BRACEWELL

INSIGHTS

Diving Into Ransomware

October 20, 2021

*By: **Matthew G. Nielsen** and **Seth D. DuCharme***

In this episode of Bracewell Sidebar, we are joined by ***Seth DuCharme*** for a dive into unique risks and challenges presented by ransomware attacks.

Seth is a partner in Bracewell's government investigations and enforcement group in New York. Seth was recently the acting United States Attorney for the Eastern District of New York. He also had various leadership positions in the Department of Justice and the US Attorney's Office in Brooklyn, and he worked to establish the National Security and Cyber Crime Section at the Department of Justice.

What Is ransomware?
Ransomware is accessing a computer or a network of computers and through technical means holding data for ransom through encryption technology. Many of our listeners may be familiar on a personal level with encrypting a file for their privacy reasons. Maybe it's a PDF file or some other type of file, and they take the reasonable step of setting a password so they can get access to that file. Ransomware essentially encrypts many or even all files it finds on a computer or within a network and creates a private key. Then, whomever has perpetrated that ransomware on the computer or the network, makes that key ideally available for a price. And I say ideally because there are no guarantees that the hacker will provide the key upon the payment. But the ransomware is essentially locking you out of your house, changing the locks and then charging you to get a key back into your home – but on the level of a computer or a network of computers.

Is there something unique to how ransomware attacks happen?
There are several different ways that ransomware can end up on a computer or a computer network. Most of them come down to the failures of the kind of good cyber hygiene habits that folks have been sounding the alarm over for a decade. So, for example, if you've been to cyber security conferences, many of the one-hour presentations end with "and that's why you shouldn't click on links." It's well known by now that if you get an unfamiliar email encouraging you to click on a link, whether it's suggesting it's a cute picture of a kitten or some free vacation or whatever, they're trying to entice you and perhaps that's been engineered by looking at your social media to confirm that you like kittens and free trips to Hawaii. People can find the links irresistible, so clicking on the link is an invitation to another computer that's out there to do things to your computer.

Innocuously, it would show you a picture of a kitten or a Hawaiian resort, but with ransomware, it's essentially an invitation to infect your computer with malware. So that's one way. It's a

common way. It's almost embarrassing to repeat it because people have heard it so much, but it's a real thing, and people have a hard time resisting the impulse to click on something that they think will be immediately gratifying and rewarding, whether it's an image or an opportunity.

Another way is that, as creatures of habit with limited memories, many people are in the habit of using the same password for multiple accounts.

Who should you call when a cyber-attack happens?
Cyber security requires a team approach. You have to have internal experts that know how to communicate appropriately to their level of responsibility. You have to have sophisticated outside counsel and perhaps subject matter expert consultants that know how to help you deal with a particular threat. It's tough to find in one place all the solutions you need for the myriad complications and potential problems that can arise from a cyber-attack ransomware breach. It comes down to assembling that team on the front end and getting that team to communicate effectively.

When, where and how should you get the government involved in a cyber-attack?
Sometimes it's simply because the law requires notification under certain circumstances. But in many cases, it's not, and it will be a judgment call. If it's a significant event eventually people will find out. How do you want that conversation to start? Do you want the US government calling you and you reacting to that while you're dealing with a lot of other stuff? Or do you want to go to them on your terms with a concise summary of accurate information? Going to them could potentially be helpful to you and will almost undoubtedly be beneficial to the collective effort. The government operates in good faith on the notion that it does not want to leave victims worse off than it found them.

Have questions about ransomware or cybersecurity? Email your questions to ***Matthew Nielsen*** or ***Seth DuCharme***.

The opinions expressed in this podcast are those of the speakers and do not necessarily reflect the viewpoint of their institutions or clients.