ULEDGER

ENCRYPTION KEYS ARE NOT A COMPREHENSIVE REMEDY

Ransomware Threat:

On September 15, 2016, the Federal Bureau of Investigation issued Alert Number I-091516-PSA. The PSA explicates the risk and shortcomings of relying upon encryption as a comprehensive platform for email security.

Salient points of the PSA:

- Ransomware as is a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid.;
- Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware, or through drive-by downloads (which does not require user-initiation) from a compromised Web site;
- New ransomware variants are emerging regularly and cyber-security enterprises report that infections are at an all-time high;
- Recent variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts, thereby multiplying the number of potential infected servers and devices on a network;
- Actors engaging in this targeting strategy are also charging ransoms based on the number of host (or servers) infected (thus leveraging the number of hosts to support an exponentially higher ransom from the victim, who, in turn, faces exponentially increased risk exposure as the volume of information increases);
- Victims who have been infected with these types of ransomware variants have not been provided the decryption keys for all their files after paying the ransom, and some have been extorted for even more money after payment, with the result that victims could suffer increased costs for recovery of their encryption keys, prolonged delay in recovering their keys, the possibility that victims will not obtain full decryption of their files or never even receive their encryption keys back.

Executive Summary:

The FBI makes it clear that reliance upon encryption as a comprehensive solution for cyber security is not sufficiently secure. Ransomware attacks can compromise encryption systems and both deprive victims of data recovery and expose victims to exponential risk, even while extracting ransom payments. Responsible security must extend beyond mere encryption.