DOI:10.1145/3097347

Adam L. Young and Moti Yung

Privacy and Security

Cryptovirology: The Birth, Neglect, and Explosion of Ransomware

Recent attacks exploiting a known vulnerability continue a downward spiral of ransomware-related incidents.

Cryptovirology was born out of scientific curiosity of what the future may hold for software attacks that merge cryptographic technology with malware. It started at Columbia University as a natural by-product of an unnatural union: a former hacker placed in a room with a cryptographer, both given ample time with which to contemplate the dystopia of tomorrow. Collectively, given our backgrounds, we had amassed a body of highly unconventional scientific problems that hackers face when infiltrating computer systems as well as the foundational cryptography with which to solve those problems.

Our list of problems included the following question: How devastating could the most insidious malicious software attack be against a target? To put things in perspective this was circa 1995. Many people had not heard of the Internet, and among those that did, many were obtaining an email address for the first time. The typical home computer was not online all the time. Users had to use dial-up modems when they wanted to check email. USB technology did not exist. 3.5-inch floppy disks were the norm. Cryptography, for millennia, had been perceived as a purely protective technology, and in particular as a way to hide the content of messages, secure data at rest, and authenticate users.

On the one hand we were aware of the failed AIDS Information Trojan that scrambled the names of the victim's files using a symmetric key and demanded a ransom to unscramble them. From a technological perspective this attack crumbled since the decryption key could be extracted from the code of the Trojan.

In addition, we had in mind the grotesque vision of H.R. Giger in the science-fiction movie *Alien*.[5] Of particular interest to us was the alien facehugger. This creature resembled a cross between an insect and an octopus. It would wrap its legs around the victim's face and insert a tube down the victim's throat. It wrapped its long tail around the victim's neck and squeezed. The victim would enter a form of coma, while the egg the facehugger implanted into the abdomen would incubate into a drone (or queen) and burst through the stomach of the victim, thus completing a phase of the alien life cycle.

There was no way to safely remove the facehugger once attached. Touching the facehugger caused it to tighten its tail and restrict the flow of air to the lungs. Cutting it caused its corrosive alien blood to bleed out and disintegrate everything it seeped through (including the floors of the spaceship). Try as they did the crew's scientists could not find a way to safely remove facehuggers from their victims.

The AIDS Trojan and the facehugger idea defined in our minds the "where we are now" versus where malicious software attacks might evolve

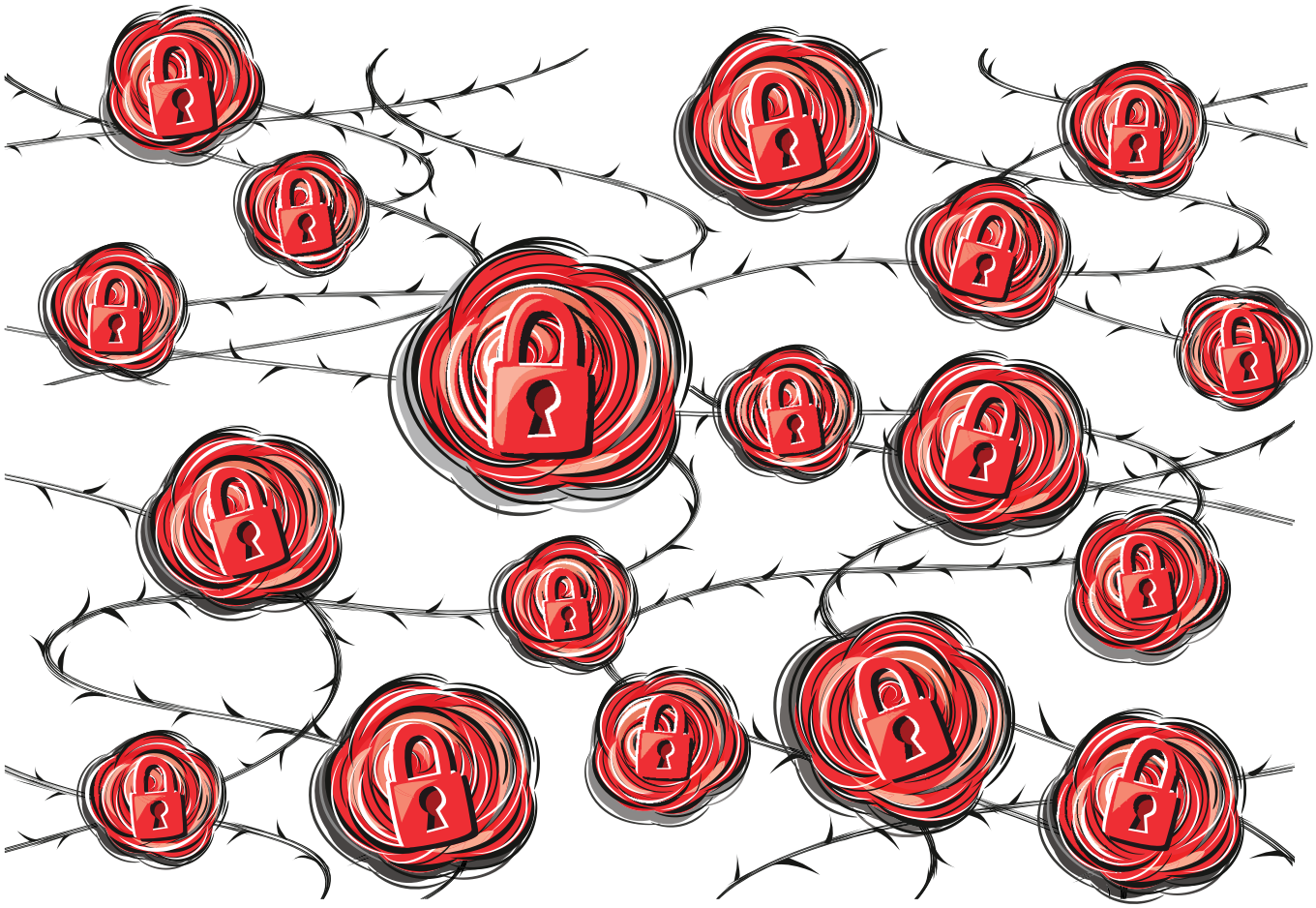

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

to, respectively. We sought a digital analogue of the facehugger, namely, a forced symbiotic relationship between a computer virus and its host where removing the virus is more damaging than leaving it in place.

But what we discovered was not exactly that which we sought. We discovered the first secure data kidnapping attack. We called it cryptoviral extortion. In cryptoviral extortion, the attacker generates a key pair for a public key cryptosystem and places the "public encryption key" in the cryptovirus. The corresponding "private decryption key" is kept private. The cryptovirus spreads and infects many host systems. It attacks the host system by hybrid encrypting the victim's files: encrypting the files with a locally generated random symmetric key and encrypting that key with the public key. It zeroizes the symmetric key and plaintext and then puts up a ransom note containing the asymmetric ciphertext and a means to contact the attacker. The victim sends the payment and the asymmetric ciphertext to the attacker. The attacker receives the payment, decrypts the asymmetric ciphertext with his private key, and sends the recovered symmetric key to the victim. The victim deciphers his files with the symmetric key.

At no point is the private key revealed to the victims. Only the attacker can decrypt the asymmetric ciphertext. Furthermore, the symmetric key that a victim receives is of no use to other victims since it was randomly generated.

We presented this attack along with the facehugger analogy at the 1996 IEEE Security and Privacy conference.[8] The discovery was perceived as being simultaneously innovative and somewhat vulgar. Years later, the media relabeled the cryptoviral extortion attack as ransomware. In the conference paper we proposed that electronic money could be extorted by the attacker. This is what happens today using bitcoin. We have observed that what we described over 20 years ago is the exact "business model" used today in an estimated $1 billion-a-year criminal industry: the industry of ransomware.

We discovered that public key cryptography holds the power to break the symmetry between the view of an antivirus analyst and the view of the attacker. The view of the antivirus analyst is the malware code and the public key it contains. The view of the attacker is the malware code, the public key it contains, and the corresponding private key. The malware can perform trapdoor one-way operations on the victim's machine that only the attacker can undo. A multitude of cryptovirology attacks, both overt and covert in nature, are based on the unique advantage this gives to the attacker. These methods weaponize cryptography as an attack tool as opposed to the previous uses that were defensive in nature.

In our 2004 book *Malicious Cryptography: Exposing Cryptovirology*[9] we presented the following analogy: cryptovirology is to penetrating computer systems as cryptanalysis is to cracking ciphers. It is a proactive anticipation of the opponent's next move and suggests that certain countermeasures should be developed and put into place. To counter cryptoviral extortion we recommended a diligent backup strategy and searching for crypto code where it

does not belong. We warned the public about these threats and similar ones by publishing our findings, thereby providing a significant head start to develop and deploy defenses.

It has been a long road that we have followed, fraught with skepticism and criticism, ultimately resulting in worldwide recognition that cryptoviral extortion is a severe threat. Over the years we have given numerous lectures on cryptovirology. We have experienced the spectrum of possible reactions. Some concurred that the threat is real. Others insisted that cryptoviral extortion was pointless, that it offered nothing to the attacker beyond deleting the hard drive. Still others professed that no victim would ever pay.

Shortly after we published our book, it was met with harsh criticism. An expert who had written books on computer viruses published a scathing review, concluding that for those seriously involved in the study of malware the book is of "little practical use." This opinion directly translates to telling the public there is no need to worry about ransomware. We attributed such reactions to the inherent resistance many people feel toward new ideas, especially ideas that merge two previously distinct disciplines, in this case, malware and cryptography. It seemed to us that the difficulties known as the "innovator's dilemma"[2] apply also to proactively addressing threats and risks.

Cryptovirology has proven itself to be a formidable threat. Ransomware attacks make the news daily. Victims include individuals, hospitals, police precincts, universities, transportation systems, and government offices. We even saw the development of "ransomware as a service" where cryptovirology tools are sold to criminals that perpetrate cryptoviral extortion (for more details on ransomware, see https://en.wikipedia.org/wiki/Ransomware). This past year we have witnessed a vicious downward spiral: the more organizations that were attacked, the more news coverage there was on ransomware. The more news coverage there was on ransomware, the more criminals got in on the action, prompting ever more news coverage. The media amplified cryptovirology awareness among law-abiding citizens and criminals alike.

Cryptovirology has proven itself to be a formidable threat.

Social and legal reactions to the damage followed. In fact, the trip further down the spiral changed the very definition of a "computer breach." Prior, a computer breach was synonymous with the exfiltration of sensitive data from an organization. This past year the meaning expanded to account for ransomware. A recent fact sheet published by the U.S. Department of Health and Human Services on ransomware and HIPAA states that when electronically protected health information is encrypted by ransomware a breach has occurred and the incident therefore constitutes a disclosure that violates HIPAA.[6] The justification for this definition is that the adversary has taken control of sensitive health information. This is a significant change in the definition of a computer "breach" since now, due to the threat of cryptoviral extortion, a breach can occur even when no sensitive data is exfiltrated!

A highly publicized and effective ransomware attack was carried out against the Hollywood Presbyterian Medical Center, and the hospital paid $17,000 in bitcoin for restoration. This, along with the epidemic levels of similar attacks, prompted the state of California to enact a new law that addresses ransomware.[1] "SB-1137 Computer crimes: ransomware" amends Section 523 of the Penal Code to outlaw the introduction of ransomware into a computer system with the intent of extorting money. Reuters reported that the WannaCry cryptoworm from May 2017 locked up more than 200,000 computers in more than 150 countries.[7] The attack exploited a vulnerability hoarded by the NSA that was exposed by whistle-blowers and later patched. The attack was nonetheless severe since organizations and individuals were not diligent enough in patching.

We finally point out that cryptovirology has influenced popular culture as well, inspiring the plot in Barry Eisler's techno-thriller *Fault Line*.[3]

Over the years we have observed a palpable reluctance by security companies to describe the cryptoviral extortion attack in detail and discuss countermeasures. We view this as being fundamentally flawed; it is the classic phenomenon of "reactive security" (acting after the attack) as opposed to the preventative "proactive security."

We believe ransomware is the tip of the iceberg. Most cryptovirology attacks are covert in nature, allowing the adversary to securely steal information completely unnoticed. These attacks would slip past or stymie the vast majority of computer incident response teams. It took over 20 years for cryptoviral extortion to gain worldwide recognition, and it appears that the bulk of these other attacks, which are fully described in the scientific literature, are heading in the same direction: destined to be overlooked until a large-scale real-world attack is publicized. Santayana's aphorism: "those who cannot remember the past are condemned to repeat it"[4] seems to apply equally well to malicious cryptography. C

References

1. Barth, B. California ransomware bill supported by Hollywood hospital passes committee. *SC Magazine* (Apr. 13, 2016).
2. Christensen, C. *The Innovator's Solution: Creating and Sustaining Successful Growth.* Harvard Business School Press, 2003.
3. Eisler, B. *Fault Line.* Ballantine Books, 2009.
4. Santayana, G. *Reason in Common Sense*, (1905), p. 284, volume 1 of *The Life of Reason.*
5. Scott, R. *Alien.* 20th Century Fox, 1979.
6. U.S. Dept. of Health and Human Services. FACT SHEET: Ransomware and HIPAA; http://bit.ly/29zm57B
7. Volz, D. and Auchard, E. More disruptions feared from cyber attack; Microsoft slams government secrecy. Reuters (May 15, 2017).
8. Young, A. and Yung, M. Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings of the IEEE Symposium on Security and Privacy*, (1996), 129–140.
9. Young, A. and Yung, M. *Malicious cryptography—Exposing cryptovirology.* Wiley, 2004.

Adam L. Young (ayoung235@gmail.com) is a researcher at Cryptovirology Labs.

Moti Yung (motiyung@gmail.com) is a Security and Privacy Scientist, Snap Inc., and Adjunct Senior Researcher, Computer Science Department, Columbia University.