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

Cyber Incident Report #2019-CPC-01

Report Date: July 26, 2019

Incident Date: March 1, 2019

Where Encountered: Committee for Public Counsel Services (CPC)

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

---

1. Issue

On March 1, 2019 a CPC employee opened an email attachment and enabled a macro that downloaded the RYUK Ransomware virus which spread through CPC servers encrypting files and compromising CPC's network servers, PCs, email and phone system.

2. How was the Cyber Incident Discovered?

Employees were unable to access files and a ransomware message requesting bitcoin as payment to restore CPC systems was discovered. CTR was notified by the Executive Office for Technology Security and Services (EOTSS) that a ransomware event had occurred. CPC emails and phones were offline and CTR Risk Management staff went in-person to CPC to communicate with staff.

CPC had already engaged a security vendor, Vancord, to assist with malware containment and remediation services to remove the RYUK Ransomware from all impacted PCs, servers and networks and to rebuild CPC systems to their pre-infection state. In addition, CPC engaged Vancord to advise on immediate and future security measures to mitigate future attacks.

3. Remediation – Office of the Comptroller Remediation Plan:

Upon notification that a cyber-incident had occurred and CPC IT staff were in the process of containment, CTR's Incident Response Team convened to assess the threat and initiated an immediate security freeze process to inactivate HR/CMS, MMARS and PartnerNet access for all CPC users. EOTSS's CommonHelp was instructed not to reset passwords for any CPC staff. In addition, the CTR Security Team contacted EOTSS to inactivate data warehouse (CIW) and DocDirect access, as well as access to VPN to prevent any traffic into CPC or Enterprise systems. CTR Payroll staff were alerted that CPC would require assistance with payroll processing until HR/CMS security was restored. Payment interfaces for batch processing were suspended.

All CTR staff were informed of the incident and instructed not to open any emails from CPC and to be on the alert for other suspicious emails or requests for transactions or actions. CPC established separate email addresses for secure communication.

On Monday March 4, 2019 CTR restored security access to users identified in the Incident Response Mitigation Plan. Support for transactions in HR/CMS, MMARS, and other needs, were provided during the period of remediation, including the use of CTR and Employee Service Center (ESC) PCs for accounting and payroll data entry.

On Monday March 29, 2019, Coalfire, a cyber remediation vendor on Statewide Contract PRF56, was engaged to conduct an independent incident response assessment and to provide pre-scanning of interface files prior to Enterprise System upload.

On April 3, CTR and CPC implemented an Incident Response Mitigation Plan for CPC to deploy two (2) safe computers (initially) 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 CPC server or its email system.

On May 9, 2019, after CPC had completed containment and remediation efforts, Coalfire began a Third Party Remediation Review and issued a report on June 14, 2019 finding that the security incident was contained and resolved in an effective manner, that there did not appear to be any remnants from the attack left on the affected systems, and that access to the Enterprise systems could be restored. A majority of recommendations made by Coalfire were implemented by CPC prior to the final report issuance and were consistent with similar recommendations made by Vancord during the containment and remediation phases.

After CTR review of the remediation efforts and reports, on July 17, 2019 (approximately 138 days from the date of the incident), CPC was provided with a return to operations notice that CPC was being restored to full Enterprise System access.

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

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

1. **Executive Office for Technology Security and Services (EOTSS)** for VPN, CIW and DocDirect suspension
    a. **CommonHelp** for notice to withhold any User requests for HR/CMS password resets.

2. **Employee Service Center (ESC)** allowed CPC Payroll/HR staff to use ESC computers for continuity of operations.

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