In light of evolving threats - like the recent WannaCry ransomware outbreak - the data security industry is seeing a shift in approach from traditional signature-based tools to more behavioral analytics. This is a particularly important trend for the healthcare industry to follow given the targeted attacks many systems across the country, and throughout the world, have experienced in recent years.

Security Threats That Make You WannaCry

On Friday, March 12 the world experienced a well-coordinated ransomware attack, known as WannaCry,[1] that infected systems on a larger scale than has ever been seen before. Ransomware,[2] and more specifically crypto ransomware, is a virus designed to search for a certain predefined set of file extensions that are typically used with protected data on a network. It encrypts, or locks it, requiring the owner to pay a ransom for a decryption key. This seems to be the preferred tool for attacking healthcare institutions; with lives on the line organizations are forced to pay the ransom quickly to gain access to patient information critical to providing proper care.

rmp
Receive More.

More than 150 countries and 200,000 systems were infected by the WannaCry attack across businesses, universities, and yes, health systems. The U.K.'s National Health Service (NHS) was the first identified victim, and was the day's most severe hack. A total of 48 NHS organizations were hit, rendering patient records unavailable and forcing it to suspend operations.

Outsmarting Tradition

As viruses become "smarter," - capable of seeking out the most sensitive information on a network to encrypt - our data security efforts must exceed their pace.

Traditional antivirus protection is signature-based. Like a vaccine it uses the signatures of previously identified viruses to detect new incoming threats. The software is updated for each new virus or malware signature detected, but it cannot keep pace with rapidly mutating ransomware strains. Ransomware signatures multiply quickly as hackers put their own spin on existing strains, and by the time your traditional antivirus protection is updated for the most recent one, a new mutation could already be hitting your inbox.

Next Gen Antivirus

The future of data security is in behavioral analytics-based protection. Just as viruses are learning to identify sensitive information, behavioral-based tools are learning how to identify ever-mutating virus signatures. These tools are more like a broad spectrum antibiotic; they look for the behavioral cues of a virus rather than a specific signature. Many even have the ability to sever a connection before any damage can be done. Essentially, rather than searching for the signature of a virus that encrypted something yesterday or last week, it searches for a signature that looks like it might be able to encrypt something.

These tools not only address unpredictable new threats, but also solve the limited resource problem faced by my organizations. Most of the ARM industry, and certainly most of the healthcare industry, does not have the manpower to dedicate a team to keep up with the new threats that are created every day. Using this next gen antivirus protection, organizations have the ability to leverage the security experts who designed and maintain the software for them.

Placing your trust, and your data, in the hands of security experts can help your organization avoid attack, even on the scale of WannaCry. For example, by leveraging the experts at Sophos CryptoGuard, we protected our healthcare clients across the country from an attack that could have suspended operations, and cost thousands of dollars to resolve.

Defense In-Depth

Behavioral analytics protection is one of what should be multiple layers of defense surrounding your patient's PHI and financial information. More healthcare organizations should be shifting to a defense in-depth strategy, one in which layers and layers of security systems are put in place so that you are able to protect not only against incoming threats, but also against those that may already be in your system. SIEM, or Security Information and Event Management tools, funnel all security information and events into one place, providing alerts and fast response to any potential threats. RMP's InsightIDR tool monitors our 20 million daily events and can warn our data security team of any suspicious activity, and monitor everyone already within the system to ensure all activity is sanctioned.

Play Offense, Not Defense

Protecting your system from known risks is a good way to get hacked. What we thought was ransomware yesterday is different today; we understand that more than ever after the WannaCry attack. Big organizations and healthcare systems are particularly vulnerable because of outdated technology. Protect your patients by playing offense and going above and beyond traditional protections, because you never know what new cyber-threats tomorrow brings.

Written by Greg Haar, Data Security Officer, Chris Shelly, Cyber Security Specialist, and Ali Bechtel, Digital Marketing Manager for RMP

rmp
Receive More.

Sources:

[1]"Global Cyberattack Reaches 'Unprecedented' Scale", Aria Bendix, The Atlantic, May 13, 2017, www.theatlantic.com/news/archive/2017/05/global-cyberattack-reaches-unprecedented-scale/526647/

[2]"Beware Ransomware: The Latest Threat to your Data Security," Eric Cicale, Marketing Multimedia Developer, Receivables Management Partners, July 21, 2016, hub.arlogix.com/blog/beware-ransomware-the-latest-threat-to-your-data-security

1809 N. Broadway, Greensburg, IN 47240
855-831-3426 | ReceiveMoreRMP.com

Want to get RMP Insights delivered right to your inbox?
Subscribe at www.ReceiveMoreRMP.com/Subscribe-to-Insights

This information is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure this information is up-to-date as of the date of publication. It is not intended to be a full and exhaustive explanation of the law in any area, nor should it be used to replace the advice of your own legal counsel.