RISKIQ I3 INTELLIGENCE BRIEF:

Ransomware in Health Sector 2020:

A Perfect Storm of New Targets and Methods

April 9, 2020

Team RiskIQ

Summary:

This digital revolution happened quickly, but with the outbreak of COVID-19, it has suddenly gone into hyperdrive. Almost overnight, workforces and business operations decentralized and were flung around the world, widening the protection gaps and decreasing visibility into their attack surfaces. Cybercriminals are capitalizing on coronavirus concerns, which has led to a spike in malicious online activity that we assess will increasingly impact healthcare facilities and COVID-19 responders.

BleepingComptuer found that on March 24, cybercriminals targeted hospitals with Ryuk ransomware. Likewise, Forbes reported on March 23 that Hammersmith Medicines Research, a British medical facility on standby to test COVID-19 vaccines, was attacked by a ransomware group called Maze. Fortune also reported a rise in ransomware attacks against medical facilities.

The Maze attackers managed to exfiltrate data—in this case, patient records—and published some of it on the dark web. Additionally, due to the threat of contamination, much of the hospital support staff is working remotely, according to research by the Wall Street Journal. Remote staffs make it harder for IT teams to police computer systems and prevent cyberattacks.

In the past few weeks, security protocols have completely changed—firewalls, DLP, and network monitoring are no longer valid. Attackers now have far more access points to probe or exploit, with little-to-no security oversight. Meanwhile, IT is feverishly standing up new systems, new access, and new channels and, in many cases succumbing to human error, such as critical misconfigurations.

To hone in on their victims, attackers look for entry points such as unknown, unprotected, misconfigured, and unmonitored digital assets. Microsoft, for example, has seen one operation known as REvil, which targets vulnerabilities in VPN devices and gateway appliances to breach networks, and many other groups are operating the same way.

In addition to having more targets, cybercriminals have, over the past few years, increased their capabilities. The first known healthcare-focused ransomware attack targeted AIDS researchers in 1989, aptly called the "AIDS virus." This virus came on a floppy disk and scrambled the contents of its victims' computers by encrypting filenames. The perpetrators offered to unlock the files once a "licensing fee" had been transferred to an offshore bank account. Today, ransomware is produced by hackers who have had years of virus development. These hackers can take advantage of industry-standard cryptography to attack their targets.

Against the backdrop of this ransomware "perfect storm," RiskIQ studied 127 of these attacks between 2016 and 2019. What follows are insights into what is yet to come as well as strategies healthcare providers can use to protect their patients' data now.

Small Hospitals and Health Care Centers are Most Often Targeted

Based on the ransomware attacks we studied, we found assaults on healthcare facilities are up 35% between 2016 and 2019. Cybercriminals tend to go after direct patient care facilities such as hospitals or health care centers (51%), medical practices (24%), and health and wellness centers (17%). We assess cyber-attackers prefer these facilities because they are more likely to pay to prevent disruption to patient care. Small facilities are also singled out, likely due to their lean security support—70% of the attacks we reviewed were directed at facilities with fewer than 500 employees. This trend is particularly concerning since 85% of small- or medium-sized hospitals lack a single qualified IT security person on staff, according to a Fierce Healthcare report. We also found that facilities in virtually every state have been targeted, with slightly higher rates occurring in California (13%), Indiana (5%), Texas (4%), and New York (4%).

While most facilities we examined did not disclose paying a ransom, 16% did. Unfortunately, paying the ransom does not guarantee the recovery keys will be provided or, if they are, that they will work. In fact, in 2019, the FBI issued an alert urging private and public organizations not to pay ransoms, noting some victims were never provided the decryption key after paying. In one of the cases we studied, the Kansas Heart Hospital was not able to regain access to their network after paying a $47,000 ransom. Instead, the hackers demanded another payment.

The FBI further warned that not all files are recoverable due to flaws in the encryption algorithms. Last month, the Wall Street Journal found that recovery keys are only effective less than 50% of the time.

What Does the Attack Look Like?

There have been 237 strains of ransomware observed since 2015, according to the New Jersey Cybersecurity and Communications Integration Cell. These variants fall into one of several subcategories: encryption ransomware, lock screen ransomware, master boot record ransomware, ransomware encrypting web servers, and mobile-device ransomware. The mechanisms behind each of these subcategories result in different behavior.

Variants of Ransomware

Encryption ransomware:	Encrypts a computer's personal files and folders then deletes them. A user may only become aware of the infection when they attempt to open a file, at which point they will be presented with a screen demanding a payment in exchange for release of encrypted files.
Lock screen ransomware:	Locks the screen of a computer demanding payment. This ransomware does not encrypt files.
Master boot record ransomware:	Alters the Master Boot Record (MBR) so that the normal computer boot process is interrupted. A ransomware notice is instead displayed on the screen during the boot up process.
Ransomware encrypting web servers:	Files on web servers are encrypted. This type of ransomware often uses vulnerabilities in Content Management Systems as an attack vector.
Mobile device ransomware:	Ransomware specifically targeting mobile devices with Android devices being a frequent target. This ransomware often uses drive-by-downloads or fake apps imitating legitimate services as an attack vector.

The ransomware attacks carried out since 2016 have utilized a variety of techniques to penetrate networks and propagate the malware. One ransomware strain, WannaCry, uses a vulnerability in the Windows Server Message Block (SMB) protocol. This vulnerability allows the malware to move laterally throughout a network and expand its pool of impacted systems quickly. Attackers can identify SMB on a network by scanning for devices listening on ports 139 and 445. Although WannaCry itself has fallen out of use, the abuse of SMB vulnerabilities remains. According to IBM X-Force Threat Intelligence Index 2020, 80% of ransomware attempts utilized exploits in the SMB protocol.

In addition to SMB vulnerabilities, ransomware can use Remote Desktop Protocol (RDP) attacks, phishing emails that either attempt to trick the user into opening a malicious attachment or lure the user to a website with malicious downloads or exploit kits, and even exploiting users' trust in removable media devices. "Phishing emails can be particularly dangerous, as networks with strong security protocols could be compromised due to human error," said Aaron Inness, a Senior Threat Intelligence Analyst for RiskIQ's i3 team. One study found that 27.75% of users in the healthcare and pharmaceutical industries fell for phishing lures before taking phishing awareness training.

RDP attacks take advantage of security flaws in the implementation of RDP-enabled machines. By default, RDP runs over Port 3389, so attackers will scan the internet to identify publicly-facing devices listening on that port. Once an RDP-enabled machine is identified, an attacker may then begin to brute force the RDP logins by using open-source password cracking tools. In some cases, attackers take advantage of the BlueKeep vulnerability—a wormable remote code execution vulnerability—to conduct ransomware attacks at a high volume across the internet.

Clicking on links in malicious emails can also open up a user and, by extension, a network to the threat of ransomware attacks. A user may follow a link to a compromised page that contains an exploit kit (EK). EKs are web-based attacks that take advantage of vulnerabilities in browsers or browser integrations, such as Adobe Flash Player or the Java Runtime Environment. The EK will then deploy a payload containing malware, with ransomware being the most common payload. An example of this is the Neutrino EK used to deploy Locky ransomware.

The Attacks are Vicious and Can Have Dire Consequences

The average ransom demand is $59,000, according to the cases we looked at, but that is often just the beginning of the costs associated with an attack. A Healthcare Dive study found that the downtime from a ransomware attack can last months and end up costing much more than the ransom payment. One of the facilities we looked at, Brookside ENT and Hearing Center, was forced to close down after attackers wiped all the office files, including appointment schedules and payment and patient information, when the owners refused to pay the $6,500 ransom.

In addition to the financial costs, there are also tragic human life costs to consider. Hospitals that have been hit by a data breach or ransomware attack can expect to see as many as 36 additional deaths per 10,000 heart attacks per year, according to a recently published study by researchers at Vanderbilt University's Owen Graduate School of Management.

"Even if a facility is able to recover from a ransomware attack, that doesn't mean that it is safe from future attacks. In some cases, it's the contrary. Being hit once means you are more likely to be attacked again." said Mr. Inness. Kentucky-based Park DuValle Community Health Center, for example, fell victim to two ransomware attacks within three months—the first locking down its systems for three weeks and the second restricting operations for about two months. Combined, these attacks cost the medical center over $1 million in security improvements, ransom payments, and lost revenue.

Likewise, following an attack, some health facilities have been hit with class-action lawsuits citing a failure to monitor their attack surface, including their network and systems that store sensitive data. One lawsuit filed last month against Hackensack Meridian Health in New Jersey alleges that if the facility had adequately monitored the network, the intrusion would have been detected earlier. Hackensack paid an undisclosed ransom and was forced to shut down their system for multiple days while it recovered its data.

Backing Up Your Data May Not Be Enough

Cybercriminals behind ransomware have also begun targeting the backup processes and tools. According to a Dark Reading report, several ransomware programs delete the shadow volume copies created by Microsoft's Windows operating system. Shadow copies are a method that Microsoft Windows provides for easy restoration. According to a KnowBe4 blog, attackers have also been known to infect machines and then lie dormant to allow backups to be created that include the ransomware. Once the ransomware is activated, facilities are still unable to access their data since even the backups contain the ransomware. In either case, backups become mostly useless.

It's important to note, however, that not all ransomware attacks compromise the victim's backups. Consequently, the first step in defending against ransomware is to ensure you're backing up your data on your system. The following includes additional technical and administrative tips to help mitigate this threat.

- After backing up your data, the next step is to store data offline or on a different network to defeat those cybercriminals who do target backup systems.
- Given the sensitivity of healthcare data, it should be encrypted so that even if a cybercriminal acquired it, they would not be able to read it.
- Have an incident response plan ready to help mitigate the impact of certain destructive malware attacks.
- Security personnel should track the company's digital assets that are connected to the organization outside the firewall because attackers search for unknown, unprotected, and unmonitored digital assets. This is particularly important now as healthcare facilities' digital attack surface expands and becomes more complex with some staff working from home. Contact support@riskiq to get a free Digital Footprint Snapshot report.
- Similar to above, health care facilities need to be aware of vulnerabilities on devices outside their firewall. For example, Microsoft recently found that ransomware attackers were targeting VPN devices (Pulse) as well as the Citrix ADC (netscaler) CVE-2019-1978. These are exactly the type of vulnerable assets RiskIQ can identify.
- To harden their networks and connected equipment, healthcare facilities with devices running open services should place them behind a firewall. They should also whitelist via the firewall any external IPs which require access. Placing these devices within a VPN adds another layer of protection.
- The importance of patch management can not be overstated when developing strategies to reduce risk of ransomware and other malware infection.
- Organizations can improve individual readiness for phishing attempts by taking part in phishing training. According to Security Magazine, on average, organizations across all industries dropped from an average of 27% of users falling for phishing attempts to 13% of users 90 days after phishing awareness training.

- Be aware of current ransomware threats. For example, BleepingComputer recently found a new ransomware aptly called CoronaVirus. According to the report, the ransomware has been distributed through a fake website pretending to promote WiseCleaner, a system tune-up software package. The downloads on the site distribute a file that acts as a downloader for both the CoronaVirus Ransomware and a password-stealing Trojan.

- Similar to the above, be alert to attack trends. For example, most ransomware attacks take place during the night or over the weekend, according to a recent FireEye report. This is most likely because many companies don't have IT staff working those shifts.

- See RiskIQ's recently published article Ransomware Attacks the Next Consequence of the Coronavirus Outbreak, for more information about how to mitigate these types of cyberattacks.

RiskIQ's Solutions for Ransomware, Cyber Threats

RiskIQ Executive Guardian®: RiskIQ uses internet-scale visibility to provide insight into emerging cyber threats. RiskIQ's team of cybersecurity experts and former intelligence officers minimize the likelihood of private data falling into the wrong hands and maintain visibility into security risks resulting from data exposure to better protect executives, key employees, and brand reputation.

RiskIQ Digital Footprint®: catalogs known and likely assets belonging to an organization by comprehensively searching the open web. With RiskIQ's unique access to internet data at scale, and with ten years of internet data history, we can create a comprehensive picture of which assets are exposed to the open web. Digital Footprint can help your organization combat ransomware attempts by searching for publicly-facing open ports, which in the case of ransomware attack vectors, could help identify exposures of RDP and SMB services.

RiskIQ PassiveTotal®: empowers analysts to identify potentially malicious infrastructure used by threat actors. PassiveTotal's proprietary, open-source, and third-party data sets create a powerful tool for tracking potentially harmful infrastructure. PassiveTotal can help organizations understand threat infrastructure and identify indicators of compromise through crowd-sourced research into threat actors and malicious campaigns.

RiskIQ is currently providing lists of newly observed infrastructure matching coronavirus themes. Apply code COVID19 in PassiveTotal for 30-days of access. Click here to explore other RiskIQ products designed to help you mitigate these and other cyber threats.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com