THE FBI FEDERAL BUREAU OF INVESTIGATION

Incidents of Ransomware on the Rise
Protect Yourself and Your Organization

04/29/16

Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation.

And, of course, home computers are just as susceptible to ransomware, and the loss of access to personal and often irreplaceable items—including family photos, videos, and other data—can be devastating for individuals as well.

Ransomware has been around for a few years, but during 2015, law enforcement saw an increase in these types of cyber attacks, particularly against organizations because the payoffs are higher. And if the first three months of this year are any indication, the number of ransomware incidents—and the ensuing damage they cause—will grow even more in 2016 if individuals and organizations don't prepare for these attacks in advance.

Tips for Dealing with the Ransomware Threat

While the below tips are primarily aimed at organizations and their employees, some are also applicable to individual users.

Prevention Efforts

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.

- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).

- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.

- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.

- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.

- Disable macro scripts from office files transmitted over e-mail.

- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

Business Continuity Efforts

- Back up data regularly and verify the integrity of those backups regularly.

- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

More info

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

One the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals.

And in newly identified instances of ransomware, some cyber criminals aren't using e-mails at all. According to FBI Cyber Division Assistant Director James Trainor, "These criminals have evolved over time and now bypass the need for an individual to click on a link. They do this by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers."

The FBI doesn't support paying a ransom in response to a ransomware attack. Said Trainor, "Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

So what does the FBI recommend? As ransomware techniques and malware continue to evolve—and because it's difficult to detect a ransomware compromise before it's too late—organizations in particular should focus on two main areas:

- Prevention efforts—both in both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack. (See sidebar for more information.)

"There's no one method or tool that will completely protect you or your organization from a ransomware attack," said Trainor. "But contingency and remediation planning is crucial to business recovery and continuity—and these plans should be tested regularly." In the meantime, according to Trainor, the FBI will continue working with its local, federal, international, and private sector partners to combat ransomware and other cyber threats.

If you think you or your organization have been the victim of ransomware, contact your local FBI field office and report the incident to the Bureau's Internet Crime Complaint Center.

Resources:
- More on the FBI's Cyber Division
- Ransomware brochure
- Internet Crime Complaint Center (IC3)