Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

September 10, 2019
CS-05-2019

RANSOMWARE – PROTECTING YOUR DATA

OVERVIEW

Ransomware is becoming more and more common with incidents occurring all over the country on a regular basis. Ransomware, at a basic level, is malicious software that encrypts computer systems and locks important files until the organization pays for a key to unlock the system or information. Typically, ransomware will target user created files such as documents, pictures, and spreadsheets, as well as backup files.

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES ARE ENCRYPTED

Image Source: fbi.gov

Multiple entities across the country have fallen victim to ransomware in recent weeks. In Florida, Riviera Beach paid $600,000 and Lake City paid almost $500,000 to get their data unlocked, according to representatives from those cities. Recovering from a ransomware incident can cost millions of dollars when adding other costs associated with an attack. Additional costs could include cost to hire IT mitigation specialists, loss of sales opportunities, loss of employee productivity, full restoration of systems or files if data is never recovered, damage to brand reputation, or penalties for unmet contractual obligations to customers, all due to the effects of downtime in basic business functions.

Repercussions from a ransomware attack can be prevented, with a method as simple as backing up files and data. Systems can be restored from backups during a ransomware incident if the backups themselves have not been infected.

The Michigan Cyber Command Center recommends the following ransomware controls:

- **BACKING UP DATA**
  - Make it a priority to implement a regular backup regimen to an external device or backup service. Backed up files should be kept off-line. Keep backups for a sufficient amount of time based on your business needs.
  - Automatically mount and unmount backup devices. Backup devices should only be mounted while in use. An automated script can be used to accomplish this.
  - Keep at least one copy of backups offsite.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP:WHITE. Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.

Page 1 of 2

  - If backups are stored on the same system or network, rename the backup file extensions using an obscure naming convention. Ransomware typically encrypts known backup file extensions.
  - Test and verify backups. Email alerts can be set up within some backup managers providing early detection for issues related to scheduled backups, or insufficient disk space on a backup server.
  - When storing backups in cloud-based solutions, ensure the files cannot be altered/modified.

- **SYSTEM HARDENING**
  - Segment networks as much as possible. This may limit the scope of data the ransomware can infect. Consider whether each computer needs to have access to the entire network.
  - Ransomware may be delivered via JavaScript files. Disabling the Windows Script Host (responsible for running JavaScript files outside a browser) can prevent users from inadvertently running a malicious JavaScript file.
  - It is common for ransomware to use Windows' own encryption DLLs. Enabling security software to block calls to these DLLs by untrusted applications or requesting confirmation from the user that an encryption operation has been requested is recommended.
  - Use file integrity monitoring capabilities to detect changes to system files and the registry. Monitoring for mass modifications can help detect and block applications that are trying to create or modify large numbers of files or change file names.

- **SOFTWARE & TOOLS**
  - Use a reputable security suite that incorporates multiple layers of protection, both anti-malware software and a software firewall to help identify threats and suspicious behavior. Software should prevent ransomware from communicating with the command and control server.
  - Utilize an email scanner to filter attachments by extension and deny emails sent with any ".exe" files. Also deny emails sent with attachments containing two file extensions such as ".pdf.exe". This option includes using an effective spam filter that is continuously updated from a cloud-based threat intelligence center.

- **CYBERSECURITY INSURANCE**
  - Consider cybersecurity insurance to mitigate losses from a cyber-related incident.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP:WHITE. Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.