AMINA
CORP.CA

Data Protection Advisory: CryptoLocker Ransomware

The Canadian Cyber Incident Response Centre (CCIRC) has issued a Cyber Alert regarding CryptoLocker Ransomeware.

What is the Risk?

CryptoLocker ransomware prevents access to files on infected computers and networks by encrypting files and then demanding that victims pay a ransom in order to regain access to their data.

Once a computer is infected with this malware, a pop-up window appears demanding a sum of money, usually between $100 and $300, paid via GreenDot, MoneyPack or Bitcoins. The victim is then given a window of 72 to 100 hours to pay the ransom, and told that they will lose the ability to decrypt their files when the time limit is reached.

Cryptolocker encrypts files on the local computer, and can also encrypt files within shared network drives, USB drives, external hard drives and even some cloud storage drives. This means that if the malware infects one user who has access to shared file drives within an organization's network, it is possible that all those files might become encrypted. The greater the access, the greater the risk that more files will become inaccessible.

How Does the Problem Occur?

The primary means of infections is when a user clicks on a link or opens attachments in phishing e-mails. Subject lines used by attackers include:

- Payroll Received by Intuit
- ADP RUN: Payroll Processed Alert
- Payroll Manager Payroll Invoice ADP RUN
- Annual Form - Authorization to Use Privately owned Vehicle on State Business
- Payroll Processed Alert Annual form ACH Notification
- DNB Complaint - (Number)
- Voice Message from Unknown Caller
- We have received your secure message
- Payroll Department
- UPS, DHS and FedEx
- American Express
- Administrator@<companydomain>
- Outlook Settings .zip file attachment
- Company Report .zip file attachment

For more information about practical ways to protect privacy and reduce risk, visit www.AMINAcorp.ca or contact us by email at info@AMINAcorp.ca or by phone at +1.403.254.4376 for a private conversation.

• Data Protection • Privacy • Information Risk Management •
• pragmatic • trustworthy • reliable • secure • dedicated • ethical •

Global Headquarters
Suite 330, Unit 440
10816 Macleod Trail SE
Calgary AB Canada T2J 5N8
Telephone +1.403.254.4376
www.AMINAcorp.ca

Data Protection Advisory: CryptoLocker Ransomware

What to Do?

If a ransomware infection occurs, CCIRC does not recommend paying the ransom. Even if users pay the ransom and regain their data, there is no guarantee that the malware has been removed or won't re-infect the computer at a later date. Instead, CCIRC encourages users and administrators experiencing a ransomware infection to report the incident to local law enforcement.

Most often, attacks of this type are detected by diligent and well-informed users who receive current situational awareness and training; are familiar with organizational policies, processes and data protection education; and who know how and when to report unusual or suspicious emails to their IT security team.

1. If an infection occurs, avoid clicking on any link or attachment that meets the above criteria, and immediately disconnect the system from the network. This might prevent the malware from further encrypting additional files on the network.
2. Do not try to troubleshoot this on your own or try to recover your data.
3. Immediately notify your organization's Help Desk or Cyber Security Team if you suspect that your system has been infected with this or other malware.

Other Suggested Actions

A privacy-aware organizational culture is important to help reduce the risks posed by this and other threats to data.

- Implement Privacy by Design principles to ensure adequate safeguards are the default for all systems, processes, and practices.
- Apply the principle of least privilege to the extent possible.
- Implement regular and detailed training to ensure users understand organizational policies, processes and data protection requirements.
- Perform regular backups of all critical information to limit the impact of data or system loss.
- Contact AMINAcorp.ca for more information about how to protect privacy, reduce data risks, and comply with privacy and access laws.

For more information about practical ways to protect privacy and reduce risk, visit www.AMINAcorp.ca or contact us by email at info@AMINAcorp.ca or by phone at +1.403.254.4376 for a private conversation.