CYBERSECURITY COMMUNICATION

Please circulate

February 20, 2020

To: University Cybersecurity Communication Recipients
From: University Systems
RE: Ransomware Targeting UVic

University Systems has analyzed a series of malicious emails and found evidence that UVic users are being targeted by an email-based ransomware attack.

Example 1:

- A campus user received an email from a fake UVic account referencing an updated contract
- The email contained a link to a password-protected file “contract.zip” and the user was provided with the passphrase
- The archive contained a malicious “contract.scr” file; this file was ransomware and would begin to encrypt files if opened

Example 2:

- A campus user received an email claiming to be a package delivery notification
- The email contained a password-protected file “Receipt-Tracking-Number.zip” and the user was provided with the passphrase
- The file also contained ransomware

In both cases, the targeted user correctly identified the email as suspicious and reported it, allowing our team to perform the above analysis.

University Systems is continuing to investigate these attacks and wanted to make you aware that this scam is targeting UVic users. If you encounter a suspicious message, please report it using the Report Phishing button or by contacting the Computer Help Desk. To learn more about how to identify malicious email messages, please visit www.uvic.ca/phishing.

If you have any questions about this notice, please reply to this message.

Regards,

Marcus

Marcus Greenshields
Cybersecurity Working Group
University Systems
University of Victoria

University of Victoria

To verify the authenticity of this message, visit:
www.uvic.ca/systems/verify