RCMP
ROYAL CANADIAN MOUNTED POLICE

RANSOMWARE BULLETIN

Recognize, Reject and Report it!

*The incidents of ransomware in Canada are rising at an alarming rate. In 2015, Canadians were affected by **1,600 ransomware attacks a day**.[1] By September 2016, the attacks nearly doubled. Those are the known cases. Unfortunately, many incidents still go unreported.*

Bulletin 1. Version 1.1
September 2019

RECOGNIZE IT!

What is Ransomware?

It is malicious software also known as malware, which infects a computer and denies access to the system or data, and demands a sum of money to restore the information. At present, the most common form of ransomware will encrypt data. Victims will receive an on-screen alert stating their files have been encrypted or a similar message, depending on the type of ransomware. Here is an actual example: →

```
1  Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
   generated for this computer.
2
3  To decrypt files you need to obtain the private key.
4
5  The single copy of the private key, which will allow to decrypt the files, located on a
   secret server at the Internet, After that, nobody and never will be able to restore files...
6
7  To obtain the private key and php script for this computer, which will automatically decrypt
   files, you need to pay 1 bitcoin(s) (approx.. 1,200 USD).
8  Without this key, you will never be able to get your original files back.
9
10
11 ____________________________
12
13 !!!!!!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT (ALSO AUTHORIZATION CODE) :
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

PERSONAL COMPUTER USER

REJECT IT!

How can I protect myself?

- Do not click on links or open attachments in e-mails sent to you by someone you do not know.
- Do not provide personal information over the phone or online to untrusted sources.
- Install only trusted software.
- Back up your system/data regularly and keep the backups on a separate removable hard drive. Don't forget to disconnect when done. If possible, check the backup(s) from a separate computer that uses a different operating system.
- Install a reputable security software suite on all devices, including personal computers, mobile phones and tablets.
- Secure your wireless router.[2,3]
- Disable file sharing and remote desktop.
- Make sure all your software, including anti-virus software is up to date on all your devices including personal computer, mobile phones and tablets.

BUSINESS COMPUTER USER

REJECT IT!

How can I protect my business?

- Train and educate staff on good security practices.
- Do not click on links or open attachments in e-mails sent to you by someone you do not know.
- Use a reputable security software suite.
- Restrict administrative privileges.
- Back up your system/data regularly to a cloud or removable media such as an external hard drive not constantly connected to the server. If possible, check the backup (s) from a separate computer that uses a different operating system.
- Use application whitelisting to help prevent malicious software and unapproved programs from running.[4]
- Make sure all software, including anti-virus software, is up to date on all computers, servers and devices including mobile phones and tablets.
- Develop a business continuity plan and incident response plan.

1 – https://www.getcybersafe.gc.ca/cnt/blg/pst-20161205-en.aspx accessed on February 20, 2017.
2 – https://www.getcybersafe.gc.ca/cnt/prtct-dvcs/hm-ntwrks-en.aspx "Securing your home wireless network" accessed on April 04, 2017.
3 – https://www.us-cert.gov/ncas/tips/ST15-002 DHS Tips (ST15-002) – "Securing Your Home Network" accessed on April 04, 2017.
4 – https://www.asd.gov.au/publications/protect/application_whitelisting.htm accessed on April 04, 2017.

RANSOMWARE BULLETIN

PERSONAL COMPUTER USER

REPORT IT!

How should I respond?

If you become a victim, do not panic. Do not do anything further on your computer. Contact a trusted IT professional who can try to isolate the threat.

Report the incident to your local police force of jurisdiction. Please remember that every report counts and is a valuable tool for investigators.

Please also contact the **Canadian Anti-Fraud Centre** (CAFC) by reporting the incident online 24/7 at: www.antifraudcentre-centreantifraude.ca, select "Report an Incident", and the link to the "Fraud Reporting System (FRS)", or alternatively call the CAFC at 1-888-495-8501, between 8:30 am and 5 pm EST Monday to Friday.

Additional help may be found on the 'No More Ransom' website at https://www.nomoreransom.org. The site is a tool to help victims retrieve their data, and was developed by law enforcement and IT security companies globally.

BUSINESS COMPUTER USER

REPORT IT!

How should my business respond?

Do not do anything further on your computer. If available, consult your local IT department or an IT professional for assistance.

Critical infrastructure, businesses and provincial/territorial/municipal governments should immediately report the incident to the **Canadian Centre for Cyber Security** via e-mail at: contact@cyber.gc.ca, or visit www.cyber.gc.ca for more information. The Centre will assist in mitigation and prevention.

You are encouraged to open a criminal investigation into the matter by reporting the incident to your local police force of jurisdiction. Please remember that every report counts and is a valuable tool for investigators.

You may also contact the **Canadian Anti-Fraud Centre** (CAFC) by reporting the incident online 24/7 at: www.antifraudcentre-centreantifraude.ca, select "Report an Incident", and the link to the "Fraud Reporting System (FRS)", or alternatively call the CAFC at 1-888-495-8501, between 8:30 am and 5 pm EST Monday to Friday.

We strongly suggest that you DO NOT PAY THE RANSOM for the following reasons:

- There is no guarantee that your data will be recovered.
- You may be extorted for more money after the original ransom is paid.
- You can make yourself a future target.
- Extortion via Ransomware is a criminal offence, and the money you pay will be used to fund criminals and/or criminal organizations and motivate them to further victimize others.

We understand that there may be legitimate reasons for paying the ransom, such as the potential harm of not having access to the data as a result of no backup. We still encourage you to report incidents even if you have paid the ransom demanded by the extortionists.

Additional guidelines can be found at:

https://www.getcybersafe.gc.ca/

https://www.cyber.nj.gov/threat-profiles/ransomware/

Additional guidelines can be found at:

Get Cyber Safe Guide for Small and Medium Businesses:
https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

US-CERT Tips
https://www.us-cert.gov/ncas/tips

NIST (National Institute of Standards and Technology) Guide:
http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

In consultation with:

CALGARY POLICE SERVICE