What You Don't Know About Ransomware Can Hurt You

This morning you were greeted by a large red message replacing your login screen. "Your Computer Has Been Locked! Pay the Fine or Your Data Will Be Destroyed." A hacker is threatening to destroy all local files and data unless you pay a fine through an untraceable payment system and a ticking time bomb counts down the seconds until all your data is destroyed. "Ransomware" infections like this originated in Russia in 2005 and have exploded to an estimated 30,000 incidents per day worldwide today. There are even dark web vendors providing ransomware to clients as a service.

Large enterprises and small businesses are increasingly contacting security firms to confidentially scope the resulting damage, identify the infiltrated security hole, repair the systems involved and implement a preventative solution. You may not hear about these potentially disastrous breaches since the publicity surrounding a breach could be more damaging than the breach itself. But there's little doubt that, at one time or another, the data of a business you use every day has been ransomed. Online security experts and authorities have been unlocking the secrets of a wide and growing range of ransomware types for over a decade.

Ransomware enters a system as a trojan, through a downloaded file or a network service security hole. The trojan unloads malware that generates a warning or locks the system so that the user must pay for an encryption key to access the files. Common methods of locking the files include setting the Windows shell to itself or editing the master boot record or partition table. Ransomware locks files until the user makes payment through an untraceable system such as Bitcoin, Ukash or Paysafecard. Security technology providers have documented some of the most damaging ransomware technology types including Reveton, CryptoLocker, TorrentLocker and Cryptowall.

Reveton begins as a Citdel (Zeus) trojan, generating a police warning that the infected personal computer has been used in illegal activities. Reveton might even display computer webcam footage to convince the user that he has been under police surveillance. CryptoLocker.F disrupted the Australian Broadcasting Corporation, evading standard security features by arriving as a parcel delivery notification email, downloading payload after the user visits a webpage and enters a CAPTCHA code. TorrentLocker gathers email addresses from infected computers and distributes itself to victims' contacts. CryptoWall distributes malware via an online ad network, then steals passwords and Bitcoin wallets. Especially damaging is CryptoWall's ability to encrypt files on any drive that connects to the infected computer.

The infection rate and profitability of ransomware is astounding. In just six months, CryptoLocker, for example, infected over 500,000 computers. Bitcoin, in protecting the anonymity of the malware hackers, is rapidly paving the way for ransomware to become a growing industry. Profits are significant, with CryptoLocker netting up to $27 million and CryptoWall, $15 million. A single ransomware command server alone might rake in $5 million in a year. Ransom amounts for data on individuals' home systems are limited by what an individual is willing to pay, often around $200. But when ransomware infects the laptop of a key business executive, the value of the business' reputation and future determines the hacker's fee.

What can you do to ensure your business isn't a victim? A company-wide policy of keeping up-to-date anti-virus detection software on all systems is a given. A requirement that employees, even top executives, automate remote system backups and store date in the cloud is another strong deterrent. The best insurance though is an ongoing relationship with experienced networking experts like Terrapin Systems with partners like Fortinet, who can survey your environment, identify potential breach opportunities and recommend the best technology to keep your data safe.

Contact Terrapin Systems today to schedule a consultation with a security partner who can secure your network.

TERRAPIN SYSTEMS:

Please contact us for a consultation.

Chris Becerra
info@terrapinsys.com
(408) 705-4126