Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

May 11, 2021
CS-03-2021

MALWARE AND ADDITIONAL CYBER THREATS

OVERVIEW:

Malware infections have become a normal part of operating a business in cyberspace. As a result, many organizations have adopted best practices to maintain operations for when a cyber-attack occurs. One of these best practices includes maintaining good, offline backups and restoring from those backups. After successful restoration, organizations have usually been able to resume normal operations without having to worry about additional cyber threats. However, as of recently, the MC3 has observed malware infections such as new variants of ransomware which have introduced new cyber threats that continue to haunt organizations even after successfully restoring from backups and removing the malware from their systems.

Aside from the more common problems caused by malware infections, such as data corruption and encryption, fraud, and temporary disruption of business services, organizations must now worry about additional problems that may have a more detrimental effect on the whole organization. The repercussions of these new cyber-threats include increased costs and prolonged damage to business operations, company trust, and reputation. These negative effects can make it more difficult for an organization to fully recover from a malware incident.

Image Source: reasonsecurity.com

ADDITIONAL CYBER THREATS:

The MC3 is aware of organizations who have experienced continuous distributed denial of service (DDoS) attacks after recovering from a ransomware incident via backups. These DDoS attacks can cause extended outages of a company’s website and other online business services. The malicious actors may not stop the DDoS attacks until the originally requested ransom has been paid.

Another modern cyber threat an organization may now face after a malware incident is the exfiltration of sensitive/confidential data and personal identifiable information (PII). During ransomware incidents, not only do the malicious actors encrypt data files, but many times they also steal the organization’s data. The malicious actors then use the threat of leaking or selling the data online as another extortion method to convince the organization to pay the ransom. If the ransom is not paid, the data is then published online for anybody to view, download, or buy. This data usually contains sensitive information related to an organization’s customers, members, or employees which could then cause these individuals to be targeted in the future. The malicious actors could use this sensitive information to tailor and launch further cyber-attacks against these individuals, or demand ransom from them to prevent the release of their own sensitive data and PII.

Lastly, the MC3 is aware of ransomware groups that install backdoors on victim systems and subsequently sell the backdoor access to other malicious actors, despite the organization paying the requested ransom to decrypt their data. This exposes the organization to cyber-attacks from different actors in the future if these backdoors are not discovered and removed.

CONCLUSION:

Due to the negative effects caused by present day malware infections and the large amount of time and money it takes to recover from an incident, organizations need to be vigilant and proactive by taking steps to prevent malware incidents from occurring in the first place. These steps could include:

- Conduct regular cyber security and awareness training for employees.
- Implement an external sender email banner.
- Disable remote desktop protocol (or use behind a virtual private network), disable macros in Office documents, disable legacy authentication, and block personal email access on work computers.
- Utilize a reputable anti-virus / endpoint security software, firewall, and intrusion detection/prevention system, and ensure they are configured properly.
- Utilize encryption for data in transit and at rest.
- Implement a strong password policy which requires strong, unique passwords / passphrases along with utilizing multi-factor or two-factor authentication.
- Limit employee information published on websites.
- Enable enhanced logging and review logs regularly.
- Scrutinize policies and procedures of vendors and outside online resources housing company data or having access to it.

In addition, an organization should ensure they regularly backup their data, store these backups in a secure offline location, and practice restoring from these backups. Organizations should consider obtaining cyber insurance. Finally, all organizations should have written policies and procedures in place, including an incident response plan, which can be referred to when an incident occurs.

ADDITIONAL RESOURCES:

For more information and additional resources, please visit www.michigan.gov/mc3.

To report a cyber incident to the MC3, please contact 1-877-MI-CYBER or mc3@michigan.gov.

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.