Office of Cyber-Security
& Information Assurance
Oik son Shickyrys Lectraneagh as Saoghys Fysseree

Supplemental Advisory Notice

Issue Date 10th March, 2020

TLP: WHITE

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE

WHITE **Public** - May be distributed freely, without restriction.

Ransomware: Additional preventative measures

Note: This document acts as a supplement to our previous advisory notice, 'Protecting yourself from Ransomware'. We would recommend reading that advisory notice for a description of ransomware and basic guidance on preventing a ransomware infection.

If you are suffering a ransomware incident, please refer to the UK NCSC list of urgent steps to take.

Overview

Ransomware cases have increased dramatically in 2020 and as long as it remains profitable, the number of attacks will likely keep on rising.

Ransomware attacks are being seen in both large and small organisations. Individuals are also at risk. The Internet knows no borders meaning that any computer system is potentially at risk of suffering from ransomware if effective preventative and defensive measures are not employed.

By implementing preventative measures we can disrupt this criminal enterprise and make ransomware an unsustainable activity, as well as reducing the impact and cost of a successful ransomware attack. In addition to the recommendations set out in our advisory, 'Protecting yourself from Ransomware', this document sets out further considerations and associated preventative measures.

Office of Cyber-Security & Information Assurance (OCSIA)
OCSIA@gov.im (01624) 685 557

Recommended Action

1. The "3-2-1" rule for backing up your data

The "3-2-1" rule refers to having at least 3 copies of your data, on 2 devices, and 1 offsite. This rule is the most common method for creating resilient data backups.

Keep in mind that at any given time, one or more of your backups should be offline and backups should only be connected when absolutely necessary. There is, of course, no value in a backup that can be infected because it is connected to a live system.

For further information on securing data backups, please refer to the UK NCSC article: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

2. Securing file indexes

Businesses can potentially run into issues when recovering their data from backups after a ransomware attack. Although the business may have been able to restore their data and files, they may not have considered the index files which might have also been encrypted.

Indexes are used to quickly locate and access data without having to search every row in a database table. For large databases, indexing can be critical for efficient business operations. It can even potentially grind some services to a halt whilst re-indexing is performed, so it is a good idea to consider regularly backing up index files and any other data cataloguing mechanisms.

3. Microsoft Windows 10 Ransomware Protection

Microsoft Windows 10 has an in-built anti-malware service called Defender. Windows Defender includes a security feature called "Ransomware Protection". This feature is disabled by default but it is recommended to enable it in order to get the most protection you can for your computer systems.

This feature is comprised of two components; Controlled Folder Access and Ransomware Data Recovery.

Controlled Folder Access - This component allows you to specify certain folders that you wish to monitor for and block changes to the files contained within them. This will block all programs, except the ones you allow, from making any modifications to the monitored folders. This, in effect, will protect them from being encrypted by ransomware.

Ransomware Data Recovery - Ransomware Data Recovery will automatically sync common data folders with a Microsoft OneDrive account in order to backup your files. If this component is enabled, ransomware victims can use OneDrive to recover their files.

Easy to follow instructions on how to enable this security feature can be found here: https://www.bleepingcomputer.com/news/microsoft/how-to-enable-ransomware-protection-in-windows-10/

4. Show file extensions

Malicious files can masquerade as legitimate file types. A file attachment in an email or downloaded file might appear to be a PDF (.pdf) or word document (.doc) but in actual fact be an executable (.exe), batch file (.bat) or other format that, when clicked, can perform malicious operations.

Be especially cautious if you see an attachment with a similar format to "invoice.pdf.exe" or similar.

Instructions on how to display file extensions can be found on the following links:

MS Windows: https://www.techadvisor.co.uk/how-to/windows/windows-10-file-extensions-3697651/

Mac OS: https://www.techradar.com/how-to/computing/apple/how-to-show-or-hide-file-extensions-in-mac-os-x-1295830

5. Configure alerts and notifications

Ransomware will attempt to traverse networks in order to spread - this may require the ransomware to make modifications to the services that manage access controls.

Where possible, set anti-malware/end point protection to monitor, and create notifications and alerts for any changes to Group Policies, Active Directory or any other services managing access control.

6. The rule of "Zero-Trust" for privilege rights

The idea behind "zero-trust" is to provide the minimum amount of access to information, networks and applications required to do a required job or task.

For example, a database administrator should not have default access to all databases, only the ones they need to work on that day. This reduces the attack surface should the administrator's account be compromised.

It is important to consider what systems can access the Internet and email. Administrator accounts with access to business-critical systems or data should be isolated from the Internet wherever possible. Workstations intended for administrator accounts or accounts with heightened privileges should not be used for standard user accounts as malware could be introduced and subsequently compromise the account with increased rights.

The National Cyber Security Centre (NCSC) and National Crime Agency (NCA) advise **not** to pay the ransom, as there is no guarantee that you will regain access to your device or data.

For more advice and guidance on mitigation malware attacks, please refer to the UK NCSC article: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

More advisory notices and guidance can be found on our website: www.gov.im/ocsia.

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security & Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.

TLP: WHITE