ANDREW W.
MAYLOR
COMPTROLLER

Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

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

STATEWIDE RISK MANAGEMENT TEAM

Cyber Incident Report #2019-MAS-01

Report Date: July 24, 2019
Incident Date: April 1, 2019
Where Encountered: Massasoit Community College (MAS)
Reporter: Peter Scavotto, Assistant Comptroller for Risk, 617-973-2450 Peter.Scavotto@mass.gov

---

1. Issue

On April 1, 2019 an employee opened what appeared to be a legitimate email from a known vendor with an invoice attached requiring payment. The attachment contained a link to a spoofed Office 365 page where the employee entered credentials allowing the perpetrator to take control of the employee's email account.

2. How was the Cyber Incident Discovered?

The MAS Information Technology Office received reports from staff on April 11, 2019 that they were receiving emails from a MAS account containing a suspicious link. IT staff searched for the phishing emails in all employee mailboxes and deleted them. In addition, Accounts Payable received an email - allegedly from the known vendor (same as above) - requesting a bank account change. The change was not made.

Processing rules had been set up in the affected employee's email account to delete responses from other MAS accounts. These rules were identified and deleted. Subsequent forensics revealed no extraction of data from the employee's PC. Suspicious IPs were identified and blocked at the MAS firewall.

All employees who received an email with the malicious link had their credentials immediately reset. There was no evidence that their accounts were compromised. No suspicious rules were found in any other accounts. All computers associated with the phishing emails were scanned; no malware was detected.

3. Remediation – Office of the Comptroller Remediation Plan:

The Office of the Comptroller (CTR) was contacted on April 11, 2019 that a cyber incident had occurred and MAS IT staff were in the process of containment.

The CTR Incident Response Team initiated a security freeze process and inactivated HR/CMS, MMARS and PartnerNet access for all MAS users and CommonHelp was instructed not to reset HR/CMS passwords for any MAS staff. In addition, CTR worked with the Executive Office for Technology Security and Services (EOTSS) to deactivate VPN access to prevent unwanted traffic into

the Enterprise Systems. Intercept access was also suspended. There were no interfaces from MAS to Enterprise Systems to address.

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

All CTR Payroll staff were alerted that MAS would require assistance with payroll processing until HR/CMS security was restored.

CTR coordinated an Incident Response Mitigation Plan with MAS to deploy four (4) safe computers with a clean installation of Microsoft Windows 10 to be used solely for Enterprise System and on-line banking transactions. The safe computers were connected through a dedicated business class internet service not connected to any MAS server or its email system.

Compass IT Compliance, a cyber remediation vendor on Statewide Contract PRF56, was engaged to conduct an independent remediation assessment. Compass was familiar with the MAS infrastructure having recently completed a Payment Card Industry (PCI) assessment.

On April 12, 2019 (within 24 hours of incident notice) CTR restored security access to users identified in the Incident Response Mitigation Plan using the 4 safe computers. Support for transactions in HR/CMS, MMARS and other needs were provided during the period of remediation.

In mid-May Compass began a Third Party Remediation Review and issued a report on June 12, 2019 finding that the security incident was contained and resolved in an effective manner. There did not appear to be any remnants from the attack on MAS systems, there was no evidence of any data extraction, and it was recommended that security to the Enterprise systems could be restored.

After CTR review of the remediation efforts and reports, on July 17, 2019, approximately 97 days from the date CTR was informed of the incident, MAS was provided with a return to operations notice that MAS was being restored to full Enterprise System access.

It was determined that other than remediation costs to rebuild the single employee PC, additional security measures and third party assessment costs, MAS incurred no other financial losses. The Enterprise Accounting and Payroll systems were not impacted by this cyber-incident.

4. Other Involved Parties:

1. **Executive Office for Technology Security and Services (EOTSS)** (assisted with VPN suspension)
    a. **Commonhelp** (Notice to withhold any User requests for password reset)

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