Fire Chief's and Public Safety Executives:

In recent weeks, the Department of Public Safety assisted in two very significant cyber attacks on municipal and county agencies in Colorado and is investigating a third. The confirmed attacks used ransomware that exploits known vulnerabilities for which patches were available last year. These attacks directly impacted public safety entities, degrading their ability to function and threatening critical public safety services.

The ransomware variant has been identified as BlackCat, which is a Ransomware-as-a-Service (RaaS). It has impacted at least 60 known entities nationwide since March. The typical initial access method is via compromised user credentials through phishing or similar means.

The primary advice for dealing with this in advance of an attack is:

1. Make sure your systems are patched
2. Have people change-up their passwords (consider forcing password updates)
3. Use multi-factor authentication
4. Enforce account lockouts after a maximum of six (6) bad login attempts with a requirement that an administrator must unlock the account
5. Make sure your IT folks are part of Colorado Threat Information Sharing (CTIS). They can contact Kevin McElyea (kevin.mcelyea@state.co.us) at the CIAC to be added to the CTIS list.

Contact the MS-ISAC's 24x7 Security Operations Center via soc@msisac.org or 1-866-787-4277 immediately if you suspect your organization is having an incident, and contact the CIAC at cdps_caic@state.co.us or at 877-509-2422 as well.

For your agency's IT professionals:

1. The Indicators of Compromise (IOCs) can be found at:

   https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/an-investigation-of-the-blackcat-ransomware-via-trend-micro-vision-one/an-investigation-of-the-blackcat-ransomware-via-trend-micro-vision-one-iocs.txt

2. Sign up for the Multi-State-Information Sharing and Analysis Center's free Malicious Domain Blocking and Reporting if your organization does not already have DNS protection technologies in place. (https://www.cisecurity.org/ms-isac)

Stay safe,

Mike Morgan, Director

COLORADO
Division of Fire
Prevention & Control
Department of Public Safety