New Technologies and Criminal Investigations

- One of the biggest challenges facing our legal system, is the constant evolution of technology and the myriad of ways individuals find to circumvent law enforcement.
- It has long been recognized that the speed at which technology advances has presented a continuous challenge for law enforcement investigations.
- Social networking, cloud-based services, the Internet of Things, and increasing cyber threats to personal data, company records, and critical infrastructure are just a few of the ongoing challenges.
- Cybercrime is borderless and a single investigation can lead to offenders, evidence, and witnesses in multiple jurisdictions and other countries across the globe.

Cybercrime Investigations

- Ransomware investigations are still a primary concern.

Note:

- ➢The ransomware attacks against Ontario Municipalities continues. Municipalities have been contemplating the purchase of Cyber Insurance, and if announced publicly the purchase Cyber Insurance, there have been attacks shortly after the announcement.

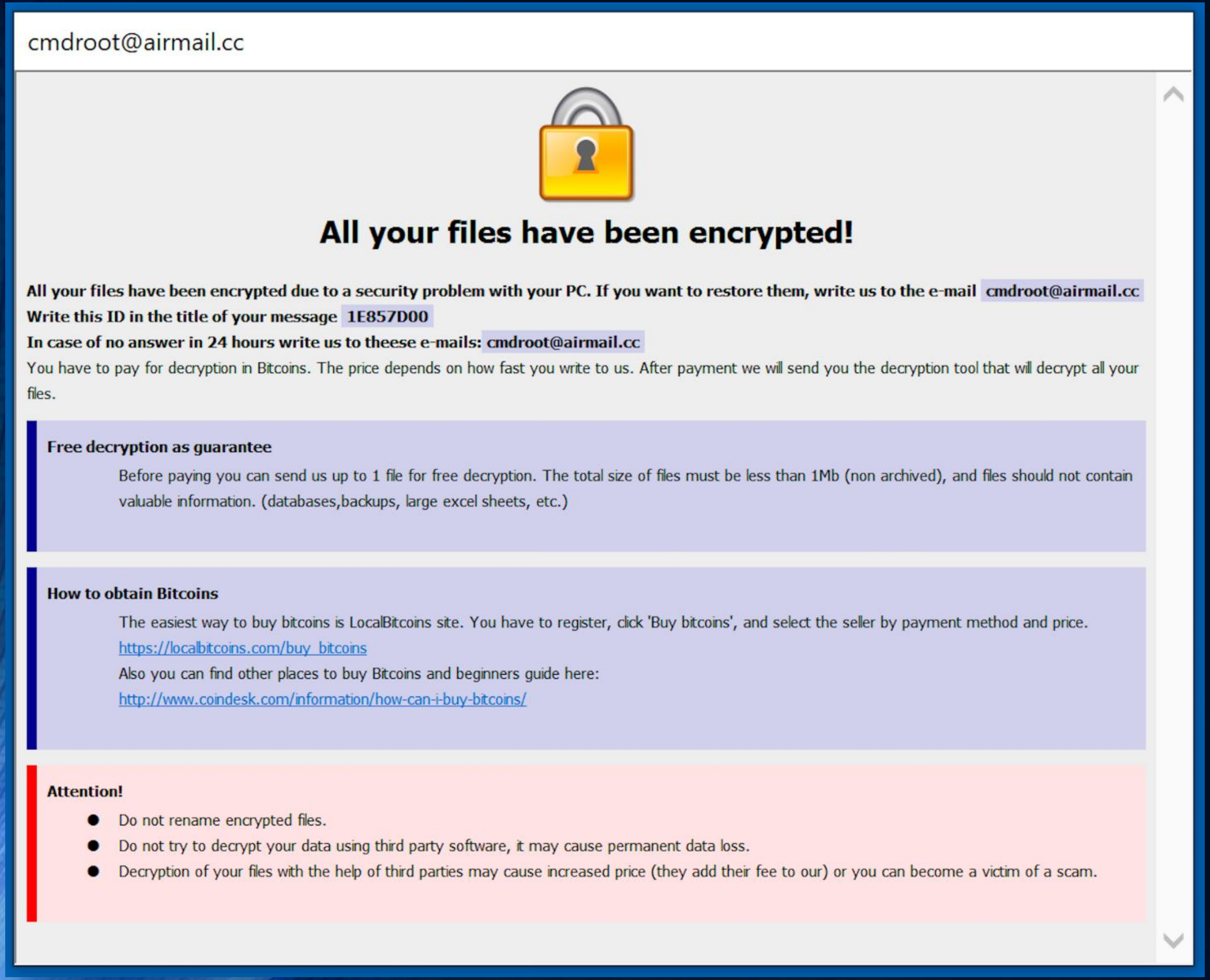
- ➢The purchase of Insurance does not mitigate the loss of important data.

- ➢Prevention is Key.

What is Ransomware:

- Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion.
- In most cases, your data is encrypted (Crypto-Ransomware) and rendered useless.
    - Note: In the latest variants, the encryption can not be broken without the decryption key
- Ransomware is frequently delivered through spear phishing emails, however many current attacks has seen Remote Desktop Protocol (RDP) used as the attack vector to gain entry into systems.
- After the victim has been locked out of their data or systems, the cyber threat actor demands a ransom payment, usually in Bitcoin.
- After receiving payment, the cyber actor will purportedly provide an avenue to the victim to regain access to the system or data.
- Recent iterations target enterprise end users, making *awareness and training a critical preventive measure.*

Ransomware Note [Dharma]



cmdroot@airmail.cc

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail cmdroot@airmail.cc
Write this ID in the title of your message 1E857D00
In case of no answer in 24 hours write us to theese e-mails: cmdroot@airmail.cc
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

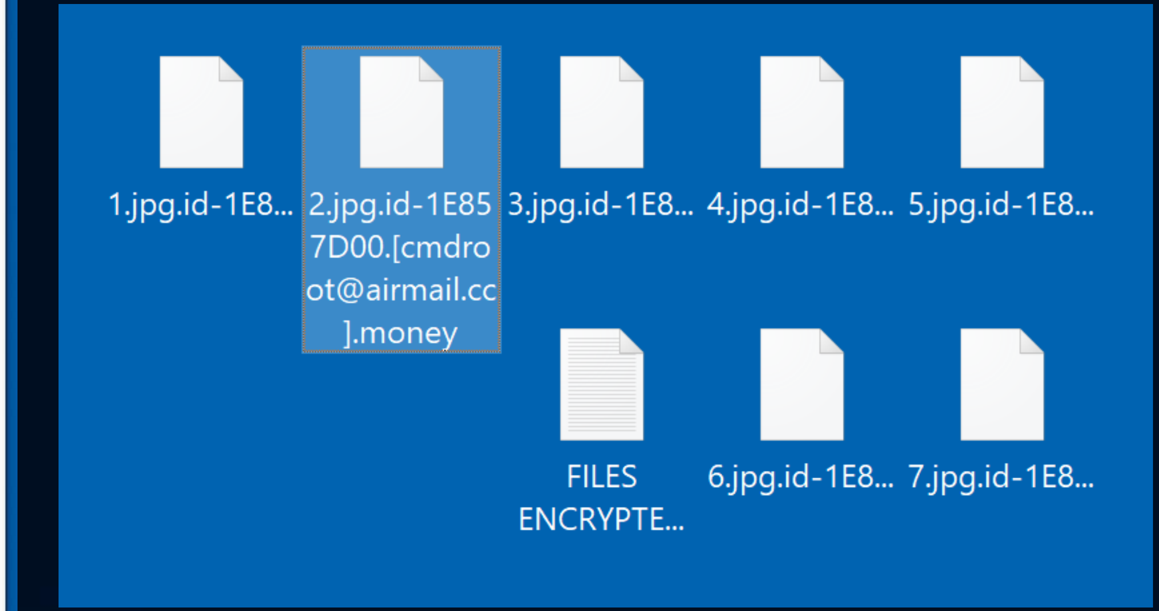
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.



How Do I Protect My Networks?

A commitment to cyber hygiene and best practices is critical to protecting computer networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups**: Do we backup all our critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?

2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?

3. **Staff Training**: Have we trained staff on cybersecurity best practices?

4. **Vulnerability Patching**: Have we implemented appropriate patching of known system vulnerabilities?

5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?

6. **Incident Response**: Do we have an incident response plan and have we exercised it?

7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?

8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

How Do I Respond to a Ransomware Attack?

- Implement your security incident response and business continuity plan.
- It may take time for your organization’s IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization’s essential functions according to your business continuity plan.
- Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.
- ***Contact law enforcement immediately***. You should to contact your local Police Service immediately to report a ransomware event and request assistance.

Do I Pay The Ransom?

There are serious risks to consider before paying the ransom.

Law enforcement does not encourage paying a ransom. It is understood that when a business is faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- **Paying will encourage this criminal business model.**

Note: Publically stating ransom will not be paid has discouraged attacks within the same sector.

Reporting

As with any other crime, a cybercrime should be reported to the local police detachment.

- Report as soon as possible
- Describe what systems are affected, the type of data affected, and how they are affected
- Describe the level of jeopardy: # of employees affected; Status of data backups and ability to recover; Impact on the operations of the organization

Report the specifics of the incident:

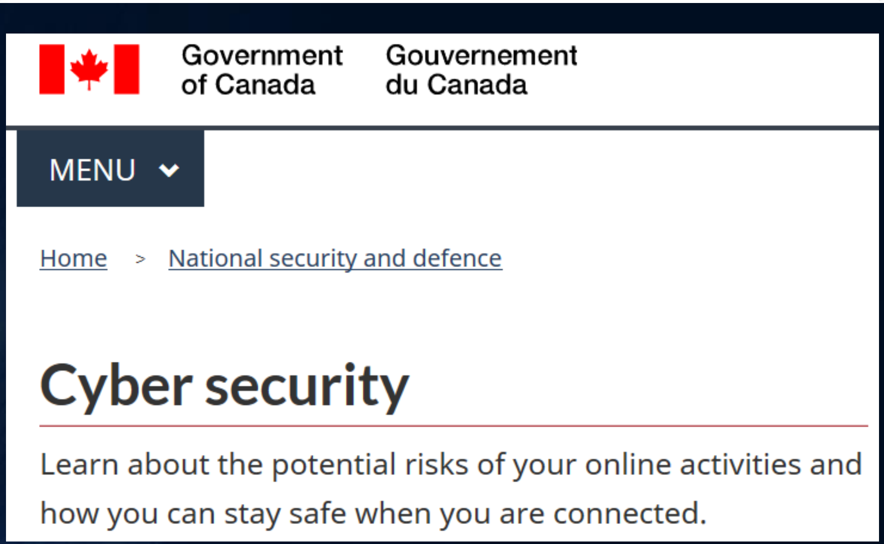
- When was the attack first noticed\reported ?
- What actions are being taken to correct the issue ? Is there a 3rd party assisting ?
- Who is the contact person for this incident ?

Preserve any digital evidence such as: email addresses, the ransom note, suspicious or malicious files, event log files, computer system affected, etc.

Law enforcement’s role is determining attribution (who did it). The mitigation and remediation of the computer systems is the victims responsibility. Law enforcement will work alongside the victim organization and 3rd party security company to collect any potential digital evidence.

Good Resources

Canadian Anti-Fraud Centre
CAFC
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT.
LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.
Competition Bureau Canada
Bureau de la concurrence Canada
Royal Canadian Mounted Police
Gendarmerie royale du Canada
Canadä

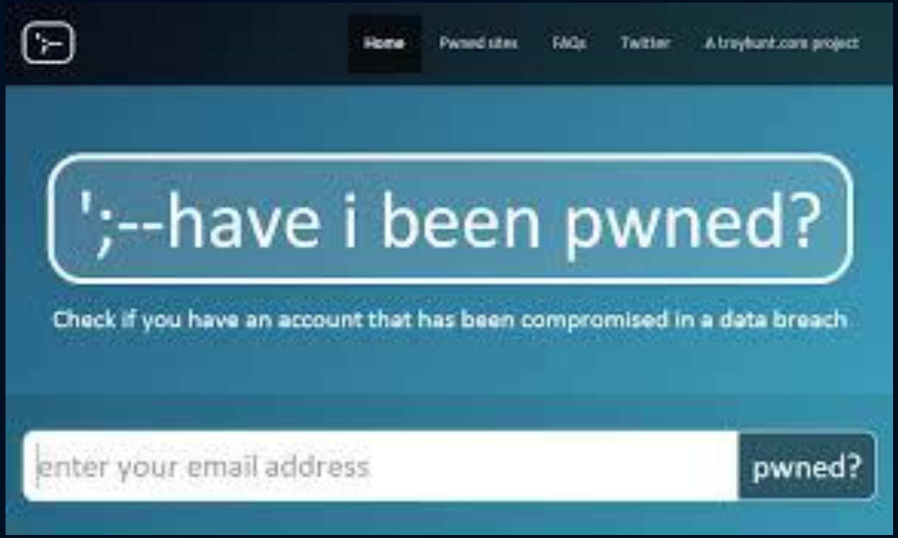


Cyber security

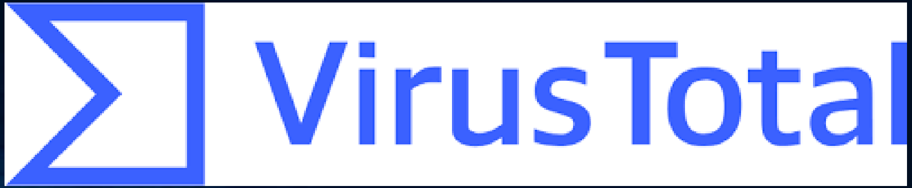
Learn about the potential risks of your online activities and how you can stay safe when you are connected.

https://www.canada.ca/en/services/defence/cybersecurity.html

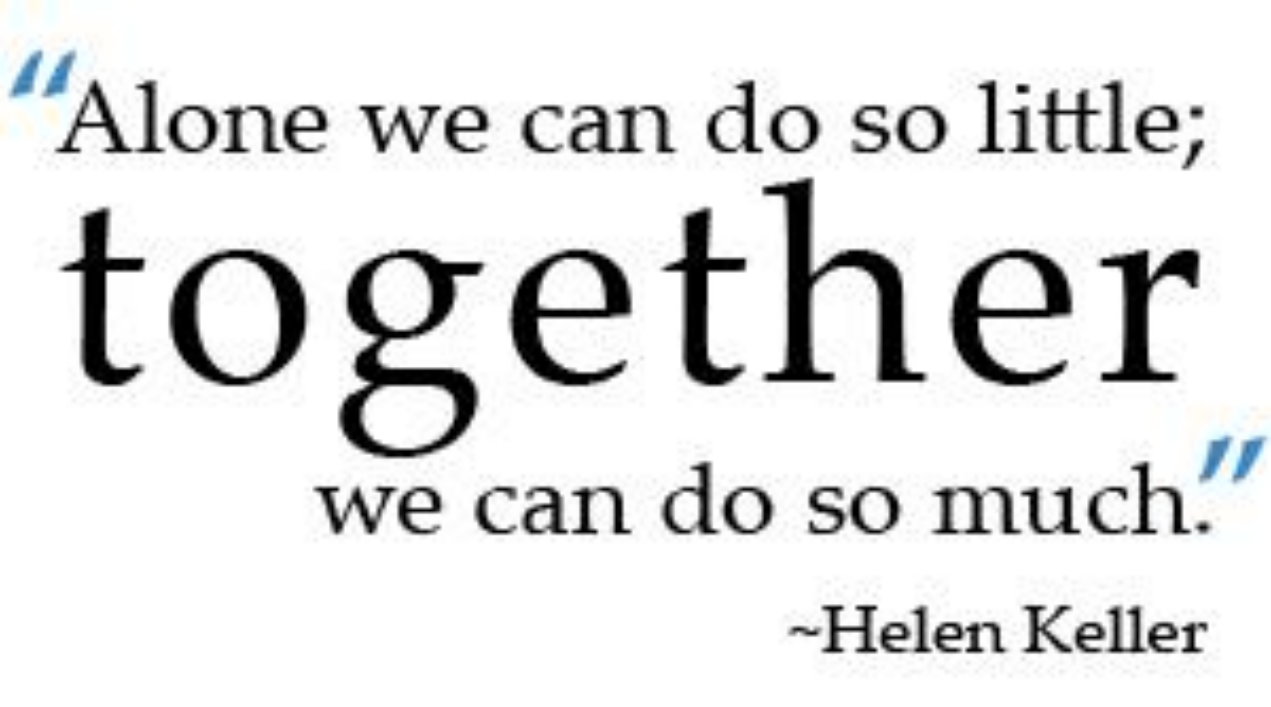
https://www.cybersec101.ca/



Check if you have an account that has been compromised in a data breach



Share the Knowledge!



"Alone we can do so little;
together
we can do so much."

~Helen Keller