Tri Valley PLASTIC SURGERY

HEALTHCARE INFO SECURITY®

Plastic Surgeons Warned About New Face of Cyber Extortion

FBI Says Patients, Doctors at Risk of Ransom Demands After Theft of Records, Photos

Marianne Kolbasuk McGee | October 19, 2023

The FBI is warning plastic surgery practices and their patients of cybercriminals targeting their sensitive health information and medical photos for extortion schemes. The alert followed recent hacking incidents at several plastic surgery practices involving data theft.

The FBI in an alert this week warned that cybercriminals are targeting personal identifiable information and health records, including sensitive patient photographs taken by the medical practices.

The criminals then extort ransom payments from the practices and patients to remove or stop the information and images from being disclosed on public-facing websites or shared with the patients' friends, family or colleagues, the FBI warned.

The attacks include three phases - data harvesting, data enhancement and extortion. In the first phase, cybercriminals spoof email addresses or phone numbers to phish and deploy malware at the practices and then harvest sensitive patient information and images.

In phase two, the cybercriminals use open-source information, including information harvested from social media sites and collected through social engineering schemes, to enhance the stolen patient data.

In the third phase, criminals contact the plastic surgery practices and patients through social media accounts, emails, text messages or messaging apps, and demand cryptocurrency payments to prevent the disclosure of the stolen information and images, the FBI said.

Recent Attacks

Several plastic surgery practices in recent months have reported hacking incidents to regulators involving stolen patient information, including California-based Beverly Hills Plastic Surgery, which reported a hacking incident to the California attorney general in August.

In its report, the practice said it had detected unusual activity in its IT environment on June 16. The investigation determined that an unauthorized actor may have acquired certain files and data - including patient names and medical information - stored in its systems, the practice said.

Data breach blog site DataBreaches.net reported last month that BlackCat/Alphv threat actors had posted photos and information on their dark web leak site that the group claimed to have stolen from Beverly Hills Plastic Surgery.

Beverly Hills Plastic Surgery did not immediately respond to Information Security Media Group's request for comment.

In July, a California-based plastic surgery practice operated by Dr. Gary Motykie reported to Maine regulators a hacking incident that potentially affected the health and personal information, including medical images, of nearly 3,500 patients.

In its breach report, Motykie said that on May 9 the practice was notified that "a third party" may be in possession of its patient information.

Motykie's practice said it worked with law enforcement and an incident response team and determined on June 6 that patient information had potentially been compromised in the breach. That includes name, address, Social Security number, driver's license or identification card number, healthcare insurance information, financial account or payment card number, medical information and history, and medical images taken in connection to the medical services provided.

The practice said it had responded to the incident by disabling access to the affected computer, taking the system offline and implementing various other security measures.

DataBreaches.net reported in July that patient information and photos allegedly stolen from Motykie's practices had been uploaded to a dark web site that appeared to be operating from Russia. No criminal group claimed credit for the leak.

Local media NBC Los Angeles reported that police records show that threat actors in May demanded Motykie pay $2.5 million to prevent the public release of his own and his patients' data.

An attorney representing Motykie in the breach incident did not immediately respond to Information Security Media Group's request for comment.

Lucrative Target?

So far, reports to the American Society of Plastic Surgeons about these types of incidents have been "minimal," Dr. Steven Williams, the group's president-elect, told ISMG.

"However, it is clear that as the world becomes more connected and more digital, we will have more incidents and bad actors trying to jeopardize medical care and patient safety. Hospitals, insurers and doctors' offices have all become targets because data is critical to patient care," he said.

While healthcare groups of all types have been targeted by cybercriminals and ransomware attackers in recent times for ID theft, fraud and extortion, plastic surgeons and their patients appear to have a special appeal for some threat actors, other experts said.

"Plastic surgery is a profitable business where customers primarily pay upfront," said Shawn Surber, senior director of technical account management at security firm Tanium. "This means that both the surgeon and patients generally have substantial disposable income and are interested in protecting their privacy more against embarrassment than concerns about identity theft."

Plastic surgeons also tend to work independently. They have small offices with limited and usually contracted IT support, and they often partner with private surgery centers that have similar limitations, Surber said.

"This also means that the physician and the surgery center are also potentially communicating outside of usually secure channels - such as using personal or web-based email, for example - creating additional opportunities for malicious actors to intercept data, credentials and intelligence."

The FBI advised medical practices and their patients to carefully review the profile settings in their social media accounts, limit what can be posted by others on their profiles and take other steps to secure accounts, including using unique and complex passwords.

Stan Mierzwa, who heads the Center for Cybersecurity at Kean University in New Jersey, advised medical practices to consider blocking access from certain parts of the globe.

"The motives and targets of cyber attackers will evolve and change, and although certain sectors may not be a focus in the immediate time frame, it is important for organizations to remain vigilant and aware of this potential," he said.

Williams of the ASPS said the professional association has resources to help mitigate cyber risk and hosts educational meetings and webinars to keep its members up to date. He also said members should consider obtaining cyber insurance coverage.

"Some of it comes down to common sense. The most important practices include an offline backup of all critical data that is backed up systematically and routinely and encryption of any sensitive or patient data that is stored," he said. "The next most important step is team education so that all members are aware of the risks and strategies to mitigate those risks."

https://www.healthcareinfosecurity.com/plastic-surgeons-warned-about-new-face-cyber-extortion-a-23355