COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 6. June 05, 2019 Ransomware on Rise Again; CEs, BAs Need Strong Backup Plan

By Jane Anderson

Ransomware attacks may have slacked off in 2018, but health care entities should not get complacent and let down their guard, warns a former top FBI official.

"Ransomware goes in cycles. Lots of times it tracks with Bitcoin," since bad actors frequently ask to be paid off in Bitcoin, said John Boles, principal at PwC and former assistant director for international operations at the FBI. "If the first couple of months of 2019 are any indicator, ransomware is going to be back this year," Boles told attendees at a recent conference in Washington, D.C.

In fact, ransomware attacks are on the rise again following a lull in 2018: a report from Malwarebytes Labs found a 195% increase in business detections of ransomware attacks from the last three months of 2018 to the first quarter of 2019.

"Compared to the same time last year, business detections of ransomware have seen an uptick of more than 500%, due in large part to a massive attack by the Troldesh ransomware, also known as Shade, against U.S. organizations in the first part of the year, the Malwarebytes Labs report found.

Troldesh, which has been around since 2014, is typically spread by "malspam," or malicious email attachments, which are presented to the receiver in zip file format as something that needs to be opened quickly. The extracted zip file is a JavaScript that downloads the malicious payload, which is the ransomware itself, and is often hosted on sites with a compromised content management system, according to Malwarebytes Labs.

A significant amount of ransomware originates in a few nation states, such as North Korea and countries that were part of the former Soviet Union, Boles explained. For example, Ryuk ransomware, which disrupted major U.S. news publications toward the end of 2018, originally was suspected of being the product of a single group linked to North Korea, but now is thought to come from Russia or former satellite states.