Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
TELEPHONE (617) 727-5000
WWW.MACOMPTROLLER.ORG

ANDREW W.
MAYLOR
COMPTROLLER

STATEWIDE RISK MANAGEMENT TEAM

CTR Incident Report #2019-MBC-01

Report Date: July 24, 2019

Incident Type and Date: Cyber Incident on May 7, 2019

Where Encountered: Massachusetts Bay Community College (MBC)

Reporter: Peter Scavotto, Assistant Comptroller for Risk, 617-973-2450
Peter.Scavotto@mass.gov

---

1. Issue:

MBC IT staff discovered on Wednesday May 8, 2019 that, on Tuesday May 7, 2019 at approximately 11:00 p.m., an intruder used malicious software that compromised a web front-end server and downloaded ransomware that encrypted a series of files on several servers.

The compromise appears to have been a result of not including the impacted front end server on the list of blocked foreign addresses in the Intrusion Prevention System (IPS). MBC had not previously added this server on such list as it is used by international students for their online college applications.

2. How was the Cyber Incident Discovered?

MBC IT staff received notices on Wednesday May 8, 2019 that several employees could not access files on several servers. The IT staff discovered that files had been encrypted and a text file had been saved in each directory asking for money to unlock the files.

MBC IT began containment by identifying the compromised account and immediately changing administrator passwords and disabling the account. Names of all encrypted files, machine images and other artifacts were recorded in a separate repository for future review and forensics. Event logs for all impacted servers were also added to this incident repository.

3. Other Involved Parties:

Executive Office for Technology Security and Services (EOTSS): Assisted with VPN suspension. CommonHelp notified to withhold any user requests for HR/CMS password resets.

4. Remediation – Office of the Comptroller Remediation Plan:

The Office of the Comptroller (CTR) was contacted by phone shortly before noon on Friday May 10, 2019 that a cyber-incident had occurred and MBC IT staff were in the process of containment.

At 12:00 p.m. the CTR Incident Response Team met to assess the threat and initiated an immediate security freeze process around 12:15 p.m. that inactivated HR/CMS and MMARS Security for all MBC users. CommonHelp was contacted not to reset passwords for any MBC staff for HR/CMS. In addition, the CTR Security Team contacted EOTSS at approximately 12:18 p.m. to inactivate VPN access to prevent any traffic into the Enterprise Systems; as well as the CIW and DocDirect. Intercept access to upload intercepts was also suspended. No interfaces were impacted. CTR Payroll staff were alerted that MBC would require assistance with payroll processing until HR/CMS security was restored.

All CTR staff were informed by email and an employee portal message of the incident and not to open any email from MBC and to be on the alert for other suspicious emails or requests for transactions or actions.

On Friday May 10, 2019 at 2:13 p.m., Coalfire, a cyber remediation vendor on Statewide Contract PRF56, was contacted to conduct an independent remediation assessment. Coalfire had recently completed a Payment Card Industry (PCI) assessment at MBC and was familiar with the MBC infrastructure and an independent assessment could be completed more quickly and efficiently.

Between Friday May 10th and Monday May 13th the RMT coordinated an Incident Response Mitigation Plan for MBC to deploy three (3) safe computers with a clean installation of Microsoft Windows 10 to be located in secure offices and would be used solely for Enterprise Systems and on-line banking transactions. The safe computers were required to connect only through a dedicated business class internet service that was not connected to any local MBC server or email system that could potentially infect the computers.

On Monday May 13, 2019, within 1 business day of notification of the incident, CTR restored security access to the users identified in the Incident Response Mitigation Plan using the 3 safe computers. CTR also provided support for transactions in HR/CMS and MMARS during the period of remediation.

Coalfire completed the independent cyber remediation review and issued a report on June 17, 2019 finding that the attack did not maintain persistence in the MBC networks and that security to the Enterprise Systems could be restored.

On June 20, 2019 MBC provided a response to the CTR Team on the recommendations contained in the Coalfire report and the progress to be completed during remediation.

On Friday July 12, 2019, approximately 63 days from the date CTR was informed of the incident, MBC was provided with a return to operations notice that MBC was being restored to full Enterprise System access.

It was determined that other than remediation costs to contain ransomware, restore servers, additional security measures and third party assessment costs, MBC incurred no other financial losses. The Enterprise Accounting and Payroll systems were not impacted by this cyber-incident.