BioSpectrum the business of Bio & Health Sciences ASIA EDITION

The State of Healthcare Cybersecurity: VMware Carbon Black Explores the Surge in Cyber Threats

20 April 2021 | Opinion

A Look Back at 2020 Healthcare in Crisis: By Samantha Mayowa

On the frontline of the pandemic, perhaps no industry was impacted and forced to innovate and transform as quickly as healthcare in 2020. Whether it was the rapid development of COVID-19 testing technology or the explosion of telehealth, healthcare organizations accelerated digital transformation in record time. But with these innovations came new and unprecedented security vulnerabilities that cybercriminals quickly looked to exploit and profit from.

Healthcare in Crisis: A Look Back at 2020

To help understand the state of healthcare cybersecurity, we took a look back at 2020 and found that there were 239.4 million attempted cyberattacks targeting VMware Carbon Black healthcare customers. We also found an average of 816 attempted attacks per endpoint in 2020, a staggering 9,851% increase from 2019. The surge in attacks began as early as February just as the pandemic started to spread worldwide. From January to February, the number of attempted attacks shot up by 51% as cybercriminals set their sights on vulnerable healthcare organizations that were navigating tremendous changes in the way they operate and treat patients.

In the latter half of the year, we saw the attempted attacks per endpoint peak with an 87% increase from September to October. The timing of this significant spike corresponds with the October alert from the Cybersecurity and Infrastructure Security Agency (CISA), which warned of increased cyberattacks by a Ryuk ransomware gang specifically targeting healthcare organizations.

“Amid the pandemic, cybercriminals now have limitless attack methods,” said Rick McElroy, Principal Cybersecurity Strategist at VMware Carbon Black. “Whether it’s using tried and true malware like EMOTET or using BitLocker to ransom systems, malicious actors continue to gain ground. The FBI, Department of Homeland Security (DHS), and other federal agencies have all issued warnings about the surge in cyberattacks against healthcare organizations.”

We are now also seeing “secondary infections,” which are leveraged to facilitate long-term cyberattack campaigns, happening across the digital healthcare supply chain and have led to a surge of extortions and helped fuel a cybercrime market. Our research found protected health information (PHI) being bought and sold on dark web markets as cybercriminals look for the easiest way to cash in on data.

A Ransomware Pandemic

In 2020, we saw ransomware go mainstream. The wide-reaching impact of ransomware has been assisted largely by way of affiliate programs. With many ransomware groups offering ransomware-as-a-service (RaaS), making the deployment of ransomware easily accessible to millions of cybercriminals who previously didn't have the tools to carry out these attacks. Compounding these risks is the adage of affiliate programs for ransomware groups, providing new and unique ways for malware operators to have others deploy their payloads for a cut of the eventual profits.

"As RaaS explodes in popularity on the crimeware forums, cybercriminals are finding new and unique ways to deploy ransomware across organizations," said Greg Foss, senior cybersecurity strategist at VMware Carbon Black. "Similar to how spies are recruited for espionage against government agencies, regular everyday people with access to high-value targets can be recruited to deploy malware. Often, they are lured through offers of significant sums of money or even a percentage of the ransomware payout, with some offering hundreds of thousands of dollars per victimized organization. Affiliate programs and partnerships between ransomware groups have also become a common occurrence alongside the general recruiting of insiders. These affiliate programs look to partner with initial access brokers – criminals that specialize in breaking into organizations and subsequently sell direct access and other ransomware gangs in order to improve their tradecraft, furthering their reach and overall profitability.

Throughout 2020, we have seen expansions in the use of ransomware with some threat actors repurposing ransomware for use as pure wipers, wherein the decryption keys will be able to recover the lost data, and more recently in Denial-of-Service (DoS) attacks, impacting core services that citizens rely on every day. There is no sign of these groups slowing down. In fact, we are witnessing the exact opposite, with groups beginning to collaborate at an unprecedented scale, share stolen resources, and even combine forces.

"COVID-19 test results are a hot commodity on the dark web right now, mostly in the form of large data dumps," said Greg Foss. "An interesting component around today's ransomware attacks is that underqualified, lesser-known cybercriminal groups are behind them thanks to the rise in RaaS. All it takes is a quick search on the dark web for someone to license out a ransomware payload to infect targets. Today, it's unfortunately just as easy to sign up for a grocery delivery service as it is to subscribe to ransomware."

The Rise in Secondary Extortion

Ransomware groups have widely adopted double extortion as a core tactic to ensure profitability. By taking time to quietly exfiltrate sensitive information from the organization, cybercriminals gain incrementally significant leverage on their victim organizations, forcing organizations to not only pay to decrypt their content but also prevent potentially harmful data from being sold or otherwise publicly disclosed. Thus, significantly increasing the impact and damage that ransomware groups can inflict upon their victims and sending a stark warning to others to protect their networks from this ever-evolving threat.

How to Fight Back: Three Security Recommendations for Healthcare CISOs

For healthcare organizations, understanding the evolving threat landscape is half the battle. Now that CISOs have a grasp of what they're up against, there are key defenses that should be in place. Here are three best practices to help CISOs stay one step ahead of attackers:

1. **Next-generation Antivirus (AV):**CISOs can start by ensuring their endpoint protection solution incorporates defenses for each phase of ransomware attacks: the delivery, propagation, and encryption stages. Today, traditional AV focuses mostly on the delivery stage, but this leaves a security gap with new malware. To detect and stop these attacks from propagating, solutions should also track endpoint activity to root out common behaviors such as privilege escalation and lateral movement, and finally prevent encryption by employing decoys and protecting local files and critical boot sequences. VMware Carbon Black Cloud™ Endpoint Standard offers protection through each of the common ransomware stages and breakthrough prevention for today's advanced cyberattacks.

1. **Endpoint Protection:** CISOs need an endpoint protection solution that easily scales and deploys to new users. The inability to rapidly provision new remote endpoints is another vulnerability and break in security postures. Healthcare organizations need the ability to easily provision access to new users while maintaining data privacy, compliance, and security practices. Siloed and on-premise security products increase complexity and delay progress in standing up and securing remote workers. VMware Carbon Black Cloud Endpoint helps organizations transform security with cloud-native endpoint protection that eliminates many of the time and resource-consuming barriers that often slow down deployments. The solution also offers security teams the full visibility and control required to help prevent, detect, and

respond to endpoint threats.

1. **IT Tracking Tools:** For CISOs to understand any area of vulnerability it's important to employ a solution that enables organizations to assess and harden system state. It's much easier to patch and prevent attacks than it is to remediate them. When it comes to helping prevent ransomware attacks, solutions that offer automated reporting to track configuration drift will help ensure environments stay as secure as possible. The VMware Carbon Black Cloud Audit and Remediation solution allows security teams to easily track drift and comes ready with built-in response tools to apply updates or run scripts for full remediation in minutes.

Securing Healthcare Organizations in 2021 and Beyond

The pandemic has brought about not only operational and patient challenges but also new cybersecurity threats and vulnerabilities for healthcare organizations. For CISOs and security leaders, it's time to ensure the proper security controls are in place as new technology is implemented to support remote work, patient care and more.

Healthcare organizations will continue to be extorted by cybercriminals looking for a payday or to monetize medical and patient data. As we move forward, it's critical to pay close attention not only to how these criminals achieve their goals, but also how we respond to these threats. We must continue to leverage organizations like the H-ISAC to bring the industry together and enable real-time collaboration and threat intelligence sharing. Our 2020 findings should serve as a starting point for a discussion between the cybersecurity community and the defenders of the healthcare sector on how to best collaborate and ensure patient care is not disrupted by cyberattacks.

***About the Author**: Samantha Mayowa is Head of Global Communications at VMware Carbon Black, responsible for driving and executing global communications strategies.*