Ministry of Health Services

doctors of bc

Doctors Technology Office (DTO): Technical Bulletin

Ransomware – What Should I Do?

DTO TB - #17-001	**Objective:** Reduce impact due to ransomware.

Brief Description (Non-Technical):

Ransomware, are a type of malware that is created with the intent to extort money from victims. There are two types of ransomware:

- "Locker Ransomware" - locks the interface restricting systems access.
  - Limited computer usage, except the ability to pay.
- "Crypto Ransomware" - locks / encrypts files restricting data access.
  - Full usage, but no file access.

With both methods there is an on-screen alert to inform users that their systems or data have been locked/encrypted and that they have a limited time to pay the ransom before everything becomes unrecoverable. The ransom amount varies greatly, but for individuals, the average amount is between $200US to $400US, to be paid in virtual currency such as Bitcoin.

Authorities encourage individuals or organizations to seek alternate solutions instead of paying the ransom. Paying the perpetrators of the crime only encourages this type of criminal activity. In addition, paying does not guarantee that your data will be released.

Potential Impact:

Ransomware has the following potential impacts or consequences:
Temporary or permanent loss of sensitive information.
Significant disruption to regular workflow.
Financial losses (restore systems/files, ensure the systems are now clean, downtime).
Potential harm to an organization's reputation.

Tech News World recently reported that 72% of companies infected with ransomware could not access their data for a minimum of two days, and 32% could not access their data for five days or more. The costs of downtime often exceed the cost of ransom.

Pro-Active Solutions:

Ransomware is often spread through:

- Phishing emails that contain malicious attachments.
- Malicious or infected website.
- Social media such as Web-based instant messaging applications.
- Vulnerable Web servers which may be exploited and used to access into your network.

Author: Patrick Wong
Original Date Created: 2016-12-12

How Did I Get Infected?

- Social Engineering:
  - Opening phishing emails that entice the user to click on a link.
  - Downloading or opening a malicious attachments.
  - Redirection from adult content sites, media piracy sites, gaming sites etc., to malicious sites.
  - Malvertisement for on-line shopping. These sites use security and encryptions similar to legitimate sites.
- Layered Attacks:
  - Systems already compromised are sold to ransomware criminals.
  - Systems with undetected malware called "zombie" machines can stay dormant for future attacks.
- Self-Propagation
  - Fake software updates that have embedded "Trojan Horse" ready to infect systems. For example:
    - Fake Adobe Flash updates.
    - Fake Flash updates.
- Self-Propagation
  - Ransomware can infect additional computers on your network via SMS messages or user's contact list.

Preventative Measures:

- **Have a good backup and recovery plan**.
  - **Test your backup often.**
  - **Isolate your backup from your network.**
- Application WHITE LISTING is one of the best security strategies.
  - Only allow WHITE LIST (your personal AUTHERIED list of software) applications to run.
  - Do not login as the "administrator", but as a limited user.
- Keep all software up to date, including operating systems and device drivers (software programs for hardware).
  - Outdated software such as Windows XP have known vulnerabilities.
- Use high-quality, purchased versions of anti-malware software.
- Avoid enabling and running macros from email attachments.
- Save and scan all email attachments for malware before execution. (TRUST NO ONE.)
  - Do not run or open attachments directly from emails (save a copy to your hard drive first).
  - Follow safe email hygiene practice. Recognize and Avoid Email Scams.
  - Follow safe Internet Web browsing practices. Good Security Habits and Safeguard Your Data.
- Never click to follow unsolicited links or redirections when surfing the Internet.
- Never click to follow unsolicited links from within emails (Do your own search).
- Avoid Social Engineering and Phishing Attacks.
- **Visit nomoreransom.org**

Author: Patrick Wong *Original Date Created: 2016-12-12*

Another option that is becoming more popular, as Internet performance improves, is to use the Cloud. Datacentres are better equipped to protect their clients' data than individuals, but it's still a cat and mouse game. At this time:

- Not Protected: Software as a Service that appears as a drive letter - as a part of your network.
  - i.e. Dropbox, One Drive, Google Drive etc.
- Protected: Applications where end users access their data through browser authentications.
  - (ASP) Application Service Provider. EMR (electronic medical record) vendors that have deployed their secure ASP model.

However, WHAT IS NOT VULNERABLE TODAY MAY BECOME VULNERABLE TOMORROW.

Mitigation:

- Plan, plan and plan. Take appropriate steps to limit the damage; do not under estimate this critical step.
- Train staff to spot and avoid phishing emails.
- If possible, segment systems where possible (subdivide your local network).

While we still have to use passwords, make them difficult for hackers. (refer to TB 16-004)

Reactive – Check List:

If you find you have fallen victim of a ransomware attack:

1. Stay calm and do not panic especially if you have a good backup not attached or isolated from your network.
2. Call your local IT support vendor.
   a. Do not randomly turn your computer off. This may make things worse. You must first isolate the infected systems from your network and the Internet.
3. Use the Internet and learn about the ransomware you are dealing with.
   a. Visit nomoreransom.org.
   b. Enter the threatening phrase into a search engine to learn how others are dealing with this.
   c. Are there free decryption tools that can be used to restore your systems?
4. Do not let those messages scare you into paying too early.
   a. "Your computer has been infected with a virus. Click here to resolve the issue."
   b. "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $500.00 fine."
   c. "All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data."

Paying does not guarantee that your files will be restored, and that there is no further infection.

<u>Other Factors to Consider</u> (when paying is the only solution):

Extortionists' choice of payment is usually some form of "crypto-currency" such as Bitcoin – a digital, virtual currency. Unlike PayPal which is linked to a credit card or a bank account, Bitcoin is money. Although it's virtual money held in a Bitcoin "wallet", it's one application working with another application holding people's money. There is no issuer and no Federal Reserve to track all transactions or control the value of these currencies.

- Bitcoin value does fluctuate like money exchange between currencies.
- Bitcoin offers no protection and is untraceable.
    - Victim have to go to Coinbase, use real money to buy bitcoins to be placed in your Bitcoin Wallet, then move those bitcoins from your wallet to the extortionist's wallet.
    - Bitcoin is completely unregulated.
- Your account can be exploited.
    - When there isn't a Bitcoin ATM, you'll need to use a Bitcoin exchange. The exchange will require a bank account and or a debit card.

Bitcoin exchanges are notorious for being hacked. Mt. Gox, went bankrupt after it was hacked in 2014, losing an estimated $450 million worth of its customers' bitcoins.

<u>To reduce the risk, open a temp bank account with the money to buy Bitcoins, and then terminate the account.</u>

Buy extra Bitcoins to avoid delay of not meeting extortionist's demand.

- Bitcoin value fluctuates – did you buy enough Bitcoin to meet the extortionist's demand?
- Once you paid by Bitcoins, your money is gone, the attacker is gone. What if they cannot release your data etc.?

(Smart attackers will not take your money and run, but amateurs who are using a free version or someone else's ransomware may not have the skill to release your data intentionally or unintentionally.

If you must pay, consider your options carefully.

<u>Background:</u>

Ransomware began in the early 1980s. Those early versions did not tamper with data, but used scare tactics to extort money. Not until 2006 did ransomware that impacted data access become prolific. And last year, security experts named 2016 the year of ransomware and digital extortion.

Today, ransomware gains access to computer systems, infecting them, making either these systems or their data inaccessible. Kevin Bottomley, OpenDNS Seucrity Analyst, found that the infection to encryption time can be less than three minutes. In addition, extortionist limit the time available to pay, after which the data may be permanently lost. In order to regain access, owner must pay a ransom, typically in some kind of untraceable cyber currency.

Brian Contos, VP and Chief Security Strategist at Securonix said, "[Ramsomware] is a volume business.

It's simple, relatively anonymous, and fast." Ransomware is highly profitable to criminals. It's big business with quick payoff and little to no risks to the racketeers. Victims pay criminals directly, and often, the transactions happen within hours in untraceable cyber currency.

It's spreading like the plague.
&
Healthcare organizations must know that they ARE a target and will be attacked.

Details and Additional Information (Technical):

Call your local IT vendor and get professional help.

Due to the profitability of ransomware, new generations of preventative measures and counter measures are being developed and deployed continually. We will continue to monitor and update our information going forward.

Doctors Technology Office, 604-638-5841, dtotechsupport@doctorsofbc.ca

Resources:

- ID Experts:
  - Breach Essentials (What, When and How to Defend Yourself
  - Ransomware 101 (What to Do When Your Data is Held Hostage
- Nomoreransome.org
- Gartner Reports: Use These Five Backup and Recovery Best Practices to Protect Against Ransomware
- Study: Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2016:
- Verizon 2016 Data Breach Investigations Report:
- 12 Steps to a Successful Data Breach Response Guide: Link1; Link2
- Breach Response Buyer's Guide:
- YourResponse™ Product Datasheet:
- MyIDCare™ Product Datasheet:
- The Growing Threat of Ransomware, PG Mag:
- 2016 Threats and Predictions, McAfee Labs:
- The ICIT Ransomware Report, ICIT:
- The Cost of Phishing & Value of Employee Training, Wombat Security:
- Please Don't Pay Ransoms, FBI Urges, ISMG: Data Breach Today:
- Bitcoin Converter, CoinDesk:
- The Cyber-Crime Super Highway - A Tour of the Dark Web:
- Ransomware in Healthcare - Where the Stakes are Higher:
- Fight Fire WIth Fire - Grasp the Economics of Cyber Crime: