Cyber Informational Message

Connecticut Intelligence Center / 1111 Country Club Road / Middletown, CT 06457
(860) 706-5500 / ctic.cyber@ct.gov

TLP:WHITE

CYIM 20-008 **17 April 2020**

Sextortion Email Campaign

(U) SCOPE: The Connecticut Intelligence Center (CTIC) is providing this information for situational awareness as there has been a large volume of sextortion emails sent to citizens in the state over the last several days. The information used in this product was derived from cyber incidents reported to CTIC.

(U) SUMMARY: CTIC has recently received several reports of citizens in the state receiving "sextortion" emails. This well-known scam addresses the targeted person by name and references one of their passwords, often in the subject line, to catch their attention. The email then claims to have hacked their computer and filmed them watching pornography. The malicious actor threatens to send the videos to all of the victim's contacts unless they pay a bitcoin ransom. The passwords used in these scams are obtained from large data breaches that were leaked onto the web and it is important to note that the victim's computer was not actually hacked. It is likely the extorters behind this campaign are capitalizing on the current shutdowns, which has resulted in many people working from home and using their personal emails.

(U) MITIGATION: Users should ensure they change the passwords for any of their accounts that use the mentioned password, and delete the email, as there is no further threat.

(U) INDICATORS: The email addresses used in this campaign were comprised of 10-15 randomized characters @outlook.com. Furthermore, the bitcoin addresses used had three asterisks inserted somewhere in the start of the address, in an effort to avoid automated detection or analysis. All of the bitcoin addresses used in this campaign had the same format and included a caveat below the address telling users to remove the *** and then copy and paste the address as it is case sensitive. The originating IP address for these emails comes from Microsoft and should not be blocked, as it is a legitimate mail server.

(U) CTIC will continue to monitor the situation and will keep its partners updated on any changes or new information. Incident reporting and/or inquiries should be directed to CTIC at ctic@ct.gov or (860) 706-5500.