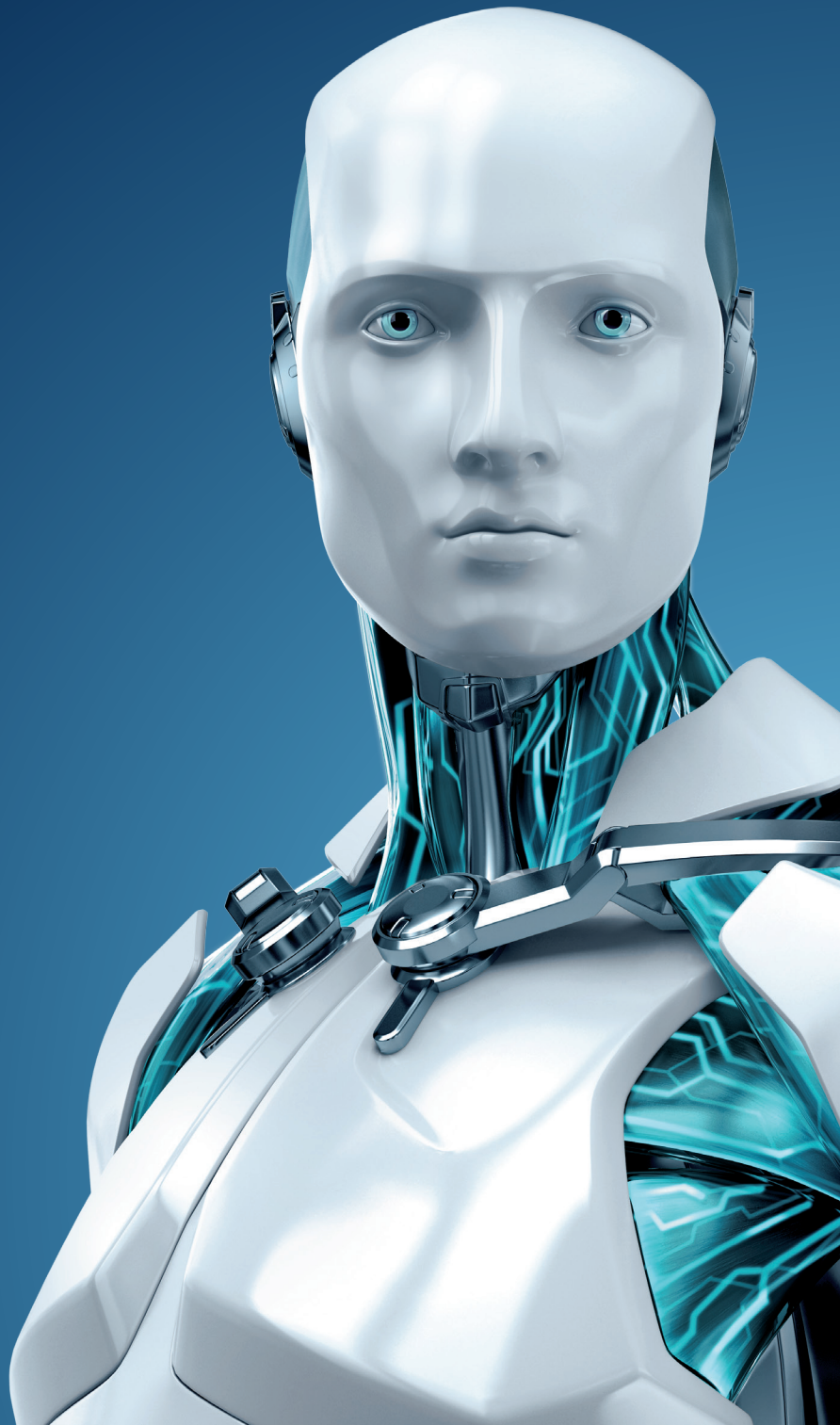
TECH BRIEF

Healthcare telemedicine security and the malware industry



ENJOY SAFER TECHNOLOGY™

HEALTHCARE TELEMEDICINE SECURITY AND THE MALWARE INDUSTRY

By Stephen Cobb, ESET Security Researcher

Telemedicine—the practice of electronically connecting geographically separated doctors, patients, and other elements of healthcare delivery—is not new, but it's now growing faster than ever before. Interestingly, the same can be said for another industry, one that many medical professionals know surprisingly little about: malware production. This brief looks at the implications of this situation for the long-term success of telemedicine and its potential to deliver benefits to society.

> **The global telemedicine market is expected to grow by nearly 20 percent per year for the next few years, and is on track to exceed $27 billion by 2016.**

Right now, the pressure on telemedicine to deliver both health benefits and cost savings has never been greater. As a result, the global telemedicine market is expected to grow by nearly 20 percent per year for the next few years, and is on track to exceed $27 billion by 2016. America probably represents more than a quarter of that market— around $7 billion. Such a rapid pace of technology deployment, particularly one that is partially driven by changes in industry regulation, tends to ring alarm bells for information security professionals due to a long history of unhappy consequences.

Consider the electronic filing of tax returns, introduced in 1986. Telemedicine could learn some lessons here. Recently, Treasury Secretary Jack Lew testified that more than 80 percent of Americans now file their tax returns electronically, "saving the Department [the IRS] millions of dollars every year." Sounds like a success story, right? Unfortunately, Lew avoided mentioning that in July of last year the Treasury's inspector general for tax administration estimated that fraudulent tax refunds made possible by electronic filing have already cost the Treasury $5.2 billion. In addition, more than $20 billion in potentially fraudulent refunds could be issued electronically in the next five years.

These are not theoretical losses. In cities like Miami and Tampa, we've seen multiple cases of criminals "earning" a million dollars or more, each, from such schemes, which rely on a form of identity theft. Why is this relevant to telemedicine? Because it tells us that any security vulnerabilities in telemedicine technology that can be used to make money will eventually be exploited, mercilessly and at scale. It also tells us that building security into systems from the outset works much better than bolting on security after technology has been deployed (just as a healthy lifestyle to prevent heart disease is more effective than fixing up a diseased heart).

Three factors for success

So what are the chances that telemedicine will succeed in maintaining the confidentiality, integrity, and availability of health-related information in the foreseeable future? Right now, they do not look good, and I base that assessment on three factors:

1. Historic lack of focus on security within telemedicine.

The systematic review of telemedicine literature published in 2011 by Garg and Brewer made it pretty clear that the sector was not yet living and breathing security in the way it must if it wants to survive exposure to the malicious elements that will eventually attack

it: "There is a dearth of standardization in telemedicine security across all chronic illnesses under study. It also appears that many telemedicine researchers are unfamiliar with the field of security in general."

2. The sad state of healthcare security in general.

You need look no further than the Ponemon Institute's Third Annual Benchmark Study on Patient Privacy & Data Security, published in late 2012, to know that all is not well: "Healthcare organizations seem to face an uphill battle in their efforts to stop and reduce the loss or theft of protected health information (PHI) or patient information… The consequence of not having adequate funding, solutions, and expertise in place is clear. Since first conducting this study in 2010, the percentage of healthcare organizations reporting a data breach has increased and not declined."

> **Healthcare organizations seem to face an uphill battle in their efforts to stop and reduce the loss or theft of protected health information (PHI) or patient information… The consequence of not having adequate funding, solutions, and expertise in place is clear.**

During the rollout of the HIPAA privacy and security rules a decade ago, I had the pleasure of working with Dr. Larry Ponemon, and I know that he does not jump to conclusions or make casual assessments. The above is his considered opinion, and it is a chilling one when you flesh it out with statistics like the percentage of organizations in the study that had at least one data breach in the past two years: 98 percent. Indeed, the average number of breach incidents for each participating organization in the past two years was not one or two, but four. Clearly, the existence of a framework of privacy and security regulations and fines has not forced healthcare institutions to do a stellar job of protecting patient data.

3. The emergence of the malware industry.

While factors 1 and 2 would be bad news enough for telemedicine, the third factor, the emergence of a sophisticated malware industry, is perhaps the scariest. Why? Because it is not yet on the radar of enough people in the world of healthcare IT. Indeed, right now there are not enough people in general who know that all it takes to engage in cyber crime is a lack of ethics and a basic knowledge of how to surf the Web.

In recent years, we have entered a new phase of digital malfeasance, in which all of the elements you need to rip off people and companies, from malware to mules, are available to rent or buy. For those not familiar with the jargon of this thriving underworld that exists just below the surface of the Web, malware is malicious code, the software that infects and suborns digital devices, from desktops to smartphones, laptops to tablets, card readers to Web servers. Mules are the people who turn fake credit cards into cash, like the $45 million that was taken from ATM machines around the world earlier this year, in a matter of hours.

Thanks to these markets, and the natural processes of specialization and division of labor that they foster, the people who write the elements of malicious code—the droppers, bootkits, rootkits, keyloggers, exploit packs, DDoS modules, spam modules, obfuscators, packers, and injection scripts—have been able to focus on what they do best, then sell their wares and services to the highest bidder, in most cases with very little risk of detection, let alone prosecution. That means new exploits can be developed and deployed quicker than ever.

As soon as they figure out how to profit from compromising the massive amounts of data flowing through telemedicine systems, the bad guys will attack that "market" with the same vigor we have seen in their exploitation of the banking system, retailers, telecom operators, and just about any business that handles a lot of money. The fact that malware-based attacks on telemedicine may put people's lives at risk will pose no impediment to the perpetrators.

Conclusion

As a big fan of technology, I can see the enormous benefits that people and society are poised to reap from telemedicine. The president of the American Telemedicine Association, Edward Brown, MD, recently pointed to exciting new initiatives "like ACOs, Medicare readmission penalties, and the medical home—programs that need telemedicine at their core—including telehomecare, remote monitoring, text messaging, videoconferencing, and eConsultation." Yet there is one set of bars on a chart in the Ponemon study that tells me the task of realizing these benefits in a safe and sustainable way is not going to be easy. It shows the percentage of healthcare data security incidents classified as criminal attacks. That number rose from 20 percent in 2010 to 33 percent in 2012. I fear we are seeing the result of too little security expertise applied too late. Whether it is healthcare in general, or telemedicine in particular, failing to respond adequately to this situation could have tragic consequences for an industry full of promise.