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-CCC-01

Report Date: October 18, 2019

Incident Date: Cyber Incident on November 26, 2018

Where Encountered: Cape Cod Community College (CCC)

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

---

1. Issue:

On November 26, 2018 a CCC employee opened an email attachment and enabled a macro that downloaded the Emotet virus. The virus, while limited to the Administration Building, initiated a multi-pronged attack on the college, including denial of service and social engineering, which resulted in stolen banking credentials and unauthorized wire transfers from the college's accounts.

2. How was the Cyber Incident Discovered?

Over two days, one employee reported a suspicious email and another noticed unusual pop up screens on Business Office computers. Another email was received, purportedly from the college's bank, asking a CCC manager to log into the bank's website. While unable to log in, the manager received a phone call from someone posing as a bank representative offering assistance. After credentials were shared with the caller, twelve (12) wire transfers were initiated from CCC's bank, nine (9) of which were successful, totaling $807,130.

Upon the twelfth wire transfer, the bank contacted CCC's Comptroller seeking confirmation of the transfers. Online access to college bank accounts was halted. Bank officials, campus police, State Police, the Cape and Islands District Attorney, the FBI and the Attorney General were notified of the attack and stolen funds.

During this same time frame, a denial of service attack prevented staff from accessing the internet. The IT team was focused on addressing this problem.

After ninety (90) business days, all funds were recovered except for approximately $127,000.

3. Remediation – Office of the Comptroller Remediation Plan:

On November 28th, the Office of the Comptroller (CTR) was notified and joined a conference call with college representatives to address issues of suspension from Commonwealth enterprise systems, continuity of operations, and remediation and recovery of the college's system stability.

The CTR Incident Response Team convened to assess the threat and initiated an immediate security freeze process to inactivate HR/CMS and MMARS access for all CCC users. In addition, the CTR Security Team contacted the Executive Office of Technology Services and Security (EOTSS) to inactivate VPN access to prevent any traffic into the Enterprise Systems including the data warehouse (CIW) and DocDirect. CTR Payroll staff were alerted that CCC would require assistance with payroll processing until HR/CMS security was restored.

All CTR staff were informed of the incident and instructed not to open emails from CCC; and to be on the alert for other suspicious emails or requests for transactions or actions.

On 12/2/18 Ernst & Young (EY), a cyber remediation vendor on Statewide Contract PRF56DesignatedOSC, was engaged to assist with the investigation and incident response. A second Emotet outbreak occurred on 12/7/18 in the CCC library when a user opened an email with an attachment ultimately enabling another macro.

EY identified and isolated the infected machines from both outbreaks and assisted with removal of the malware. EY also provided a report of the incident response along with seven (7) Tactical Recommendations and eight (8) Strategic Recommendations for remediation and future mitigation of risk.

The CTR Incident Response Team coordinated a Mitigation Plan with CCC to deploy four (4) safe computers to be used solely for fiscal and banking transactions. CTR restored security access for Enterprise System users identified in the Mitigation Plan. Support for transactions in HR/CMS and MMARS were provided as necessary during the period of remediation.

CTR conducted eight (8) on-site trainings for over 200 CCC staff on cyber security risks, fraud awareness and internal controls. Financial training was also held at CTR for 15 CCC staff on risk, fraud, internal controls and foundations of state finance.

As of October 15th, 2019, CCC is still conducting Commonwealth Enterprise System business on the four safe PCs. CCC has implemented several cyber security improvements since the incident. These and other conditions are being reviewed in order to restore full Enterprise Systems access.

4. <u>Other Involved Parties</u>:

1. **Executive Office for Technology Security and Services (EOTSS)**: Assisted with VPN, CIW and DocDirect suspension. CommonHelp was notified to withhold any user requests for password resets.
2. **EOTSS** facilitated the involvement of Ernst & Young from PRF56DesignatedOSC Statewide Contract.

If you have questions, please contact Peter J. Scavotto, Assistant Comptroller for Risk, Statewide Risk Management Team.
Phone: 617-973-2450 E-mail: Peter.Scavotto@mass.gov