHQ told him about

He spent the last week at GCHQ

Thank you,

TOP SECRET//SI//CANADIAN EYES ONLY