Yukon
Information
and Privacy
Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

RANSOMWARE ADVISORY

Ideas for individuals, businesses & public organizations – how to manage the risk

What is ransomware?

Ransomware is a form of malicious software (malware) that installs itself on an electronic device or system, including smartphones, tablets and computers, and encrypts the entire hard drive, or specific files, and then demands a ransom be paid before the information is decrypted. Ransomware may also encrypt files that are located on network drives mapped to an infected device or system. More importantly, attackers may access information stored on a device or system during the course of an attack.

Ransomware typically spreads via “phishing”. This is when an email or text message is sent with an attachment or link containing malware. The malware is installed when the link or attachment is opened, or when offered software is installed. Ransomware on one device or system may spread to others through network vulnerabilities or additional phishing emails from compromised accounts.

Recent developments

Variations of ransomware exist to attack most operating systems, including Windows, Linux, Android and iOS (Apple). Publicized ransomware attacks have occurred in Canada, including at hospitals, universities, businesses and on thousands of personal devices. In November 2019, Nunavut’s territorial government computer infrastructure was crippled by ransomware. In late 2019, LifeLabs Medical Laboratory Services suffered a breach of its systems and although only limited details have been provided about how the breach occurred, what has been publicized suggests it was a ransom-based attack. This is because personal health information (PHI) that was stored in its systems was held for ransom and used to force payment from LifeLabs. In January 2020, Saskatchewan’s eHealth system had some of its files encrypted by ransomware.

A word of warning for governments and organizations

There are typically two strategies that cyber criminals use for ransomware attacks. The first strategy is quantitative, putting out as many phishing emails and phishing links as possible, for example on social media, without discriminating between targets. Organizations that have limited security controls in place to defend against such attacks are likely to fall victim to this. The second strategy is more targeted. In these cases, the attackers have a specific interest in attacking a certain organization and they actively seek to gain access to this network by using, for example, credential stuffing attacks[1] and targeted phishing campaigns (spear phishing), or by exploiting network vulnerabilities. Organizations targeted in this way include those known to hold valuable personal (health) information, such as healthcare organizations, governments or other organizations. When any organization is infected by an attack under the first strategy, it indicates to an attacker that the organization is vulnerable and is considered to be 'low hanging fruit.' An attacker who discovers low hanging fruit will in some cases target similar organizations in anticipation of similar vulnerabilities, such as appeared to occur in 2018 and 2019 when numerous municipalities were subjected to ransomware attacks.[2]

Ransomware attacks evolve. Until recently, it was common for attackers to encrypt information on a system and demand a ransom to decrypt the information, with the threat of destruction in a specified timeframe. Now, attackers not only encrypt information on a system, they also steal information that is of interest to them[3]. It is important to note that personal health information (PHI) is more valuable to attackers than credit card information, because it trades for higher prices on the dark web.[4] Credit card numbers can easily be replaced, whereas PHI is inherent to a person and for the most part cannot be replaced.

Other variations include breaching a database, stealing the information and holding it ransom[5], and ransomware attacks against cloud service providers[6].

---

[1] https://www.owasp.org/index.php/Credential_stuffing
[2] https://hicksmorley.com/2019/10/09/municipalities-are-under-threat-of-ransomware-attacks-are-you-prepared/
[3] See https://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/ and https://www.us-cert.gov/ncas/alerts/TA16-091A for examples
[4] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
[5] Although not technically a ransomware attack, as no encryption techniques are used, many characteristics (motive, most exploitation techniques, consequences) are the same as with a conventional ransomware attack.
[6] https://www.zdnet.com/article/cloud-based-virtual-desktop-provider-hit-by-ransomware/

Advice for users of personal and business devices

Ransomware can hit both your personal devices and company-issued devices. Often, a ransomware attack results in a privacy breach. As the intruders access the information stored in a system to encrypt it for ransom, they often also scan for valuable data which commands a high price on the dark web. This may be personal information, financial information such as credit card details, user names, email addresses and passwords to log into financial services or credit card linked accounts[7], and, as noted above, personal health information. If your business device has been compromised by ransomware, it is safe to assume it has also disclosed any information stored on it, unless your IT department can prove that no data was extracted from the network or local disk. If a personal device has been encrypted by ransomware, it is advisable to preventatively change any passwords you might have stored on that device (for example, online banking, webmail or e-commerce website passwords stored in your browser).

To prevent a ransomware attack from occurring

- Make sure you follow training provided on information security practices, so that you are aware of how to prevent your computer from becoming infected. If your workplace does not provide training, read up on it online and educate yourself[8].
- Know how to recognize a phishing email. Do not open links or attachments from unverified sources.
- Avoid links to log-in portals or software via advertisements on social media or websites. They might re-direct you to a fake website, owned and operated by cyber criminals.
- Avoid pirated software and offers for ‘free’ viewers for movies or series. Both are known carriers of ransomware (and other malware).
- Verify and bookmark in your browser all websites that require you to log in. Use only these verified links to provide credentials to a website. This practice helps protect you from accidentally entering credentials on a fake login page via a malicious link in your email or in search results.
- Do not install software on your corporate devices and do not add plug-ins to your browsers on your corporate devices. These actions should be blocked by your IT department. Ask IT to install any software or plug-ins for you, and ask if IT has verified that these software or plugins comply with security and privacy policies. For your personal device, only install software and plug-ins from official sources and stick to software developers with a good reputation. Do research on the software before you install it[9], especially for devices using Android[10].

[7] E.g. amazon, ITunes etc. Any service that stores credit card information and enables you to purchase goods or services.
[8] Good free training in the form of a quiz is offered on https://www.isdecisions.com/user-security-awareness/
[9] https://www.gnu.org/proprietary/proprietary-back-doors.html
[10] https://forensics.spreitzenbarth.de/android-malware/

- Do not put media, such as USB sticks, from unverified sources (provided by someone from outside your organization or found around the office) into your devices. If necessary, ask IT to open USB sticks in a sandboxed[11] environment.

To control damage after an attack has occurred

- Immediately disconnect your device from the network (Wi-Fi and/or LAN cable), disconnect Bluetooth and attached devices such as USBs, phones and external hard disks. If done in a timely way, this may contain the spread.
- Report the incident to your IT department as soon as possible.

Advice for management

- To prevent ransomware outbreaks from happening, the management team should champion a workplace culture that encourages awareness of information security and privacy risks and that gives clear priority to attending relevant training, taking part in practice routines and obtaining education in these fields. This is a part of corporate due diligence. Neglect is very likely to cost the organization in the long run, either in money from lawsuits, damage to IT assets, damage through disruption of business processes or damage to reputation. In the case of a successful ransomware attack, all four types of costs are distinct possibilities.
- With the help of your IT staff, perform a risk assessment regarding the risk and impact of a ransomware attack. An assessment like this can be part of a broader risk management program for your organization[12]. Doing a risk assessment will turn unknown into known risks, inform you of your legal obligations, potential damages from incidents and costs of mitigations to prevent the risk from materializing.
- Ask if IT staff are making sure the recommended measures below (see *Advice for IT departments*) are implemented. If they do not implement certain measures, make sure you know why, what the risks are and that you are willing to accept these risks. Document risks, their mitigation or acceptance, as proof of due diligence.
- Make sure all personnel, including IT and management, are educated regarding their organizational role in the case of ransomware attacks and privacy/security breaches in general. Empower IT to provide the required technical training to all employees and management.
- Know when a security incident also constitutes a privacy breach, and when a risk of significant harm (ROSH) to individuals exists as a result of the breach. A ROSH will be found to exist if there is a *possibility* that a breach may result in any kind of harm that qualifies as significant, including 'bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property', or any other similar type of harm (e.g. identity theft or fraud).
    - Health care custodians must consider if the intrusion presents a ROSH. If it does, under the *Health Information Privacy and Management Act* (HIPMA), the custodian

[11] A sandboxed environment separates the USB stick from the rest of the system, negating the risk of infection through the USB stick. A properly configured virtual machine or live CD may function as a sandbox. Also see https://geekswipe.net/technology/computing/how-to-safely-open-untrusted-usb/

[12] http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf

must notify the individuals affected about the breach. Under HIPMA, the Office of the Information and Privacy Commissioner (OIPC) must also be notified. More information can be found on the Information and Privacy Commissioner website here.

- Public bodies are not required to report breaches to the OIPC under the current *Access to Information and Protection of Privacy Act* (ATIPP Act) but some public bodies are bound by policy to do so, if a ROSH exists. All public bodies are encouraged to give notice of the breach to individuals affected, so they can protect themselves against the harmful effects of the breach. We also encourage public bodies to contact the OIPC for advice, including how best to notify affected individuals and prevent breach recurrence. Under the revised ATIPP Act (expected to come into force in 2020), reporting will be mandatory when a ROSH exists.
- Businesses may need to report a breach to the Office of the Privacy Commissioner of Canada.[13]

Advice for IT departments

- Train the entire organization from top to bottom regarding the roles and responsibilities of employees in case of a ransomware outbreak.
  - Management should champion information security and privacy in general and give clear priority to employees attending training.
    - The requirement for employee training should be in policy and made mandatory.
    - The training should be designed to ensure that employees are informed about the risks associated with ransomware to the organization and the measures employed by the organization to mitigate the risks.
    - The training should include information about phishing, secure web usage, etc. to prevent ransomware outbreaks, and adequate response if an outbreak occurs (i.e. disconnecting, reporting immediately).
  - Users, as the first line of defense against ransomware threats, should be trained routinely on how to prevent falling victim to a ransomware attack.
- Ensure a ransomware incident response plan is in place and train multiple employees on the plan to facilitate an adequate response in case of an outbreak. Practice the plan periodically, especially when there are new employees. See the *Further reading* section below for ideas for the response plan.
- Ensure there is a patch management policy and audit its effectiveness with the help of tools such as vulnerability scanners.
- If you are using a cloud service provider, make sure it has adequate protection against ransomware attacks.
- Whitelist software applications that need to run on machines. Disallow users from installing software, even under user privileges, and from installing plugins. For example, Flash is a known ransomware vector.
- Give front-line employees (for example, those providing intake, customer service and reception services) a sandboxed environment for opening email and files from file transfer

[13] https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

services that they receive via the internet. Train these employees on verifying the safety of the download before taking it out of the isolated environment or have a control in place that keeps the attachments in the isolated environment.

- Back up your systems and make sure your backup systems are sufficiently isolated, so that they do not get hit by the same ransomware attack for which they are a recovery control. Test the "restore" functionality of backups periodically to have assurance that you can use them when needed.
- In addition to a firewall, use email filters, IDS/IPS and endpoint protection. Consider using specific ransomware detection and prevention products or endpoint protection that incorporates this functionality.
- Have some form of network access control in place. Restrict by policy *and* via technical controls what devices connect to your network as they may be carriers or vectors for ransomware if not properly onboarded according to the organization's standards.
- Avoid using administrator accounts for general use on a device. Administrator accounts that are exploited by ransomware cause a wider spread of the infection.
- Disable SMB v1 (as much as possible). This helps prevent some ransomware strains from spreading within your network. It is also highly recommended to block all outgoing SMB traffic from leaving your internal network, as this can indirectly result in ransomware attacks (for example, via SMB credential harvesting attacks)[14].

Obligations of organizations regarding compliance with privacy legislation and regulations (HIPMA, ATIPP Act and PIPEDA)

Yukon's privacy laws (HIPMA and ATIPP Act) require reasonable steps to be taken by public bodies and health care custodians to protect against the risks to personal information or personal health information caused by a ransomware attack. Because ransomware attacks result in the loss of and/or unauthorized access to information and potentially its integrity, adequate protection is a mandatory requirement under both Acts. If a breach does occur, public bodies and custodians can contact the Office of the Information and Privacy Commissioner (OIPC) for guidance on handling the privacy breach. Custodians have an obligation to notify the OIPC of any breaches that pose a ROSH to the individuals involved.

Businesses that are not health care custodians are not subject to Yukon's privacy laws and need to comply with mandatory breach reporting requirements under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). They must contact the Privacy Commissioner of Canada's Office if personal information is affected and a real risk of significant harm exists.[15]

[14] https://www.syxsense.com/server-message-block

[15] https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Further reading

https://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf

https://secureops.com/ransomware/ransomware-attacks-2019/

https://www.nomoreransom.org

https://www.cisecurity.org/white-papers/security-primer-ransomware/

An example of an incident response plan for medium to large organizations:

https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-incident-management/documents/cyber-incident-response-ransomware-playbook/cyber-incident-response-ransomware-playbook/govscot%3Adocument/Cyber%2Bincident%2Bresponse%2B-%2Bransomware%2Bplaybook.pdf

This document was updated and issued in January 2020 as an informative advisory intended to assist in understanding ransomware attacks and how to manage associated risks, in the context of Yukon's two privacy laws, the *Access to Information and Protection of Privacy Act* (ATIPP Act) and the *Health Information Privacy and Management Act* (HIPMA). This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the ATIPP Act and HIPMA, please read the Acts and regulations in their entirety. This document is not binding on Yukon's Information and Privacy Commissioner.