Ransomware on the Rise

FBI and Partners Working to Combat This Cyber Threat

01/20/15

Your computer screen freezes with a pop-up message—supposedly from the FBI or another federal agency—saying that because you violated some sort of federal law your computer will remain locked until you pay a fine. Or you get a pop-up message telling you that your personal files have been encrypted and you have to pay to get the key needed decrypt them.

These scenarios are examples of ransomware scams, which involve a type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom—anywhere from hundreds to thousands of dollars—is paid.

Ransomware doesn't just impact home computers. Businesses, financial institutions, government agencies, academic institutions, and other organizations can and have become infected with it as well, resulting in the loss of sensitive or proprietary information, a disruption to regular operations, financial losses incurred to restore systems and files, and/or potential harm to an organization's reputation.

Ransomware has been around for several years, but there's been a definite uptick lately in its use by cyber criminals. And the FBI, along with public and private sector partners, is targeting these offenders and their scams.

Latest Ransomware Threat

A fairly new ransomware variant has been making the rounds lately. Called CryptoWall (and CryptoWall 2.0, its newer version), this virus encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It directs the user to a personalized victim ransom page that contains the initial ransom amount (anywhere from $200 to $5,000), detailed instructions about how to purchase Bitcoins, and typically a countdown clock to notify victims how much time they have before the ransom doubles. Victims are infected with CryptoWall by clicking on links in malicious e-mails that appear to be from legitimate businesses and through compromised advertisements on popular websites. According to the U.S. CERT, these infections can be devastating and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

For more information on ransomware in general, visit the U.S. CERT website.

When ransomware first hit the scene, computers predominately became infected with it when users opened e-mail attachments that contained the malware. But more recently, we're seeing an increasing number of incidents involving so-called "drive-by" ransomware, where users can infect their computers simply by clicking on a compromised website, often lured there by a deceptive e-mail or pop-up window.

Another new trend involves the ransom payment method. While some of the earlier ransomware scams involved having victims pay "ransom" with pre-paid cards, victims are now increasingly asked to pay with Bitcoin, a decentralized virtual currency network that attracts criminals because of the anonymity the system offers.

Also a growing problem is ransomware that locks down mobile phones and

Protect Your Computer from Ransomware

- Make sure you have updated antivirus software on your computer

Story Index

By Date

By Subject

- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases
- Foreign Counterintelligence
- General
- History
- Intelligence
- International
- Lab/Operational Technology
- Linguist/Translation Program
- Major Thefts/Violent Crime
- Organized Crime/Drugs
- Partnerships
- Public/Community Outreach
- Public Corruption
- Recruiting/Diversity
- Responding to Your Concerns
- Technology
- Training
- White-Collar Crime

that locks down mobile phones and demands payments to unlock them.

The FBI and our federal, international, and private sector partners have taken proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets that facilitated the distribution and operation of ransomware. For example:

- Reveton ransomware, delivered by malware known as Citadel, falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites or other illegal online activity. In June 2013, Microsoft, the FBI, and our financial partners disrupted a massive criminal botnet built on the Citadel malware, putting the brakes on Reveton's distribution. **FBI statement** and **additional details**.
- Cryptolocker was a highly sophisticated ransomware that used cryptographic key pairs to encrypt the computer files of its victims and demanded ransom for the encryption key. In June 2014, the FBI announced—in conjunction with the Gameover Zeus botnet disruption—that U.S. and foreign law enforcement officials had seized Cryptolocker command and control servers. The investigation into the criminals behind Cryptolocker continues, but the malware is unable to encrypt any additional computers. **Additional details**.

  If you think you've been a victim of Cryptolocker, visit the Department of Homeland Security's U.S. Computer Emergency Readiness Team (CERT) CryptoLocker webpage for remediation information.

- Make sure you have updated anti-virus software on your computer.

- Enable automated patches for your operating system and web browser.

- Have strong passwords, and don't use the same passwords for everything.

- Use a pop-up blocker.

- Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars).

- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.

- Use the same precautions on your mobile phone as you would on your computer when using the Internet.

- To prevent the loss of essential files due to a ransomware infection, it's recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline.

The FBI—along with its federal, international, and private sector partners—will continue to combat ransomware and other cyber threats. If you believe you've been the victim of a ransomware scheme or other cyber fraud activity, please report it to the Bureau's Internet Crime Complaint Center.

Resources:
- Botnets 101
- Taking Down Botnets
- The Cyber Threat
- Cyber Threats Against the Financial Sector