Hackers keep trying new targets in search of easy data

April 14 2015, byBrandon Bailey

Credit: George Hodan/Public Domain

The health care sector has become the hot target for hackers in recent months, according to researchers at Symantec, a leading cybersecurity company that says it's also seeing big increases in "spear-phishing," "ransomware" and efforts to exploit newly discovered vulnerabilities in software used by a wide range of industries.

After a wave of high-profile attacks on banks and retailers over the last two years, almost 80 percent of the calls to Symantec's global "incident response" service since December have come from health organizations, said Robert Shaker, a Symantec official who oversees the commercial service.

While usually seeking valuable patient and employee data, hackers who target health organizations may inadvertently disrupt computer systems that oversee medication and other life-saving treatments, Shaker said during a press event Monday.

The health sector's vulnerability to hackers was underscored earlier this year when Anthem, the giant insurance firm, reported a data breach affecting up to 80 million customers. But as each sector strengthens its defenses, Shaker said, hackers move on to new industries that may be vulnerable. He predicted schools and universities may be the next big targets.

Higher education is "another area very similar to health care," where administrators have historically been less focused on computer security, said Shaker. He noted that university computer networks hold a variety of valuable data, including financial records for students and employees, as well as scientific and medical research.

Several universities have already reported large data breaches in recent months, according to reports compiled by the nonprofit Privacy Rights Clearinghouse, which says the University of Maryland, North Dakota University and Butler University in Indianapolis have disclosed that hackers obtained personal identifying information for hundreds of thousands of students.

Symantec Corp. is one of the biggest companies in a growing industry that sells software and expertise for defending against cyberattacks—so

it has a vested interest in highlighting security threats. But findings in its annual Internet Security Threat Report, released this week, generally echo observations of other industry experts.

Along with an overall jump in the volume of malicious software, Symantec said it's seeing an increase in software designed specifically to siphon information from smartphones and other mobile gadgets. It also counted a surge in certain kinds of "spear-phishing" attacks, in which hackers send deceptive email or text messages to consumers or company employees, hoping they will click on a link that infects their computers with malware.

In a particularly dramatic trend, Symantec reported almost 9 million incidents of "ransomware" attacks last year, more than double the total from 2013. "Ransomware" programs aim to extort money from computer users through various threats. One typical program displays a message that says child pornography or other illegal material has been found on the user's computer, and demands the user pay a fine to avoid prosecution. But in a trend that has boomed over the last year, Symantec says, hackers also use software that encrypts files on the target computer—making them unusable—and demand payment to de-encrypt them.

Some hackers have added extra code to "ransomware" that remains on a computer and even adapts itself to carry out other tasks, such as siphoning valuable information, said Kevin Haley, Symantec security response director.

Hackers are also increasingly using automated software that spams companies or repeatedly probes their networks for vulnerabilities, which means they can launch multiple attacks with less effort, said author and security expert Marc Goodman, who spoke at the Symantec event.

And even as the Obama administration is urging industry officials to share information about defending against attacks, hackers are sharing knowledge among themselves. Would-be hackers can easily buy malware online and even find instructional videos on public sites that explain how to carry out attacks, said Lillian Ablon, a researcher at the Rand Corp.