HOW RANSOMWARE AUTHORS HIT HEALTHCARE SECTOR

By David Balaban, computer security researcher

COVID-19 is not easing its global grip, and medical organizations are the driving force of humanity's efforts to turn the tide in the war against the notorious disease. Because hospitals and research labs are deluged with work that saves people's lives, they are more susceptible to malware raids than ever before. Cybercrooks are not showing due compassion, though. Some of them continue to zero in on the healthcare sector as if the pandemic were not the new reality.

A rise in phishing campaigns hinging on the coronavirus panic is one of the most disgusting cybercrime trends of 2020. Rogue emails are mimicking trusted medical entities, such as the World Health Organization (WHO) and the U.S. Centers for Disease Control and Prevention (CDC), and luring users into handing over their account passwords and downloading banking Trojans. Whereas these hoaxes are not focused on the health industry alone, ransomware rears its ugly head by affecting hospitals' computer networks in targeted attacks.

AN ESCALATING THREAT

The International Criminal Police Organization (Interpol) alerts hospitals to an increase in attempted ransomware onslaughts against them. The officials place a heavy emphasis on the fact that the aftermath of such an attack is not isolated to data impact. It complicates swift medical response and may therefore have serious real-world implications, putting numerous patients at risk.

In light of the growing ransomware activity affecting this sector, Interpol issued a Purple Notice to law enforcement agencies in all the 194 member countries. This way, the organization seeks to boost awareness about the issue across the board and asks the public to provide assistance via reports about criminals' tactics, techniques, and procedures (TTP).

Interpol additionally reassures member states that it will do its best to provide the necessary technical support and threat mitigation services. Its Cyber Threat Response (CTR) subdivision is also collecting information on rogue web domains constituting ransomware deployment mechanisms.

When it comes to prevention, the organization reiterates that ransomware is being primarily distributed via emails containing toxic attachments or hyperlinks leading to malicious payloads. With that said, the number one recommendation is to make sure that employees can identify a phishing attack and avoid getting on the hook.

Healthcare facilities should also prioritize their data and store the most important records separately from the rest of their systems. Furthermore, regular software updates, reliable anti-malware tools, and the use of strong passwords or two-factor authentication (2FA) will make it much harder for adversaries to break in.

RYUK RANSOMWARE KEEPS SUCKER-PUNCHING HOSPITALS

An enterprise-targeting ransomware operation called Ryuk continues to infect hospitals despite the crisis. Security researchers spotted one of these attacks in March 2020. According to their findings, the criminals used the PsExec remote execution tool to pollute the digital infrastructure of an undisclosed U.S. health organization. The predatory program locked down critical data and created ransom notes on plagued computers.

Around the same time, security company SentinelOne detected a well-coordinated campaign in which Ryuk operators tried to hit multiple COVID-19 response facilities across the United States. Their high-profile targets included two independent clinics and a network of nine hospitals.

DHARMA RANSOMWARE TAKES THE SAME ROUTE

An infamous ransomware family dubbed Dharma has not changed its usual repertoire either, mounting destructive attacks against hospitals amid the coronavirus emergency. It debuted in 2016 as a threat targeting individuals and was later repurposed to hunt down enterprise networks.

One of the recent Dharma variants cashes in on the COVID-19 theme in several ways. It uses a binary file called 1covid.exe, which is camouflaged as a harmless email attachment. Once an unsuspecting victim opens this file, the ransomware contaminates the system and launches a post-exploitation scenario to try and infect other computers on the same network.

Then, a mix of the RSA and AES cryptographic algorithms kicks in to encode the organization's files. Interestingly, the contact email address listed in the ransom note is coronavirus@qq.com. Depending on the size of the breached network, the ransom amount can range from several to tens of bitcoins.

RUSSIAN CROOKS HAUNT EUROPEAN PHARMACEUTICAL FIRMS

In January 2020, pharma companies based in Germany and Belgium underwent extortion attacks orchestrated by two hacking groups. According to analysts from security services provider Group-IB, Russian-speaking cybercriminal rings codenamed Silence and TA505 were responsible for these incidents. While the latter had been previously active in targeting the healthcare industry, Silence had focused on compromising financial institutions and took a sharp turn when the pandemic broke out.

Both gangs reportedly used privilege escalation vulnerabilities cataloged as CVE-2019-1322 and CVE-2019-1405 to infiltrate the targets' networks. Luckily, the onslaughts were detected and halted before they could do any damage.

Although the criminals didn't get a chance to run their code, Group-IB researchers claim the attacks were most likely ransomware operations masqueraded as data breaches. As part of their reasoning, the white hats emphasize that the TA505 crew is known to have deployed ransom Trojans in the past, including Rapid and Locky.

FAIR PLAY BY SOME THREAT ACTORS

As opposed to shenanigans described in the previous paragraphs, several ransomware gangs claim to be discontinuing attacks against hospitals. In March 2020, experts from the BleepingComputer security resource attempted to reach out to criminals in charge of mainstream cyber extortion campaigns. The researchers' goal was to find out if the bad guys were planning to leave the healthcare scene due to the coronavirus emergency.

Believe it or not, the analysts have heard back from some of the addressees. The operators of the increasingly widespread Clop ransomware said hospitals and charitable organizations never were among their intended victims, and this would not change. Even if such an institution gets infected by accident, the crooks will purportedly send it a decryption tool with no strings attached.

The villains said they did not consider businesses in the pharmaceutical sector to be worthy of their mercy, though. The reason is that these companies are prospering during the pandemic, and therefore they will have to pay up if attacked.

The authors of DoppelPaymer, another active ransomware strain, claimed to follow suit. According to their response, if a hospital ends up on their hook, they will allegedly decrypt its files without further ado. To be eligible for such treatment, though, the victim must give evidence that it is a healthcare provider. Similarly to Clop, this syndicate won't meet pharma companies halfway in terms of the ransom demands.

Cybercrime groups behind the ransomware lineages called NetWalker and Nefilim said they never specifically targeted clinics or nonprofits and were not going to do the opposite. But there is a caveat: NetWalker will expect a ransom if a healthcare organization gets trapped unintentionally.

The operators of Maze, a ransomware species that steals victims' data before encryption and uses it for extra pressure, stated that they wouldn't be plaguing computer networks of hospitals until the pandemic was over. However, they must have worn a poker face when writing that reply. Here is why. Soon after making their promise, they leaked files retrieved during an attack against Hammersmith Medicines Research, an organization testing COVID-19 vaccines. This data included personal records of numerous former patients.

In June 2020, Maze also exposed the personal information of more than a thousand patients of the Montana VA Health Care System, which provides services to veterans. The initial attack had taken place in late April, and the felons unleashed their rage against the victimized organization that was not willing to pay the ransom. What is the moral of the story? Ethics is an empty word for these double-dealing scoundrels.

THE BOTTOM LINE

The world is confronted with unprecedented circumstances that make cyber threats and real-life perils merge into a bizarre whole. Never before have people's lives depended so heavily on the integrity of electronic systems. In these challenging times, ransomware operators are showing their true colors. By targeting critical healthcare infrastructure and blocking access to hospitals' databases, they impede proper medical response where mere minutes can make a game-changing difference.

Although some extortion gangs have purportedly stopped attacking hospitals, for the time being, taking their promises on trust is a slippery slope. Instead, the healthcare industry should focus on hardening their defenses and thwarting ransomware raids proactively.

First and foremost, all valuable data must be backed up. Also, security awareness training of the personnel plays a decisive part in these countermeasures, because most ransomware incidents start with a slip-up where an employee opens an eye-catching email attachment. Proper account sign-in hygiene through hard-to-guess passwords or 2FA should not be underestimated. Furthermore, an effective anti-malware application should be able to identify all prevalent forms of ransomware and block them before they wreak havoc. ■

ABOUT THE AUTHOR

David Balaban is a computer security researcher with over 17 years of experience in malware analysis and antivirus software evaluation. David runs MacSecurity.net and Privacy-PC.com projects that present expert opinions on contemporary information security matters, including social engineering, malware, penetration testing, threat intelligence, online privacy, and white hat hacking. David has a strong malware troubleshooting background, with the recent focus on ransomware countermeasures.