TROUTMAN SANDERS LLP

WANNACRY RANSOMWARE FACT SHEET

Understanding the Cyber Attack that Rocked the World

On Friday, May 12, 2017, WannaCry, a ransomware virus that targets Microsoft Windows operating systems, also known as Wanna Decryptor and WannaCrypt, was launched infecting more that 300,000 computers in at least 150 countries demanding that users pay bitcoin ransoms in 28 languages. Hospitals who fell victim to the attack experienced system-wide lockouts, delays to patient care and function loss in connected devices such as MRI scanners and blood storage refrigerators. Though ransomware attacks on hospitals and healthcare providers have been on the rise, the scale and reach of this attack is unprecedented.

What is ransomware?

Ransomware is malicious computer code (malware) that takes control of a targeted computer and locks out the user until the attacker sends a command to unlock the computer, usually after a ransom payment is made through bitcoin. Malware will expand through a computer network and extend to other networks that are connected to the infected network. The result is that the network is locked and users are denied any access to the network.

Doesn't my network security system protect me from a ransomware attack?

No. Cyber attackers use phishing attacks to defeat common security features. A phishing attack uses an e-mail, often impersonating a company executive, to prompt employees to open an attachment that contains malware. Once the attachment is open, the malware is launched and rapidly spreads through a network. The WannaCry malware has reportedly exploited a known weakness in Microsoft's operating system. Microsoft issued a patch, but the National Health Service and many other affected computer networks had not installed the patch.

Is the threat from WannaCry over?

We hope so, but that is not clear. Though initially, a "kill switch" that could halt the malware was identified, there are reports of variations of WannaCry that are resistant to the switch. Microsoft has offered an updated patch to even older, unsupported operating systems, but the patch will not be able to protect systems that have already been targeted. Cybersecurity forensic experts are concerned that the malware can still attack computer networks in the days and weeks ahead.

Was the National Health Service specifically targeted?

It does not appear that the NHS was *specifically* targeted by the cyber criminals. Rather, the incident seems to have been a non-specific, blanket attack which explains why so many different types of companies were affected globally. This is very concerning since it means that US healthcare organizations could be hit at any time by the malware.

Is a ransomware attack a reportable breach under HIPAA?

OCR recently issued guidance on ransomware for HIPAA covered entities. The OCR guidance states that every ransomware attack should be presumed to result in a reportable breach unless the victim can prove that the attackers did not access any PHI. Whatever evidence the organization relies upon to conclude that a breach did not occur must be retained by the organization in the event that OCR wants to examine the evidence at a future date.

> *"...U.S. healthcare organizations could be hit at any time by the malware."*

What should my organization be doing about the threat of a ransomware attack?

1. Update your Incident Response Plans: Every healthcare organization should be preparing for the inevitability of a cyber attack, including but not limited to ransomware, just as organizations prepare for the wide variety of threats today. Last year Medicare amended its Conditions of Participation to require that every participating provider engage in "all-hazards" emergency preparedness and response activities. While this had been mandated by federal grants for years, all-hazards emergency preparedness is now a mandatory requirement to participate in Medicare and other federal healthcare programs. Cyber attacks are a recognizable and definitive hazard today.

2. Test your plans: Healthcare organizations should conduct ransomware specific exercises that include IT, clinical staff, incident response personnel and C-Suite executives. Tests should address the responsibilities and viewpoints of all those who could be impacted during a ransomware event.

3. Prepare for litigation: Class Action lawsuits are common when data breaches occur or if a breach is suspected. Every cybersecurity incident should be treated as a potential lawsuit. Involve knowledgeable legal counsel as early as possible during a cybersecurity event.

Steve Gravely focuses his practice in the areas of health law, information privacy and cybersecurity and emergency preparedness and response issues for critical infrastructure industries. He has represented healthcare organizations for over 20 years in a full spectrum of healthcare legal issues.

TROUTMAN SANDERS