IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Education Notice
Guidance Notice

Please distribute internally to:
Corporate Finance
Credit
Institutional
Internal Audit
Legal and Compliance
Operations
Registration
Regulatory Accounting
Research
Retail
Senior Management
Technology & Cybersecurity
Trading Desk
Training

Contact:
Suzanne Lasrado
Director, Member Regulation & Strategy (Acting)
416-943-5880
slasrado@iiroc.ca

Ryan Li
Director, Information Security
416-943-5890
rli@iiroc.ca

21-0050
March 16, 2021

Cybersecurity – Ransomware

This Notice outlines what IIROC firms and employees should do to prevent, detect, respond to and recover from a ransomware attack. The Notice also provides some information about the RCMP's National Cyber Crime Coordination Unit or NC3.

Overview

IIROC has noticed an increase in ransomware attacks on IIROC firms and in particular, over the last few months. Ransomware is the most common type of cybercrime and continues to evolve. It is a critical threat that firms need to continue to look out for[1].

Ransomware is a malware that encrypts and locks your device (server, computer, tablet or mobile phone) and prohibits access to the information on the device or network until a ransom (like bitcoin) is paid[2].

While the ransomware attacker says that they will provide a key or code to decrypt the device or network on payment of the ransom, this is not always what happens. Sometimes, even if the ransom is paid, the attacker may destroy the information or publicly expose and release the data by putting it up for sale on the dark web.

Threat vectors

Ransomware is typically installed on devices or networks through:

1) Phishing attacks, i.e. malicious links or attachments sent through emails, text messaging and other communication technology, is the most common threat vector
2) "Drive-by downloads" which occur when an individual clicks on a compromised website or on a malicious advertisement on a legitimate website (i.e. malvertising)
3) Stolen credentials, which are available on the dark web from a previous exposure or attack
4) Brute-force entry into vulnerable web networks and servers

Recommended protection, identification and detection controls

The best way to deal with a ransomware attack is to prevent it from deploying. Firms should establish controls to prevent and identify ransomware which include but are not limited to:

1) **Implementing firm-level controls, policies and procedures** that should, at a minimum,
    - Establish processes to:

[1] The Government of Canada's Canadian Centre for Cyber Security also highlights ransomware as a threat in its National Cyber Threat Assessment 2020

[2] For more information, refer to the Government of Canada's bulletin Modern Ransomware and its Evolution

- respond expeditiously to anomalous behaviour, as well as complaints, calls and inquiries about unusual activity
- quickly investigate a suspected attack to determine the root cause and extent of the attack

- Consider how much and what types of cybersecurity insurance is needed as appropriate for the risk levels of the business

2) Implementing **information backup controls** including

- Back up all systems and data, and for critical information, do it as frequently as possible
- Test backups to ensure integrity
- Keep backups stored separate from your production network and maintain separate servers and storage for your data

3) Implementing **technology controls** to protect devices and networks including:

- Implement strong access management controls including password management, multi-factor authentication, and privileged access management tools for accounts with elevated access (like administrators) and with access to software deployment functions
- Keep your operating systems patched and up-to-date to protect against any new identified vulnerabilities
- Enforce web filtering tools to restrict user access to potentially malicious websites
- Limit or disable access of remote desktops directly through the Internet
- Implement anti-malware/anti-virus capability at key points of your environment (e.g. network, email, and end point layers). Additional services should be considered such as "sandboxing" which is a process to test attachments for malicious activity in a virtual safe environment
- Implement a Security Information and Event Management (SIEM) platform that aggregates event and security data from multiple sources to help the firm respond and recover from an attack

4) **Educating employees, contractors and advisors** to exercise and remain vigilant when clicking on links in emails and on the internet:

- Conduct frequent phishing awareness training and tests, including the importance of verifying all requests for authentication not initiated by the person

- Remind employees to
    - notify IT immediately if they notice unusual activity for example, their devices or applications slowing down for no apparent reason
    - Be familiar with the firm's response protocols if their device has been locked by ransomware

5) **Monitoring for anomalous behaviour** to detect and mitigate an attack

- Implement a Continuous Security Monitoring (CSM) function to automate monitoring of threats, and Endpoint Threat Detection and Response (ETDR) solutions to detect malware and assist forensics in the event of an attack
- Implement tools to constantly monitor lists of known malicious, fraudulent IP addresses and block access by such addresses to the firm's systems
- Inspect network traffic to detect malicious activity
- Monitor for abnormal deviations in login requests or activity, including lateral movement activity[3]

Recommended recovery and response controls

Firms should implement controls to respond to ransomware attacks which include but are not limited to:

1) **Immediately isolate the infected devices** to limit scope of the attack

- Determine scope of the attack and isolate/remove affected devices from the network
- Protect the network including applying updates, suspending accounts and requiring clients to set new passwords or create new accounts

2) Determine **whether you have a salvageable backup** and what information is lost, if any

- Restore data from the last clean backup and make sure that
    i. the backup does not contain any malware, and
    ii. the ability to conduct a thorough forensic investigation is not impeded (e.g. if

[3] Lateral movement refers to a tactical technique that cyberattackers use, after infiltrating and gaining access, to move through the networks further and obtain elevated privileges in order to identify more vulnerabilities and sensitive and critical information.

recovering the data leads to overriding old servers or virtual machines).

- Check if there is a decryptor available to unlock any critical information missing since the last clean backup
- Carefully consider with legal counsel any decision to pay or not pay the ransom bearing in mind the criticality/need of the lost information, the likelihood of the attacker to make good on their promise, and the possible visibility to future attackers. Law enforcement officials generally advise against paying ransoms.

3) **Investigate the incident** to determine the scope and extent of the attack (even if it appears to be isolated to a few devices or networks)
    - Engage an external forensics team to conduct a complete investigation to determine root cause and extent of attack. Often times the deployment of ransomware may be the last stage in an attack. The malware may have been sitting in the network or device and collecting information before being deployed.
    - Determine if a data breach occurred and whether the ransomware attacker could have had access to private and confidential information. If a breach occurred, follow all incident response protocols including notifying affected individuals.
4) **Report the incident to the applicable authorities**, privacy commissioners, regulators, and/or law enforcement officials. In addition, if the incident meets the requirements of IIROC Rule 3100(B.1.1) *Cybersecurity Reporting*, then firms must contact their IIROC Financial & Operations Compliance manager to provide the required information.

RCMP's National Cyber Crime Coordination Unit (NC3)

In some cases, local law enforcement authorities may proactively contact a firm that has been the victim of a cybercrime[4]. Often, law enforcement receives this information from the RCMP's National Cyber Crime Coordination Unit or the NC3.

The NC3 is a National Police Service stewarded within the RCMP. The NC3 coordinates and deconflicts cybercrime investigations across all levels of policing to enable efficient law enforcement activities of national and international police partners as they relate to cybercrime, including apprehending and disrupting cybercriminals. Ultimately, the NC3's objective is to reduce the threat, impact and victimization of cybercrime in Canada and

[4] As with any communication, you should independently verify the legitimacy of the communication and the sender (e.g. by obtaining the contact information of the law enforcement authority, like an email address or switchboard phone number, by doing a search for the authority or the individual on an uninfected device).

contribute to achieving the Government of Canada's long-term vision of safety and security in the digital age.

On April 1, 2020, the NC3 reached its initial operating capability. Working with Canadian law enforcement agencies, government and private sector partners, the NC3:

- coordinates cybercrime investigations in Canada
- works with partners internationally to combat a wide range of cybercrime incidents
- provides digital investigative advice and access to technical capabilities to Canadian police

Through its regular operations and coordination with police domestically and abroad, the NC3 is frequently in possession of information on cybercrime victims in Canada. The NC3 provides this information to local law enforcement to ensure the victim is aware of the incident and to encourage victims to formally report a complaint to their police service. In ideal situations, the timeliness of this information allows for early warning to victims, helping to mitigate the impacts of the incident.

To learn more about the NC3, please visit the RCMP website:
https://www.rcmp-grc.gc.ca/en/nc3

Other resources

Further information and resources on managing cybersecurity threats, including guides and webinars, are available on IIROC's cybersecurity site.