UNCLASSIFIED

4/8/2016

Kansas Intelligence Fusion Center

Informational Graphic: Ransomware

Executive Summary. We assess with **HIGH CONFIDENCE** that critical infrastructure systems in Kansas will be exploited by Ransomware throughout 2016 and the foreseeable future based on a large body of both national reporting and on dialogues with cybersecurity partners throughout the state and region. We also assess with **HIGH CONFIDENCE** that many entities in Kansas are not prepared to deal with this threat and will be forced to pay malicious actors or permanently lose critical data.

Ransomware Description. Ransomware is a form of malware used by criminal actors to deny user access to critical data. Ransomware achieves this through encryption of the data unbeknownst to the user and then offers a decryption key in exchange for bitcoins or other currency. Although Ransomware has existed since 1989, nextgen ransomware is evolving in complexity and has emerged as the preferred tool for criminal cyber actors because of ease of use and effectiveness. Current Ransomware iterations may encrypt data while offline, have signatures only minimally detected by anti-virus, and may not require the operating system to run prior to booting. While Ransomware affecting home users may only extort them for a couple hundred dollars, Ransomware targeting CIKR may demands tens of thousands.

Healthcare Nexus. Ransomware poses a particularly concerning risk to the healthcare sector because of the criticality of affected system. OSINT has previously identified medical devices as key pivot points for attackers within healthcare environments. Given this interconnectivity (the "internet of things") the likelihood of an infected desktop being used to connect to critical systems is high. Furthermore, the 24/7 nature of healthcare systems may preclude timely patching. The number of healthcare data breaches in the five years leading up to 2015 doubled according to one OSINT source. We assess with **HIGH CONFIDENCE** that these factors combined with the high criticality of healthcare systems makes this sector a primary target.

Case Studies.

- Hollywood Presbyterian Med Center[1] [2] [3]
- MedStar Health [1] [2] [3]
- Methodist Hospital [1] [2] [3]
- Ottawa Hospital [1] [2] [3]
- Chino Valley Medical Center [1]

Ingress. Ransomware gains a foothold in systems in much the same fashion as other malware. Initial vectors include:

- **Phishing or Spear-Phishing**.
- **Traffic Distribution System (TDS)** – Users are redirected to a site hosting an exploit kit
- **Maladvertisement** – A form of TDS using advertisements that may appear on normally legitimate sites
- **Downloaders** – Ransomware may be coupled with other malware and packaged in freeware or pirated media
- **Self-Propagation** – Once malware is on a single machine it may attempt to spread to other devices on a given network

Prevention. We recommend implementation of the following strategies:

- Employ offsite data backup and recovery for all critical systems
- Use application whitelisting to prevent unauthorized processes
- Ensure operating system and all software packages are updated/patched
- Maintain anti-virus software
- Use Microsoft Office Viewer (no macros)
- Restrict administrator privileges
- Ensure segmentation of organization's network
- Restrict personal email usage; block or scrub external email

Response. IT personnel should consider response before the malware is extant. Otherwise, response options may be limited to acquiescence or acceptance of data loss. Preferred actions include:

- **Isolation.** Infected device is immediately quarantined from intranets.
- **Restoration.** Device is returned to last good state using backup or restoration point.
- **Notification.** User/IT personnel immediately notify stakeholders.

Reachback and Reporting. State government entities in Kansas affected by Ransomware should immediately contact 785-296-0814 to report the incident. The Kansas Intelligence Fusion (KIFC) center is interested in partnerships with private sector critical infrastructure entities within the state. The KIFC may be reached at intelligence.fusion@ag.ks.gov for intel support