Dealing with Phishing and Malware

Phishing

Phishing and fraudulent emails remain a prominent way in which attackers can gain access and compromise security; malicious parties can try to steal credentials and make victims think the emails come from a trusted party and attempt to convince them to click on malicious links or malicious attachments.

The Canadian Anti Fraud Centre provides educational material and guidance on various fraudulent activities including phishing and related scams, more information can be found at the following site: http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/phishing-hameconnage/index-eng.htm

Preparation

Preparation is key to preventing malicious infections, including ransomware, and to reducing the impact when they occur. These are some steps you can take:

- Have Backups
  - Backup all data on an isolated and protected server with separate authentication protocols and credentials.
  - Ensure that your backup strategy allows you to restore files to any point in time up to a minimum of two weeks prior to the most current backup.
- Regularly patch your environment
  - Have a method of getting informed about vulnerabilities.
  - Have a plan for responding to vulnerabilities on your systems and ensure you can activate it quickly.
- Secure services on your systems
  - Use multi-factor authentication for login wherever possible.
  - Do not have Remote Desktop Protocol (RDP) exposed on Internet-facing systems. It is trivial for attackers to exploit these systems.
  - If there is no need for Remote Desktop Protocol (RDP) running on a server, disable it.
- Educate your users on cyber security best practices
  - Conduct internal phishing campaigns to educate employees on the dangers of phishing.
  - Enable the use of passwords containing lower/upper case letters, numbers and special characters wherever possible.
  - Recommend that passphrases are used for passwords when possible, avoiding dictionary words.
  - Encourage users not to use the same password for all their accounts; different passwords for different accounts is the best practice.
  - Consider sources such as the ones below for more information
    - http://www.rcmp-grc.gc.ca/scams-fraudes/ransomware-rancongiciels-eng.htm

LOW SENSITIVITY

Dealing with Phishing and Malware

    - Contact cyberadvice@ontario.ca for educational materials and advice.

- Develop and document incident response policies, procedures and operational guidelines, with the following guiding questions:
    - Do you know who to contact in case of a Cyber incident?
    - Do you know what entities your organization connects with? Are you connected to another group/ organization to provide or receive data/services?
    - Can you procure cyber incident response and legal services quickly if needed? Consider putting these services on retainer if you can.
    - Do you have cyber insurance?
    - Do you have a BCP plan for cyber incidents?
- Assess threat detection capabilities
    - What are your in-house capabilities around detecting and responding to cyber threats?
    - How can you address gaps (if any)?
- Perform ongoing collection and analysis of threat intelligence
    - Are you subscribed to information feeds about potential cyber threats to your sector?
    - Consider signing up for the Canadian Centre for cyber security's alerts.
- Email Protection
    - Do you have spam filtering or any email protection in place? Spam filtering will reduce your exposure to fraudulent, phishing and potentially malicious messages.
    - Consider email attachment filtering, allowing only attachment types required for business.
    - Consider sanitizing attachments such as macros in Microsoft office files and JavaScript before email attachments are delivered to users.
    - Consider having email attachments scanned by an anti-virus tool.
    - Consider disabling active content in email messages, this will mean that users need to copy and paste web addresses into their browser.
    - Consider an email/ phishing education campaign to make sure that all users are familiar with phishing and related threats.
    - Reach out to cyberadvice@ontario.ca if you need more information
    - See the links in the Additional Resources section for Office365 and Google Suite configuration tips if you are using either of those services for email
    - Consider the source below for more information and guidance: https://www.cyber.gov.au/publications/malicious-email-mitigation-strategies

Dealing with Phishing and Malware

Containment and Neutralization

What to do when you experience a malware infection (including ransomware).

1. If you have an IT service provider, call them immediately.
2. Take steps to isolate your environment from any organization that connects with yours. This can be in the form of firewall blocks or disabling ENA connections.
3. Contact organizations that are connected to yours and advise them of the situation so that they can take precautions on their end.
4. Speak to your users and try to identify the source of the infection. Did they open an email attachment or click on a strange link? Record these details. They can also help you identify security gaps.
5. If you have a Web Security Gateway, Firewall or Proxy service, check the log files for suspicious alerts. These can identify IP addresses for you to block and could be used to help other organizations determine if they were impacted. Your IT service provider should be able to assist with this.
6. Was any information compromised (especially personally identifiable information)?
    a. This can be tricky to determine without professional help. We strongly recommend bringing in professional services to help with this step.

If you have staff on-site to respond to the incident, consider the steps below:

1. Are the impacted systems connected to your organization's network?
    a. If they are connected to your organization's network, disconnect them immediately.
    b. Does the infected system(s) have access to network shares? If it does, the shares were likely impacted.
    c. Can all infected machines be immediately identified and isolated?
        i. Isolation can be in the form of pulling network cables, shutting machines down, disabling VPN accounts used by impacted remote users.
2. (For ransomware infections), is a copy of the ransom note available?
    a. Make note of the ransom note file content and file extension. Both can be used to identify the ransomware family.
    b. Make note of the "Properties" tab of the ransom note file. This can help you identify where the infection originated from.
    c. Check to see if the user listed as the Owner of the file is a user account with a non-generic name. If it is, have the user disconnected from the network (VPN account disabled, AD account disabled, Machine isolated).
    d. Google the specifics of the note file, the extension of the file name and the location of the ransomware executable to try to identify the family it belongs to. Check resources below to see if a Decryptor might be available.
    e. Can any of the files be opened?

   f. Have file extensions changed?
3. Are there any email addresses or other indicators of compromise available?
4. Did anyone receive any unusual emails, or accidentally click on any unusual sites?
5. Have any IT staff carried out any actions, or attempted to clean the infection?
6. Was antivirus software installed and working?
   a. Was it up-to-date?
7. Is File Access Auditing enabled on the infected server?
   a. This can help you determine if a specific user account created/modified files as a result of the infection so you can have it disabled. It can also aid in determining if a compromised account accessed sensitive information.

Data Recovery

Questions to raise and items to consider:

1. Do Backups exist?
2. If backups exist, what kind of backups are they?
3. Have the backups been tested?
4. If backups are encrypted or otherwise not available, can key data be recovered via temporary files or forensic methods?
5. Once all impacted machines have been identified and isolated, Firewall blocks restricting access to the Organization's network can be removed.
6. Can the impacted machines be re-imaged?
7. Can the malware family be identified and if so, can a decryptor be found?

Additional Resources

Enterprise Survival Guide for Ransomware Attacks – SANS Institute https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware- attacks-36962

Demisto Ransomware Playbook
https://www.demisto.com/playbook-for-handling-ransomware-infections/

Windows Defender ATP customer engagement – Ransomware response playbook
https://www.microsoft.com/en-us/download/details.aspx?id=55090

Ransomware Decryptors
When you have identified the ransomware and are looking for decryptors, please use the

links/resources below, these are actively maintained lists of ransomware decryptors.

https://noransom.kaspersky.com/
https://www.watchpointdata.com/ransomware-decryptors/
https://www.nomoreransom.org/en/index.html https://gitlab.com/invsec/free-ransomware-decryptors-list

Tool to identify ransomware family (can identify some ransomware families)
Ransomware family identification can be a manual process, but there is a tool that can assist.
The tool requires you to upload a copy of the ransomware note and an encrypted file, it then checks its internal databases to categorize it and identify if any decryptors are available.

https://id-ransomware.malwarehunterteam.com/index.php

Office365 and G Suite Admin Configuration
Do Google or Microsoft host your email? Check out the links below for information on enhancing security for G Suite and Office365.

G Suite Admin - Advanced Phishing and Malware Protection
Protect Against Threats in Office365