New FBI Ransomware Alert: Bureau Provides Key Guidance for Prevention and Business Continuity Planning

Andrew B. Flake and Barbara J. Rogers

The Cyber Division of the Federal Bureau of Investigation (FBI) recently issued a new ransomware notice. The notice encourages organizations, regardless of industry and size, to focus on two areas in their efforts to minimize ransomware risk: prevention and business continuity.[1]

As described by the Cyber Division, "ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems." Increasingly, attackers are "spear phishing," which is sending personalized and targeted e-mail, to deliver the virus. The e-mail will contain a seemingly legitimate attachment (e.g., an invoice or electronic fax) or website link, but when an end user clicks on it, the attachment or link actually contains malicious code. Once activated, the code infects the user's computer and spreads to servers, back-up drives, attached drives and any other networked electronics, hindering proper operation and preventing the organization from accessing its data. At that point, in exchange for a purported decryption key to unlock the seized data, the hacker demands payment of a ransom, usually with bitcoins to hinder any payment tracking.

According to the FBI, ransomware attacks increased significantly in 2015, and the FBI expects they will "grow even more in 2016, if individuals and organizations don't prepare for these attacks in advance."[2] Recent attacks bear out this prediction, with victims including Hollywood Presbyterian Medical Center, which paid a ransom in February to regain control of its data and computer systems, and MedStar Health, which in March lost computer system access at ten (10) hospitals and 250 outpatient centers.

Below are the key tips identified by the FBI, in the major categories of prevention and business continuity, by which organizations can better protect themselves from the threat of a ransomware attack.

Tips for Prevention

- Implement an awareness and training program. Such a program can ensure employees are aware of the ransomware threat and of their own critical roles in protecting the organization's data. Because end users are targeted, employees are the first line of defense – or weakest link – when it comes to ransomware attacks.
- Patch operating systems, software, and firmware on digital devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update, and schedule and conduct regular scans.
- Manage the use of privileged accounts, using the principle of "least privilege." Only use administrator accounts when necessary (and remove access when no longer needed) and only assign those users administrative access who absolutely need it.
- Configure access controls, including file, directory, and network share permissions appropriately (again, keeping least privilege in mind). If a user only needs to read specific

1 Ransomware Brochure, FBI Cyber Division, May 2016, accessible at https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure (last accessed May 30, 2016).

2 Hayward, John, *FBI Warns That Ransomware is on the Rise*, May 3, 2016, accessible at http://www.breitbart.com/tech/2016/05/03/fbi-warns-ransomware-rise/ (last accessed May 30, 2016).

files, do not allow the user to have write access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail. Consider using viewer software (like Office Viewer for Microsoft Office) to open files transmitted via e-mail instead of full office suite applications.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers or compression/ decompression programs, including the AppData/LocalAppData folder).

Tips to Ensure Business Continuity

- Back up data regularly and verify the integrity of those back-ups on a regular basis.
- Secure your back-ups, including ensuring back-ups are not connected to the computers and networks they are backing up.

Tips for IT System Configuration

- Implement application whitelisting. The only programs that the IT system can execute should be those known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value, and implement physical / logical separation of networks and data for different organizational units.

As Cyber Division Assistant Director James Trainor acknowledges, "no one method or tool will completely protect you or your organization from a ransomware attack;" nonetheless, "contingency and remediation planning is crucial to business recovery and continuity – and these plans should be tested regularly."[3]

3 Incidents of Ransomware on the Rise, Protect Yourself and Your Organization, April 29, 2016, accessible at https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise (last accessed May 30, 2016).

Authors and Contributors

Andrew B. Flake
Partner, Atlanta Office
404.873.7026
andrew.flake@agg.com

Barbara J. Rogers
Associate, Atlanta Office
404.873.8522
barbara.rogers@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**