Notice for CAPP Customers

Justin Harwell, CEH, ECSA, LPT, Security+ | Sr. Information Security Consultant | CynergisTek

Recent Ransomware Threats for Hospitals

Roughly two weeks ago Hollywood Presbyterian Medical Center (HPMC) fell victim to the effects of a highly orchestrated and malicious cybersecurity attack. This attack infiltrated and affected the operation of HPMC's complete internal enterprise-wide hospital information system.

The incident began on February 5, 2016, when staff members at HPMC were prevented access to patient data stored in the hospital's internal computer network. Upon further investigation by the organization's IT department, it was determined that they had been subject to a specific type of malware attack known as "ransomware". This particular type of malware locked access to various computer systems as well as specific files on the company's network and prevented HPMC from sharing communications. Since, CynergisTek has heard from several hospitals about attempted malware attacks this week. It is imperative that we explain exactly what ransomware is, how it works and how to protect yourself, your staff and your organization from such an exploit.

Ransomware is a type of malware that restricts or revokes access to the infected computer system or network in some way. This type of malware is "scareware", as it extorts from its victims a fee or "ransom" through bitcoin and other encrypted digital currencies to regain or grant access to the end user's system(s) in order to restore data. Some forms of ransomware systematically encrypt files on the system's hard drive (with what is known as "Cryptolocker"), which makes it difficult or impossible to decrypt without paying the ransom for the encryption key. Others may simply lock the system in its entirety and display a message intended to coax the user into paying, while still ultimately leaving the system in an unusable or "bricked" state.

Ransomware is not new. It has been around since about 2009 originating from Eastern Europe and spread rapidly. Recently a new variant of ransomware was released nick named "Locky". Shortly after being identified researchers saw upwards of 4,000 new infections per hour, or approximately 100,000 per day. Locky is reportedly being distributed via a Microsoft Word attachment with malicious macros in it. Victims typically receive an email with an attached Word document purporting to be an invoice seeking payment for some product or service. Recipients who click on the attachment are presented with a document containing scrambled content and an instruction to click on an Office macro to unscramble it. Once enabled, the macro downloads Locky, stores it in the temporary folder and executes it. Locky infected thousands of machines before researchers and A/V vendors could develop a signature and update their systems.

While all malware is disseminated via different methods, ransomware typically propagates as a Trojan virus. A Trojan's payload is disguised as a seemingly legitimate file, and once executed in a system, ransomware can either (1) lock the computer screen/system or (2) encrypt predetermined files with a password, rendering them unusable/unreadable. Users may encounter this type of threat through a variety of means, including but not limited to; unwittingly downloading a malicious file disguised as something legitimate, visiting malicious or other compromised websites, downloading an attachment from a spammed email, or downloading an attachment from an email sent by a legitimate contact whose account was compromised. Some types of ransomware arrive as a payload and as such are either "dropped" or deposited by other types of malware onto the system as an aside.

Original reports noted that hackers were demanding the hospital pay a sum of 9000 bitcoins or approximately $3.4 million USD to unlock the system and restore access. However, it has since been confirmed that HPMC settled on an amount totaling 40 bitcoins or the equivalent of $17,000 USD. The malware used in the HPMC attack executed both behaviors as previously defined, both locking down the entire enterprise network, as well as access to specific files within individual host machines.

CynergisTek takes cybersecurity and all associated threats thereof very seriously, and as such are constantly assisting our customers to review their security posture in an effort to maintain the highest level of integrity, confidentiality and sustainability possible. Moving into 2016, we are well aware of the specific and ongoing need for our clients to maintain a strong and formidable security infrastructure.

That being said, we continue to work with our clients to assess and reassess specific, tangible and measurable security vulnerabilities within their networks. We also understand the need to test the effectiveness of overall staff awareness with repeated company controlled phishing campaigns. These campaigns have proven extremely valuable in providing a baseline assessment of the organization's initial security awareness level, while continued campaigns have shown a measurable difference in the overall effectiveness of increased staff awareness.

The links below provide some informational references that should be helpful to you and your organization. The first links to an attachment (verified secure) that both outlines and explains what ransomware is, how you may become infected and measures how to protect yourself and your organization from such a risk. The second links to tips on what to look for in a suspicious email. Please share this with your staff and organization, as everyone should be alert for malware and very suspicious of emails with attachments or links.

Link to ransomware definition ----------> http://tinyurl.com/trendmicro-ransomware-jpg
Link to tips on suspicious emails ----------> http://cynergistek.com/phishing-awareness/

If you have any questions please do not hesitate to contact us.

Contact us: advisory@cynergistek.com