Published on *The National Law Review* https://natlawreview.com

Ransomware on Rise - FBI Releases Alert and Guidance

Article By:

Katherine E. Armstrong

Jay Brudz

Kenneth K. Dort

Anthony D. Glosson

Key Takeaways:

- **Implement and follow robust data security practices.**
- **Train employees to be on the lookout for suspicious emails and websites.**
- **Establish business continuity plans that include regular system backups.**
- **Create and implement rigorous data retention policies to ensure that only necessary data is maintained, thus minimizing the amount of data subject to ransom.**

Ransomware attacks, which employ a devious and malicious type of malware that encrypts or locks valuable digital files and then demand a ransom payment to release those files, are on the rise. Indeed, the May 2016 edition of the *ABA Journal* magazine reports that the number of detected ransomware variants has grown to nearly 3.8 million in 2015 (from 638,000 in 2014). Ransomware attacks hospitals, businesses, state and local governments, and other institutions where access to information is critical to the target's operations. On April 29, 2016, the FBI's Cyber division issued an alert and guidance.

Ransomware generally enters the victim's systems via (i) an established attack vector such as a user visiting a compromised website, (ii) the exploit of unpatched systems, or (iii) most commonly, via a social engineering or phishing attack which attempts to get an authorized employee to execute a malicious email or click a link to a compromised site. Once it is established, the malware begins encrypting files and folders on local drives, any attached drives, backup drives and in some instances any device connected to the same network. Victims are usually unaware of the infection until they can no longer access their data or until they begin to see ransom messages on their computer. The attackers then demand payment for the key code needed to unencrypt the locked files. While older

variants of ransomware had flaws in their encryption implementations allowing some hope of recovering your data without the key, newer versions use very robust encryption for which cracking is currently infeasible.

The FBI does not recommend paying a ransom in response to a ransomware attack because, according to FBI Cyber Division Assistant Director James Trainor, (i) paying a ransom will not guarantee that an organization will get its data back, and (ii) the payment will only serve to encourage more cyber criminals to undertake additional ransomware attacks. This is hard advice for many organizations to take. Faced with the permanent loss of valuable data and a ransom demand that can sometimes be only hundreds of dollars, some organizations are tempted to pay the ransom and perpetuate the cycle. Accordingly, the FBI recommends that organizations focus on prevention, incident response, and remediation.

While there can be no guarantee against becoming a ransomware victim, this alert recommends the following information governance and security practices to close off attack vectors and manage and recover from a ransomware attack:

Prevent:

- Maintain current versions of operating systems and applications loaded on all devices with network access.
- Ensure anti-virus solutions and all other defensive measures are set to update automatically.
- Implement the principle of least privilege. Manage the use of sensitive accounts such that network users do not have privileges any higher than are needed to complete their respective tasks—for example, a user generally should not be able to write to a directory if they only need to view the files therein.
- Disable any and all macro scripts from office files transmitted via email.
- Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Allow systems to execute “whitelisted” programs only (i.e., those that are known and permitted by security policies).
- Seek to separate networks and files based upon which parts of an organization need access to those resources.
- Train users in the detection and prevention of social engineering and phishing attacks.
- Deploy proxies and firewalls to block malicious or unknown sites and eliminate malware command and control channels.

Respond:

- Create a standing incident response team and practice various response scenarios using

table-top exercises and drills. Make sure key functions such as IT, Legal, Finance, HR and senior business leadership are represented on the response team.

- Create business continuity plans which allow the business to function in the event of loss of access to key data.

- Create employee, customer and stakeholder communication plans to ensure that all key constituencies are properly informed.

Recover:

- Back up data regularly, verify the integrity of those backups, and ensure they are secure and separate from broadly-accessible system locations. Remember, if a user can access a specific network location, so can the ransomware.

- Implement good information governance practices so you know which data are critical to the operation of your business.

- Ensure that your failover/disaster recovery sites are not accessible within the same user contexts as your production sites. Test your failover and disaster recovery capabilities for mission critical systems regularly.

- Analyze any contractual or other liabilities you may have for losing access to customer or business partner data.

- Conduct an after-action review to determine the root cause of the incident and develop, document and internalize lessons learned from the incident response process.

National Law Review, Volume VI, Number 133

Source URL:https://natlawreview.com/article/ransomware-rise-fbi-releases-alert-and-guidance