New Treasury Department Ransomware Advisories Warn That Ransom Payment May Be Sanctionable

Prepared by:
Margaret Young Levi and Kathie M. McDonald-McClure
Wyatt Tarrant & Combs LLP

LORMAN®
Published on www.lorman.com - July 2021

LORMAN®

Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

www.lorman.com

New Treasury Department Ransomware Advisories Warn that Ransom Payment May be Sanctionable

Written by Margaret Young Levi and Kathie McDonald-McClure

Cyber-attacks using **ransomware** have been on the rise during the COVID-19 pandemic. Ransomware, whether it encrypts computer files or locks an entire hard drive, can block access to an organization's essential operating data, unless the organization can obtain a decryption key. In many if not most cases, a decryption key is only available by paying a ransom to the cybercriminal.

On October 1, 2020, the **U.S. Department of the Treasury Office of Terrorism and Financial Intelligence** announced the issuance of *two advisories* aimed at fighting ransomware scams and attacks. In making the announcement, Deputy Secretary Justin G. Muzinich said:

Cybercriminals have deployed ransomware attacks against our schools, hospitals, and businesses of all sizes. Treasury will continue to use its powerful tools to counter these malicious cyber actors and their facilitators.

The advisories also warned that those who facilitate ransomware payments may be sanctioned for violating Treasury law and regulations. However, Treasury's efforts to crack down on ransomware in this way places its victims in the crossfire. Ransomware victims may feel they have no choice but to pay the ransom if this is the only way to regain access to essential data, which is often the case when the most recent data back-up is also attacked, and a decryption key is not available by other means. Moreover, paying the ransom may be a matter of public safety. For example, ransomware that locks healthcare providers out of patient electronic medical records, attacks computers that support life-saving medical devices, or that shuts down computers connected to automobiles and other consumer devices, could pose a risk of injury or even death.

Treasury's **Financial Crimes Enforcement Network** (FinCEN) issued an advisory, entitled "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (Treasury Advisory). The Treasury Advisory is intended to educate financial institutions and others involved in cyber incident response measures about ransomware trends and indicators of ransomware as well as related money laundering activities. More specifically, the Treasury Advisory addresses the following areas of concern:

- *the role of financial intermediaries*, such as digital forensics and incident response (DFIR) companies, cyber insurance companies (CICs) and others, in facilitating ransomware payments to cybercriminals, often by directly receiving customers' funds and exchanging them for cryptocurrency (also known as virtual or digital money such as Bitcoin);
- *trends and types of ransomware and associated payment schemes*, such as "double extortion schemes" (which involve both stealing sensitive data and encrypting the system files) and cybercriminal partnerships to share techniques, code, and *ransomware exploit kits* equipped with ready-made malicious codes and tools;
- *financial red flags* that are associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes; and
- *the regulatory obligations of U.S. financial institutions* to file suspicious activity reports (SARs) and share information related to ransomware attacks.

Treasury's **Office of Foreign Assets Control (OFAC)** issued a related advisory, entitled "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (OFAC Advisory). The OFAC Advisory warned that making the ransom payments violates OFAC regulations, stating:

Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.

The OFAC regulations prohibit U.S. persons from engaging in financial transactions with malicious cyber actors designated by OFAC under its cyber-related sanctions program. This includes the cyber actors behind such ransomware and malware as *Cryptolocker*, *SamSam*, *WannaCry 2.0*, and *Dridex*. The OFAC Advisory describes the sanctions risks and provides information on reducing the risks through compliance programs, reporting the ransom attack, and fully cooperating with law enforcement agencies.

OFAC indicated that reporting the attack and cooperating with law enforcement could be a mitigating factor in assessing sanctions, stating:

OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.

What remains to be seen is how vigorously the Treasury Department will impose sanctions against a company that has been the victim of a ransomware attack and has no choice but to pay the ransom.

Determining Type of Ransomware. Knowing the type of ransomware is crucial to determining whether the cyber actors behind the attack are on OFAC's list of sanctioned persons, as well as knowing whether a "key" is available to unlock what the cybercriminal locked or encrypted. Forensic experts experienced with ransomware can often identify the type of ransomware (encrypting ransomware *versus* lock-screen ransomware) and even the variant within that type by reviewing the ransom note, the "vector" or method by which ransomware infected the computer and knowing whether the malware was able to move laterally across an organization's network to infect other computer hard-drives or files.

Ransomware Infection Vectors. There are multiple infection vectors used by cybercriminals to inject ransomware into a computer or organization's IT network. Security incident response firms report that *Remote Desktop Protocol (RDP)* is the top vector, being involved in over 50% of ransomware attacks. RDP is a tool often used by IT administrators to remotely access computers on the organization's network. Unsecured RDP ports and weak RDP credentials, however, allow cybercriminals to gain easy access.

Another common vector is *phishing email*. Many phishing emails are socially engineered to look like they are from a trusted source, such as an executive or manager of the organization. Assuming the email is legitimate, the recipient clicks on a malicious link or attachment that downloads the ransomware or, even worse, supplies his or her log-on credentials thereby allowing the cybercriminal to gain access to not only the recipient's computer but other computers on the network. Cybercriminals often send a phishing email just before lunchtime or near the end of the workday when employees tend to be more distracted trying to wrap up a task in order to get out on time. Clever timing of phishing emails and the multiple distractions inherent in computer-driven office work are major contributors to the lack of attention by employees to clues that an email is malicious. Flagging emails that are from outside the organization can help reduce this risk but are not failproof and should not take the place of training employees on how to identify malicious emails.

Coming in third among the top ransomware vectors are *software vulnerabilities*. These most often result from a failure to patch or update software programs, especially programs on the network that are no longer being used. The failure to change default passwords for a rarely used software program can also open the door to ransomware. Software programs that are no longer in use should be removed. Software vulnerabilities often present the most risk because, after cybercriminals gain access to the organization's network, they go undetected for months while they perform reconnaissance before deploying their ransomware attack. Other commonly used ransomware vectors include *exploit kits deployed on compromised websites*, *malicious online advertising (malvertising)* and *infected file downloads*.

Ransomware Decryption Keys. Law enforcement agencies and forensic experts may be able to provide keys to unlock certain types of ransomware encryption. There also are malware tools that can help identify some variants of ransomware and even provide a decryption tool if one is available. *Bitdefender*, for example, offers a *free ransomware tool* that can be downloaded to help identify many variants of ransomware. Several security tech firms have combined to create ***No More Ransom!***, which is a database of decryption tools that may be helpful once the variant of ransomware has been identified. However, because there are thousands of variants of ransomware with new variants continuously popping up, such free tools may not provide a solution — engaging a forensic expert experienced in ransomware incident response may be necessary.

The Wyatt Data Incident Response Team has prepared "Six Tips" on responding to a cybersecurity incident within the first 24-48 hours. For more information on *Wyatt's Data Privacy & Security Incident Response Team* see their Data Privacy & Incident Response Team brochure or visit the Data Incident Response Team.

The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.