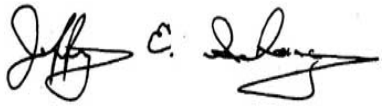
Office of Inspector General
Legal Services Corporation

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

FRAUD ALERT
20-0113-A-FA

TO: Executive Directors

FROM: Jeffrey E. Schanz
Inspector General



DATE: October 2, 2020

SUBJECT: Ransomware Attacks

The Office of Inspector General (OIG) for the Legal Services Corporation (LSC) is issuing this Fraud Alert to provide LSC grantee Executive Directors with current information regarding cyber and ransomware attacks directed at grantee Information Technology (IT) networks. The OIG releases this Fraud Alert to increase grantee awareness about cyber and ransomware attacks and recommend preventative best practices.

The OIG Hotline has recently received several reports of ransomware attacks directed at grantee IT networks. The perpetrators of these attacks exploited weaknesses in grantees' IT infrastructure to disrupt grantee access to data, financial records, and sensitive client information, or to disable servers and back-up servers, pending payment of a ransom.

Ransomware is a type of malware installed on a computer or server that encrypts files, making them inaccessible until a specified ransom is paid. It is typically installed when a user clicks a malicious link and opens a file in an e-mail that installs the malware, or through "drive-by" downloads (an unintentional download of a virus or malicious software most commonly done through phishing emails) from a compromised web site.

The Federal Bureau of Investigation (FBI) has observed cyber criminals using the following techniques and vulnerabilities to infect their victims with ransomware:

- email phishing campaigns: the cybercriminal sends an email containing a malicious file or link which deploys malware when clicked by a recipient;
- exploitation of remote desktop protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer remotely over the internet;

- exploitation of software vulnerabilities: cybercriminals take advantage of security weaknesses in widely used software programs to gain control of computer systems and deploy ransomware.

The most effective defense against ransomware is creating a system of prevention and detection. A system of prevention and detection should include an updated firewall, appropriate spam filters, current data backups, and a risk awareness plan for staff. If a ransomware attack does occur, keeping current data backups should allow grantees to restore data and operations of systems and could greatly reduce the impact of an attack from crippling your organization.

Paying a ransom does not guarantee an organization will get its data back, as there have been cases in which organizations never received a decryption key after paying the ransom and therefore were unable to regain access to their data and/or servers. While the FBI does not advocate paying a ransom, it recognizes that executives, when faced with inoperability issues, will evaluate all options to protect their employee and client data. Whatever the case, the LSC OIG strongly suggests grantees contact the appropriate federal, state, or local law enforcement authorities for advice in the event they are attacked by cybercriminals.

To avoid such attacks, the LSC OIG recommends grantees consider adopting the following cyber security recommendations developed by the FBI and the Federal Communications Commission (FCC) at https://docs.fcc.gov/public/attachments/DOC-306595A1.pdf.

Best Practices

The best way a grantee can protect its IT systems is to be proactive and aware of threats to its infrastructure. The FBI recommends organizations focus on:

- prevention efforts – through both employee training and robust technical prevention controls; and
- the creation of a solid business continuity plan to deploy in the event of a ransomware attack.

To prevent cyberattacks and ransomware:

- make sure all grantee employees are trained on ransomware prevention and are aware of their critical roles in protecting the organization's data;
- update or "patch" all grantee operating systems, software, and firmware on digital devices to protect them against RDP and software vulnerabilities (this may be made easier through a centralized patch management system);
- provide an updated firewall for the organization and route internet traffic through that internet connection;
- configure firewalls to block access to known malicious IP addresses;

- enable strong spam filters to prevent phishing emails from reaching their intended targets and scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- ensure all anti-virus and anti-malware solutions are set to automatically update and conduct regular scans;
- manage the use of privileged accounts based on the principle of least privileged: users should not be assigned administrative access unless absolutely needed and those with a need for administrator accounts should only use them when necessary;
- limit the authority of users to install software on the network or to local machines;
- configure access controls (including file, directory, and network share permissions) appropriately; if users merely require read-only authorization to certain information, ensure they do not also have write-access authorization to 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);
- back up data regularly and verify the integrity and restoration of those backups;
- place at least one copy of the system backup in the cloud or, at the very least offsite;
- secure your backups and make sure they are separate from the computers and networks they are backing up; and
- have a thorough understanding of how your cloud provider handles cyberattacks, including ransomware attacks.

For further information, please visit, https://www.fbi.gov/investigate/cyber.

The Cybersecurity and Infrastructure Security Agency (CISA) also offers alerts and tips found at: https://us-cert.cisa.gov/ncas/alerts.

The LSC OIG's Audit Unit conducts vulnerability assessments of grantees' information systems and networks to identify potential security vulnerabilities, flaws, and weaknesses. The assessments scan for internal and external vulnerabilities. At the conclusion of each assessment, the OIG issues a report to grantee management that summarizes the results of the tests and provides corrective actions and best practices to address vulnerabilities. To provide insight regarding common security issues, on March 20, 2018, the LSC OIG issued the linked report to Executive Directors of LSC grantees summarizing vulnerabilities identified in recent tests and scans. The report outlined best practices to mitigate vulnerabilities. For additional information regarding the LSC OIG's IT vulnerability program, please contact Roxanne Caruso, LSC OIG Assistant Inspector General for Audit at (202) 295-1582 or by email RCaruso@oig.lsc.gov.

Lastly, some grantees have taken proactive steps by purchasing insurance that covers its organization in the event of a cyberattack and the LSC OIG would advise all grantees to discuss its options with its insurance carrier.

We hope you find this Fraud Alert useful. If you are the victim of a ransomware attack, the LSC OIG encourages you to contact your local FBI office. Local law enforcement authorities also may have a cyber fraud unit available to assist you.

The FBI has an Internet Crime Complaint Center (IC3) which accepts Internet crime complaints and provides public service announcements on emerging cyberattacks; please visit https://www.ic3.gov/default.aspx for more information.

The LSC OIG's fraud hotline telephone number is 800-678-8868 (toll free), our email address is hotline@oig.lsc.gov, and a link to our Hotline Submission Form.

If you have any questions concerning this Fraud Alert, please contact Dan O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at 202-295-1651, or dorourke@oig.lsc.gov.