TAKE THE RANSOM OUT OF RANSOMWARE

HOW TO AVOID HAVING YOUR DATA BEING HELD HOSTAGE

Ransomware is a form of malware that encrypts victim's files with unbreakable encryption and then demands payment, typically around $200 to $500 in bitcoins, in order to unlock and get your data back.

THE PROLIFERATION OF RANSOMWARE

Ransomware has rapidly become one of the most widespread and damaging causes of downtime and data loss for IT systems. It has captured the attention of the press and end-users with leading publications calling 2016 "the year of Ransomware."

BACKGROUND ON RANSOMWARE

Ransomware has been around for over a decade but early forms were largely ineffective. They did not permanently lock or encrypt files and they were typically fairly easy to remove or avoid. With Cryptolocker came powerful encryption technology to encrypt files and extort payment in bitcoins through anonymous transaction servers.

Joseph Bonavolonta
Assistant Special Agent in Charge of the Cyber and Counterintelligence Program
FBI, Boston

Besides CryptoLocker, the most popular variants include TorrentLocker, CryptoWall, CBT-Locker, TeslaCrypt, Locky, plus many others, and they all share the following major components.

- They use strong, unbreakable encryption. Often this is 256 bit AES, RSA or ECC (Curve) based encryption which is essentially unbreakable.

- They employ some form of online network communication such as I2P network proxies or TOR which can provide anonymous backend infrastructure.

- They require anonymous electronic Payment via bitcoins typically through TOR.

HOW DOES AN ENTERPRISE MAKE SURE THEY NEVER HAVE TO PAY RANSOM?

For our ransomware offense we want to take some proactive measures that will attempt to keep ransomware out of all user and server-based systems.

Keep all of your software and operating systems up to date.

Use antivirus software for virus detection on all systems.

Educate users on security protocols.

For our ransomware defense, we want to deploy countermeasures that can block the execution of ransomware and prevent it from encrypting our data.

Disable ActiveX content in Microsoft Office applications.

Have firewalls block TOR, I2P and restrict ports.

Block binaries from running from popular ransomware installation paths.

WHAT DOES A GOOD BACKUP STRATEGY LOOK LIKE FOR RANSOMWARE PROTECTION?

Follow the "rule of three" for backup and recovery. The rule of three simply states that we want three copies of our data, across two different media types (e.g. disk and cloud or disk and tape), with at least one copy off-site.

Make sure you backup data on all systems, not just mission-critical systems. Ransomware can attack both Windows and Mac based user systems and servers.

Create some physical isolation between at least one copy of your data. That geographic isolation will help make sure that ransomware cannot spread across all copies of your data.

CLOUD EMPOWERED CONTINUITY

Ransomware protection should include both local and cloud-based backups. You can quickly recover infected systems with backups stored on the local backup appliance and Cloud-based backups provide an easy way to move copies of your backups off-site.

Ideally, your backup solution will provide the following capabilities.

- Flexible cloud deployment options
- Instant recovery capabilities to spin up workloads in minutes from backups
- Linux-based backup software – not Windows-based which accounts of the vast majority of attacks today

KEEP YOUR BUSINESS RUNNING WITH UNITRENDS

Unitrends is trusted by business visionaries and IT leaders and professionals who know that in today's digital world protecting their ideas and keeping their businesses running is non-negotiable. The Unitrends Connected Continuity Platform™ enables organizations of all sizes to protect their data and assure business continuity for physical, virtual, and cloud based environments.

UNITRENDS
unitrends.com