The Rise of Disruptionware and High-Impact Ransomware Attacks

“Disruptionware is defined by the Institute for Critical Infrastructure Technology (ICIT) as a new and “emerging category of malware designed to suspend operations within a victim organization through the compromise of the availability, integrity and confidentiality of the systems, networks and data belonging to the target.” New forms of disruptionware can be a more crippling form of cyber-attack than other more “garden-variety” malware and ransomware attacks.” warns an article in ***JDSupra***.

“Generalized forms of ransomware attacks – designed to block access to the victim’s computer systems until money is paid – are continuing to represent a more prevalent threat to government agencies, healthcare providers and educational institutions … another publication has noted the rise of ransomware attacks since the beginning of 2019 finding that there have been at least 621 reported successful ransomware attacks against U.S.-based corporations. Of these attacks, at least 491 were targeted against healthcare providers, while another 68 of the attacks were directed at county and municipal institutions, and 62 of the attacks were focused on school districts.”

“The FBI’s PSA serves as a warning to businesses that they should have a plan in place to respond efficiently and appropriately in the event of high impact ransomware and disruptionware attacks.”

Read the article.