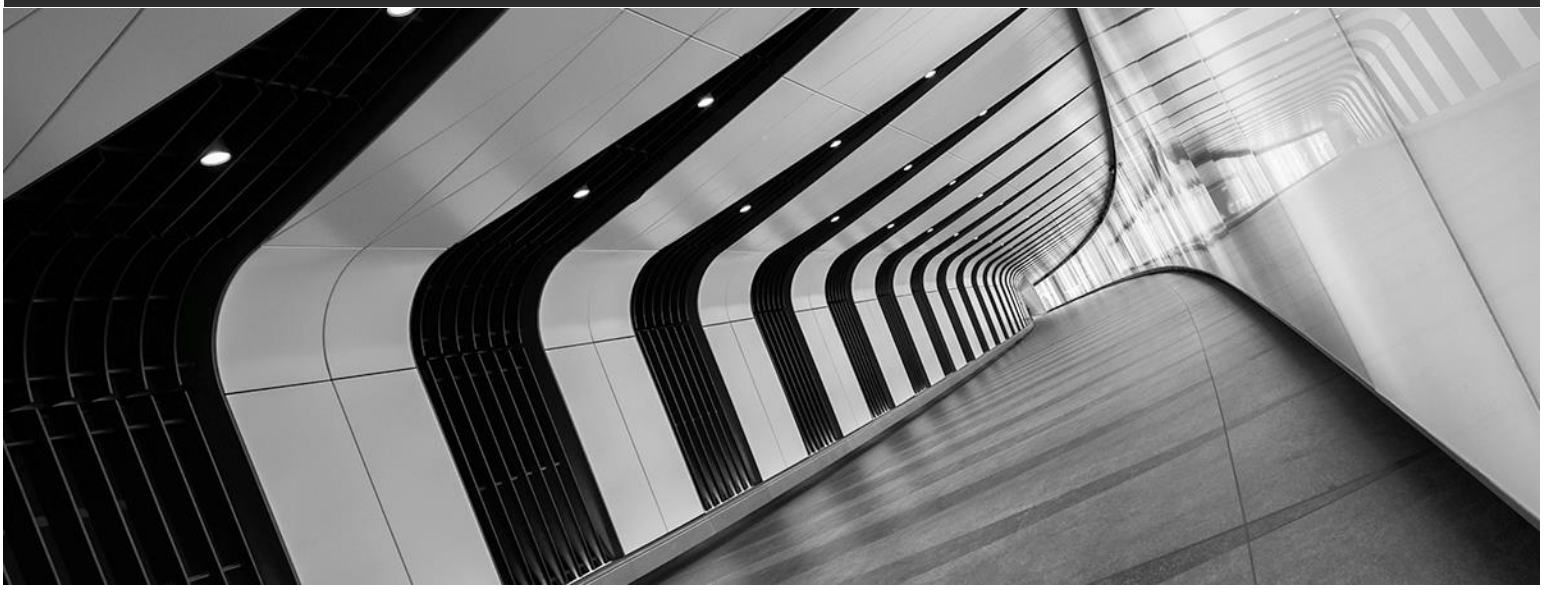
GT GreenbergTraurig

'Tis the Season for Ransomware



By Jena M Valdetero | December 21, 2020 | The Recorder

As if 2020 could not get any worse, this year has also ushered in a dramatic uptick in ransomware attacks. Threat actor groups are taking advantage of COVID-19 and the sudden massive increase in remote working. While companies were struggling to remain operational despite no longer working in a physical office, threat actors were exploiting remote access and the lack of multi-factor authentication to infiltrate their computer systems.

The size of the ransom demands and the sophistication of the attacks are also increasing. Two years ago, most demands were in the mid-five figures; now, we are routinely seeing six and seven figure demands. The higher demands are generally the result of targeted ransomware attacks against major companies that the attackers know can afford to make such large payments, but not always. Any company—big or small—can be a victim of a ransomware attack.

Threat actors are also spending more time inside a victim company's network searching for and encrypting back-up copies of files or servers, with the goal of preventing the company from restoring from back-ups and making it more likely they'll be left with no choice but to pay the ransom. Threat actors also sometimes delete logs, which are like breadcrumbs that would show where the threat actor went while she or he was inside your network, ensuring that companies will be unable to tell what data or files were accessed by the criminal actor.

Another concerning trend is for these criminal groups to exfiltrate company data and then post file names on so-called shaming sites designed to strong-arm companies into paying a ransom to have the files removed and (supposedly) deleted.

Amid all of this, the U.S. Department of Treasury published an advisory piece on Oct. 1, in which it reminded companies thinking of paying a ransom that they risk running afoul of U.S. sanctions laws. The Office of Foreign Assets Control (OFAC) publishes a list of known threat actor groups, including foreign governments, subject to U.S. sanctions. Paying or facilitating a ransom payment to one of these sanctioned entities may land a company in hot water because such payments may provide financial support for sanctioned actors' criminal activities.

This advisory is nothing new—the risk that paying an unknown threat actor may run afoul of U.S. sanctions laws has always existed. However, the practical reality of ransomware is such that, while there's little to no chance your attacker is spending the ransom payment making the world a better place (I always say there's no chance the money is funding a school for underprivileged girls in a developing country), you might not always know the identity of your attacker. Yet, OFAC may impose sanctions based on strict liability—meaning it can hold companies civilly liable even if they did not know they were engaging in a transaction with an organization on the sanctions list.

You might be saying "but surely law enforcement can step in and help companies staring down the barrel of a ransomware attack." Unfortunately, that is currently often not the case. It's not their fault. It's largely a numbers game. Law enforcement's resources are currently outpaced by the sheer number of threat actor groups and volume of attacks, not to mention the challenges posed by threat actor groups operating outside the U.S.'s jurisdictional reach.

So what's a company to do when left with two bad options: pay the threat actor or risk total loss of key data and the ability to operate? It's difficult to envision companies hit with ransomware uniformly deciding not to pay the threat actor based on Treasury's recent advisory, particularly when officers and directors have a fiduciary duty to shareholders to protect the business. Moreover, law enforcement has consistently avoided pursuing victim companies who, left with a Sophie's Choice, find themselves paying a threat actor's demands.

Treasury encourages victim companies to make a timely self-report to law enforcement concerning the ransomware attack, noting that such a report will be a "significant mitigating factor." You can do so via the FBI's online cybercrime portal, www.IC3.gov, though, some time may pass before you receive a response. In 2019 alone, IC3.gov received nearly half a million crime reports. If a victim company believes it may be negotiating with a threat actor subject to OFAC sanctions, it should contact Treasury immediately, but the advisory is silent as to what assistance Treasury may be able to provide.

While easy to say, the best solution is to take steps to prevent a ransomware attack in the first place. Most security breaches happen because either account log-in credentials were exposed or phished and multi-factor authentication was not enabled (for example, a token or a push notification required in addition to a password) or because there was open access to the network (usually via an open remote desktop protocol port). The Department of Homeland Security recommends keeping two back-ups of any important file or server and storing one offsite so it is inaccessible to a threat actor. While restoring from back-ups is not ideal, neither is paying a criminal.

About the Author:

Shareholder Jena M. Valdetero serves as co-chair of Greenberg Traurig, LLP's U.S. Data, Privacy and Cybersecurity Practice, where she advises clients on complex data privacy and security issues.

Jena M. Valdetero

valdeteroj@gtlaw.com