From:	"Johnston, Sadhu" <Sadhu.Johnston@vancouver.ca>
To:	"Direct to Mayor and Council - DL" <CCDTMACDL@vancouver.ca>
Date:	5/12/2017 7:19:58 PM
Subject:	Cyberattack update

Greetings Mayor and Council
Please see below a high level overview from Jessie and Roberts of the current state of the incident.

Through the efforts of the incident response team the scope of the potential exposure has been identified and significantly reduced. Here's an update of our knowledge and mitigation efforts:

- This malware is a self-replicating worm that will encrypt and ransom systems should an infection take place
- It is currently being propagated globally through a very specific file type received as an email attachment. That file type has since been blocked on our exchange server and the server itself has been searched to ensure that no infectious files of that type have been received in the previous week.
- The IP address that the malware uses to "phones home" after a successful infection was also identified and blocked at multiple levels of our infrastructure. The logs were searched for the previous week to ensure that there has been no communication with that address in any way.
- There are two vulnerabilities used by this malware to infect a system. The incident team is testing and pushing a patch for one of those vulnerabilities now with the majority of our computers having received the patch in April. The second vulnerability has no patch currently available from the vendor (Microsoft). The incident team will monitor for a patch and begin the implementation process when one becomes available.
- Some computers are too old to receive the patch. They are being identified and are being shut down, removed from the network or isolated based on the needs of the business.

In summary, all organizations remain vulnerable to the zero day aspect of one of the two vulnerabilities identified and will remain so until such time as Microsoft publishes a security patch. This vulnerability is common among every organization using Microsoft Office globally. The standard ingress method for this malware has been blocked, and our files and communication methods have been inspected for signs of current infection and none have been found, the propagation vulnerability allowing a successful infection to spread was patched last month on the majority of the fleet, the communication capabilities of the malware have been blocked and the outstanding systems are in the process of being identified, managed and brought into remediation.

We have a detailed actions plan, log and will have teams working over the weekend to ensure any business disruption is minimized.

Best

Sadhu

Sadhu Aufochs Johnston | City Manager
City of Vancouver | 453 W 12th Avenue
Vancouver | BC V5Y 1V4
604.873.7627 | Sadhu.johnston@vancouver.ca
Twitter: sadhuajohnston