The Rise of Ransomware

Ransomware has evolved from a low-grade nuisance to a sophisticated multimillion-dollar criminal business that now targets both individuals and corporations. It is a criminal business model that uses malicious software to cryptographically hold your personal data hostage. While an increasingly urgent challenge, ransomware can be prevented through proper training, the right risk management processes, and advanced endpoint technology. Unit 42, the Palo Alto Networks® threat intelligence team, recently released an in-depth report on ransomware history, evolution and effective defenses.

**Who’s at Risk?**

**Corporations in the crosshairs.** Ransomware attacks can have very public impact, as victim-organization operations may be severely degraded or shut down entirely, which is illustrated by recent attacks on hospitals across the United States. Criminals have realized that this is a lucrative business with low barriers to entry, and ransomware is consequently displacing other cybercrime business models. Moreover, attackers will grow more sophisticated in their ability to determine the value of compromised information, assess the victim organization’s willingness to pay, and demand higher ransoms.

**More platforms.** While historically attackers focused exclusively on Microsoft® Windows® systems, the emergence of ransomware for Android® and – as Palo Alto Networks most recently discovered – Mac® OS X®, demonstrates that no system is immune from these attacks. Nearly all computers or devices with an internet connection are potential victims of ransomware, which will be a more urgent concern with the coming rise of the Internet of Things (IoT) and the attendant proliferation of additional devices, such as home appliances, connected to the Internet.

**WHAT IS RANSOMWARE?**

Attackers must execute five steps for a ransomware attack to be successful:

1. **Compromise and control of the system.** Most attacks begin with spear-phishing, tricking a user with a fraudulent email to open an infected attachment that compromises the system. This may impact a single computer, mobile phone or an entire enterprise.

2. **Prevent access to the system.** Once infected, an attacker either identifies and encrypts certain files types likely to be of value to the victim, such as business documents or family photos, or totally denies access to the entire system through lockout screens or scare tactics.

3. **Alert the owner of the device about compromise, ransom amount, and steps to be taken.** Though seemingly obvious, attackers and victims often speak different languages and have different levels of technical capabilities, so attackers must explain to victims in terms they can understand what has happened as well as the steps to be taken to unlock their devices.

4. **Accept ransom payment.** An attacker must have a way to receive ransom payments while evading law enforcement, which explains the use of anonymous crypto-currencies, such as bitcoin for these transactions.

5. **Return full access upon payment receipt.** Failure to restore compromised systems will destroy the effectiveness of the scheme, as no one pays a ransom without confidence that their valuables will be returned.

**PREPARE FOR PREVENTION**

As ransomware attacks act quickly – typically within minutes of an infection – it is critical to deploy controls that prevent malware from entering your network and executing on the systems storing your valuable data. Ransomware attacks can be prevented, but this requires the right approach. To ensure that your organization is positioned to effectively manage the risk associated with ransomware attacks, we recommend you ask your Chief Information Security Officer the following questions:

1. **Do we protect our endpoints by preventing malware?** Unknown malware prevention systems that identify malicious behaviors are the best defenses against ransomware, as attackers test their attacks against older, legacy anti-virus products to ensure the attacks will go undetected.

2. **What is our back-up and data recovery strategy?** If you can recover encrypted files from backups, you’ll be able to recover from a successful ransomware attack with limited impact to your organization.

3. **What is our plan to handle ransomware attacks, if infected?** Beyond the technical remediation that’s required, be sure to determine when to involve law enforcement and consider the legal implications of paying the ransom.

4. **How does our company regularly train all employees to spot and avoid spear-phishing attempts?** Training employees to avoid spear-phishing emails will limit the potential for ransomware to take hold of your organization.