VERMONT INTELLIGENCE CENTER **16 OCTOBER 2020**

Ransomware Advisory for Vermont School Districts
Cyber Threat Intelligence

(U) Overview

(U) In the midst of the COVID-19 pandemic, many, if not all, educational institutions nationwide have had to switch to a remote learning environment and, as a result, have become easier targets for cybercriminals. Cybercriminals use various techniques to exploit vulnerabilities. One popular technique is the use of ransomware, which is a type of malware that cybercriminals use to encrypt data and to extort money from their victims. Ransomware often starts with phishing e-mails containing malware-embedded attachments that, if opened, install malicious content and infect the system.

(U) Transitioning to a remote environment, schools are at greater risk of falling victim to a ransomware attack. Students and teachers have become more reliant on the Internet and digital tools, like Google Drive and Zoom, to access information and to connect with classmates and colleagues. A lot of the interactions students and teachers faced in person have now moved online, so it is necessary to ensure these interactions, and information that is shared, are protected.

(U) Vermont schools are not invulnerable to ransomware attacks, and schools should remain vigilant on maintaining a safe cyber security posture.

(U) Mitigation Recommendations for Vermont Schools

(U) Offline Data Back-ups | *Users should have multiple back-ups of critical data and applications.*

(U) Continuous Security Awareness Training | *Staff and students should be informed about current and emerging cybersecurity risks and phishing e-mails.*

(U) Use a Trusted Antivirus Software | *Antivirus software is critical for every computer, tablet, and smartphone. Each educational institution is encouraged to research available options and to determine what is best suited for their community.*

(U) Routinely Scan and Update Computers and Software | *As many school districts have distributed devices to students and teachers, a remote wipe capability is encouraged to be able to track the devices, as well as to erase data on the devices remotely if they were to be stolen or lost.*

(U) Contact Criminal Cyber Analyst Megan Faulkner at Megan.Faulkner@vermont.gov to share information regarding malicious cyber activity affecting your school district.

This reporting is not for investigative purposes. The information will be used to share with other entities to determine if a threat is a national or localized concern, in an effort to prevent the compromise of other systems.

Vermont Intelligence Center | 188 Harvest Lane, Williston VT 05495 | 802-872-6110 | e-mail: dps.vic@list.vermont.gov