BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Tackling healthcare Cyber threat: Expert Opinion

December 2, 2020 | Analysis

An analysis by David Sajoto, Vice President, Asia Pacific and Japan, ExtraHop



The healthcare sector is highly vulnerable across the globe. Amidst one of the worst healthcare crises to have hit mankind, attackers are exploiting conditions like increases in telemedicine, teleworking and an overworked and distracted medical workforce. The increase in cybersecurity attacks in the healthcare industry has the potential for dire patient care consequences by interrupting the flow of hospital operating procedures and denying critical access to patient records. In Singapore, there has been a rise in cybersecurity attacks in the healthcare industry. In particular, since the start of the pandemic, Singapore has seen an increase in misinformation targeting the Ministry of Health's social media pages.

On October 28, 2020, a joint cybersecurity advisory warning of an imminent cybercrime threat to hospitals was issued, co-authored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). The advisory warned that cyber actors were targeting the healthcare sector using TrickBot and BazarLoader malware, resulting in ransomware attacks, data theft, and disruption of services.

There are many factors at play. We suspect that the recent Zerologon vulnerability has contributed to this series of attacks, and any hospital that has not patched their systems is at risk. Time is of the essence—earlier this month it was reported in Threatpost that Ryuk threat actors were taking advantage of Zerologon (CVE-2020-1472) to encrypt a victim's network just five hours after sending a phishing email.

Unfortunately, sophisticated bad actors will find a way to pass by perimeter defenses and, once inside, move laterally through the network and attempt to escalate privileges. It is during this gap, after the malware infection and before the attacker escalates privileges, that security teams have a high potential to stop the ransomware from executing.

Organizations need to play their part in protecting themselves against potential cybersecurity attacks first through the endpoint (EDR) If an attack bypasses the perimeter defenses and makes it onto the network, it is critical to be monitoring network traffic inside using network detection and response (NDR). Observed network data is considered the ground source of truth for what is happening across the distributed, hybrid network. It cannot be tampered with or evaded and provides the highest potential to uncover an attack in progress. By understanding normal traffic behaviours, security teams can identify anomalous activity that indicates an attack on the inside. It is also essential to have the capability of detecting known indicators of compromise to stop ransomware before it encrypts classified data.

NDR leverages machine learning to detect unusual behaviour taking place on your networks such as identifying lateral movement, privilege escalation, and anomalous modification of file shares. Security teams need the context of an incident, what happened before and after the alert, to immediately investigate and respond to prevent ransomware from infecting their environments.

ExtraHop finds the ransomware attacks against hospitals, as reported by CISA, during this time of crisis unconscionable. The recent Zerologon vulnerability is a factor and any hospital that has not patched their systems is at risk. Unfortunately, sophisticated and motivated bad actors may easily get through the first layer of perimeter defences, and once inside the network will move laterally through the network and attempt to escalate their privileges. Organizations must be monitoring both north-south and east-west traffic to detect unusual behavior that is missed by other tools, look for known filenames like RYUK or .ryk that indicate an attack, and quickly investigate and respond to stop the breach.

Technological innovation in healthcare promises to improve the quality and speed with which patient care is delivered. However, healthcare information security is often lagging. By improving cybersecurity measures to stop attacks before they affect a healthcare organization, the results include improved patient care and better healthcare outcomes.