(U) VFC Highlight #18-06: Ransomware Affecting Government Systems

(U) According to the United States Department of Justice , ransomware is the fastest growing malware threat with more than 4,000 ransomware attacks occurring daily.

April 6, 2018; Tracked by: HSEC-1

(U) Key Points

- (U) The Multi-State Information Sharing & Analysis Center (MS-ISAC) is reporting an increase in ransomware incidents targeting state, local, tribal, and territorial (SLTT) governments.
- (U) Law enforcement agencies and emergency service providers have experienced a surge in attacks affecting 911 systems, some with the SamSam* ransomware variant.
- (U) SLTT governments are lucrative targets for cybercriminals because of the sensitive data maintained in their systems, the critical nature of the services they offer, and the limited resources to secure their systems due to lack of funding.
- (U) The majority of ransomware attacks begin with a simple email phishing campaign.

(U) For additional information on SAMSAM and Indicators of Compromise (IOC), contact (MS-ISAC) at www.msisac.org or by calling 866-787-4722. For in-depth guidance on ransomware click here.

(U) Law Enforcement and Local Government Agencies Hit with Ransomware

- (U) In January 2018, law enforcement agencies in Illinois, Maine, Massachusetts, and Tennessee paid an undisclosed amount of money to gain access to files that had been locked through the use of ransomware.
- (U) In February 2018, Davidson County (NC) was the victim of a ransomware attack against 70 of the county's 90 servers which affected almost all operations including its police and 911 call center.
- (U) In March 2018, a local Virginia law enforcement agency was hit with ransomware that affected the 911 emergency system used by four different localities.
- (U) In March 2018, a ransomware attack against Baltimore (MD) disrupted their 911 dispatch system for 17 hours.
- (U) In March 2018, the city of Atlanta (GA) experienced a disruption of services because of a ransomware attack that forced the postponement of court dates, delayed payroll, and exposed employee data.

(U) Tips for Preventing a Ransomware Attack:

- (U) Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- (U) Keep operating systems patches up-to-date.
- (U) Enable a personal firewall on agency workstations.
- (U) Maintain up-to-date antivirus signatures and engines.
- (U) Restrict users' ability (permissions) to install and run unwanted software applications.
- (U) Regularly backup files and disengage the backup system from the network when not actively using. This will prevent backup files from being corrupted even if the network is infected.
- (U) Maintain situational awareness of the latest threats.

(U) If the Victim of a Ransomware Attack:

- (U) Immediately isolate the infected computer .
- (U) Isolate or power-off affected devices that have not been completely corrupted.
- (U) Quickly secure backup systems by taking them offline.
- (U) If available, collect and secure partial portions of the ransomed data.
- (U) Change all online account and network passwords after removing the system from the network.
- (U) Delete registry values and files to stop the program from loading.
- (U) Implement your security incident response plan.
- (U) Federal partners recommend ***NOT*** paying the ransom.

(U) Please report any information pertaining to ransomware attacks against government agencies to the VFC at VFC@vsp.virginia.gov.