CYBER STRATEGY
From Frontline to Online

Ontario Provincial Police

Cyber Operations Section
Investigations and Support Bureau

CYBERCRIME ALERT

Ransomware (Hack/Virus)

ISSUE

In recent months there have been several ransomware (hack/virus) attacks on businesses and municipal government offices within Ontario. The purpose of this alert is to inform Ontario municipalities of this recent trend, providing background details and information on handling ransomware incidents.

WHAT IS A RANSOMWARE ATTACK?

A ransomware attack occurs when a cybercriminal infects a victim's computer systems with malware that encrypts the data on those systems making them inaccessible and unusable without a decryption key. The cybercriminals will then demand some sort of ransom (usually in Bitcoin) in exchange for the decryption key. There are many types of ransomware that are distributed in various ways. The most common methods of infection begin with a phishing email or direct hacking of a vulnerable computer system.

WHO IS BEING TARGETED?

Everyone is a target, but individuals tend to be targeted by mass-market ransomware campaigns, while businesses and government offices tend to be the victims of more targeted attacks. Recently in Ontario, there has been a number of attacks on businesses and municipal government offices.

WHO SHOULD I CONTACT FOR ASSISTANCE?

- Victims of ransomware attacks should contact the police of jurisdiction.

WHAT INFORMATION SHOULD BE PROVIDED?

Information provided to your local police service can then be provided to the O.P.P. Cybercrime Investigations Team to assist in identifying the particular family and versions of ransomware impacting Ontario. This information should include:

- A screenshot/photograph of the ransomware demand
- A screenshot/photograph of the encrypted files including full file name and extension
- Any contact email address provided by the attackers
- Any bitcoin wallet addresses provided by the attackers

WHAT SHOULD BE DONE TO PREVENT A RANSOMWARE ATTACK?

IT technicians of private and public entities should constantly assess and invest in the security of their computer systems. An integral part of prevention is to ensure proper offline backups of computer system data, strong password policies, and cyber security education and awareness for their employees.

DOES THE OPP SUPPORT PAYING THE RANSOM?

Individuals or businesses that receive a security or financial threat must determine for themselves whether a ransom should be paid. The OPP does not support paying ransomware attackers, as it only encourages further criminal activity, and there is no guarantee that payment will restore the encrypted data. That being said, companies and individual victims should address threats based upon the nature and severity of the threat and only after carefully considering the best interests of the individual or company’s employees, stakeholders and shareholders. Regardless of the decision made by the municipality, business, or individual, the OPP strongly encourages reporting ransomware incidents to your local police service.