The Growing Threat of Ransomware

- BY BRIAN HEATER
- APRIL 13, 2016 07:00AM EST

Ransomware can hit anyone, but hackers are increasingly going after targets that are more willing to pay up.

It's been a strange few years for the Alina Simone. In 2011, she released her fourth full-length record to critical acclaim, followed by a book of essays and a debut novel, all while maintaining a journalism career and raising a young daughter. But it's likely a 2015 opinion piece for *The New York Times* that garnered the most recognition for the Brooklyn-based artist. "My gravestone will say, 'her mom got hacked,'" she says with a laugh.

Published in January of that year, How My Mom Got Hacked earned Simone a deluge of media appearances, from primetime news programs to an episode of the popular public radio program Radiolab. The story details her mother Inna's struggle with a mysterious form of malware and the strange and surprisingly cloak-and-dagger story that unfolded in its wake.

 "My mom called me one night, and she was ranting about needing to pay a ransom," she tells PCMag. "I had my laptop open but was also watching TV and half listening. I thought it was a typical mom rant about her hardware crashing [and] having to pay the repair people $500 because her computer crashed. I thought she was talking in air quotes. She kept saying, 'No, Alina, listen. I mean ransom.'"

By the time Simone got the call, there was less than 24 hours to hit the deadline. Her mother had attempted to withdraw the full amount of ransom, but a combination of the Thanksgiving holiday, the weekend, a snowstorm, and the highly volatile value of bitcoin had caused her payment to fall $25 short. A failure to pay would cause the $500 ransom to double.

Simone dropped everything the following morning and made a beeline to the nearest bitcoin ATM. "I had a full-time job and a toddler at home," she explains. "I had a busy morning, but I canceled everything and got a sitter. I ran over to Greenpoint where this bitcoin ATM was located in a shared workspace building. The ATM didn't work and it gave me the spinny wheel. We were freaked out by the virus, but bitcoin gave it this extra level of terror. It just freezes your brain — it's just another thing to figure out."

The story has a happy ending — at least so far as those things go. "She didn't make the deadline, and they were going to charge her double the ransom [but]

she pleaded with them and they let her go," Simone says. Mom got her files, the hackers got their money, and everyone who read the story in *The New York Times*learned about the phenomenon of ransomware, a strange, steadily growing form of malware that effectively holds a user's computer files at electronic gunpoint.

An Eye on High-Profile Targets

Simone's mother is not the only victim, of course. In a piece published late last year in *Info Security Magazine*, G Data Software Security Evangelist Andrew Hayter posited that 2016 will be "the year of ransomware," a sentiment echoed by similarly titled pieces subsequently published by big media outlets like the*Los Angeles Times* and security firms like Symantec.

Thus far, 2016 has brought with it increasingly high-profile examples, including, most notably, the case of Hollywood Presbyterian Medical Center, a 434-bed hospital whose network effectively ground to a halt after hackers breached the system in early February. After relying on pen and paper records briefly, Hollywood Presbyterian paid the 40 bitcoin ($17,000) ransom to regain control of its network.

More recently, MedStar Health and a hospital in Kentucky were hit with similar attacks, and the targeting of such larger institutions appears to be part of a growing movement.

"We're absolutely seeing that trend," explains Grayson Milbourne, Security Intelligence Director for Internet security firm Webroot. "It's true that there's an increase in focus on attacking corporate entities.

"The value of my personal files and pictures caps off somewhere. But [if] I encrypt the back-end of your corporate system and prevent you from processing payments, that has a tremendous value. And if the hacker can recognize the value of what he has, the ransom can be more dynamically set based on the content of the data."

G Data's Hayter concurs, but while hackers have been planning large-scale attacks for some time, "public companies never could admit that they had malware because it would hurt their stock," he says. "They kept security quiet. I think they've been hit all along, but they just don't talk about it."

What does seem certain is that payments like the one issued by Hollywood Presbyterian add fuel to the fire.

The Moral Quandary of Ransomware

Among the many ways ransomware is unique is in the moral quandary it presents its users. Thus far the malware's encryption has proven largely bulletproof, meaning that, once infected, the end-user has one of two options: either pay the ransom — thereby funding the activities of the criminals who hacked into their system — or lose the files forever.

 "At first I was really shocked that my mom wanted to pay it," explains Simone. "I told her not to. [I told her] 'you're funding these people. You might be funding terrorists. It's morally wrong, your files don't matter that much.' She said, 'they do to me. I've done my research and it's the only way to get it back.'"

Inna Simone was not alone in her decision. In the majority of cases, all is essentially lost once ransomware takes hold. A month after Simone paid the ransom, a police department in Tewksbury, Massachusetts, made a $500 payment after enlisting the help of the FBI. In fact, the encryption has proven so hard to crack that even the Federal Bureau of Investigation has essentially thrown up its hands in defeat.

"The ransomware is that good," Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI's CYBER and Counterintelligence Program told Boston's Cyber Security Summit in October. "To be honest, we often advise people just to pay the ransom."

The FBI declined a follow-up request, telling us that Bonavolonta was "unavailable," and instead offered up the following decidedly more noncommittal statement: "The FBI works closely with the private sector so that companies may make informed decisions in response to malware attacks. Companies can prevent and mitigate malware infection by utilizing appropriate back-up and malware detection and prevention systems, and training employees to be skeptical of emails, attachments, and websites they don't recognize."

The damage, however, was already done — at least as far as the security community was concerned.

"I think that the FBI has not helped the situation at all by coming out and saying that people should pay the ransom," says Hayter. "To me, that goes against everything we know about dealing with malware, bad guys, and cyber crime. You don't want to keep funding them, and that's what paying the ransom does. And they keep putting more funding into development, which seems to be what they're doing right now."

Webroot's Milbourne concurs. "They set a precedent of that being the only option." Small scale individual user payments of $200-$300 have already funded hackers to the tune of hundreds of millions of dollars, though he acknowledges that in real life, things are rarely so black and white.

"It's a personal decision," explains Milbourne. "[Webroot's] stance is that we don't believe what the FBI has told people to do is the right approach. That said, the hospital has a business to run. If it means people's lives, $17,000 is a reasonable price to pay to get your business back online. Does that mean it's a good precedent to be setting? No."

Easier Said Than Done

It's easy enough to pass judgment until one comes face to face with ransomware boldly announcing its presence. "Your files are encrypted," boasted the Cryptowall 2.0 lock screen that greeted Inna Simone, adding—in that fake-helpful ransomware way—that the "special software" CryptoWall Decrypter could be purchased for a limited time offer of 500 USD/EUR. All of that was ominously underscored by a clock counting down the seconds until the ransom doubled.

If there is an upside to the ransomware phenomenon, it is consumer awareness. And every party can agree that the best way to manage malware is to simply avoid getting hit in the first place.

Ransomware comes from a growing number of sources, largely through Internet connections, with a smaller percentage arriving through physical vectors like USB sticks. In most cases, however, the real breakdown occurs at a similar point of vulnerability: humans.

The same month the Hollywood hospital was hit, Baltimore-based firm Independent Security Evaluators issued the eerily prescient results of a two-year study involving a dozen healthcare facilities. In one scenario, researchers dropped 18 USB sticks loaded with simulated malware across various floors of a hospital. Within 24 hours, one unsuspecting user plugged one of the sticks in the system, requesting malware from ISE's servers. This was just a test, thankfully, but the scenario highlights the inevitable fact that a computer's security system is only as effective as the person using it.

"There's still terrible USB hygiene around the world with people still using XP service pack one," says Milbourne. "There are a lot vulnerable systems. But primarily [ransomware proliferates] through web exploit kits and direct email campaigns that trick people into being dumb and infecting themselves."

Protect Yourself

Like much of the malware out there, ransomware finds its way onto systems through untrusted sites and attachments. So the major tenants of avoiding an infection are similar to those for avoiding malware in general: install security software, keep your operating system and applications up to date, and don't visit any suspicious sites or open email attachments from unknown sources.

Hayter recommends getting rid of potential malware gateways like Flash and Silverlight, while OpenDNS Security Analyst Kevin Bottomley suggests installing an ad blocker and NoScript browser add-ons, as online advertisements become an increasingly popular vector for the spread of malicious malware.

Some websites use ad services "that generate revenue through attracting ad distributors, and they provide a lot of flexibility to those distributors with respect to how they code their ads to display on pages," says Milbourne. "It'll open in the background, the user has no idea."

This type of scenario recently hit a number of mainstream sites run by some of the most prominent names in publishing, from *The New York Times* to AOL, potentially exposing tens of thousands of users to ransomware in the U.S. alone within a 24-hour time period.

Equally disturbing is the speed with which ransomware is capable of spreading once a system has been compromised. According to Bottomley's research, "it's usually [a] sub-three-minute infection to encryption time." By the time you're finished grabbing a cup of coffee, ransomware has already had more than

sufficient time to do its thing. And as it's evolved, ransomware has become increasingly effective at propagating across a network.

The newly identified ransomware Locky, for example, has discovered how to identify and gain access to unmapped network shares. "You want to disconnect that endpoint from the network and limit any potential spread," says Milbourne. "And then it comes down to what got hit and what's infected. In a lot of cases, it's just an end-user. When we start to see problems is when these things propagate and start to hit resource servers and things that really impact the flow of business."

As ransomware becomes more sophisticated, the likelihood increases that even the most thoughtful users are at risk of getting hit, highlighting the importance of backing up files online and off. Restoring those files is admittedly inconvenient, but ransom seekers don't hold much sway when you've got unencrypted copies as a backup. It might sound like overkill, but ransomware is "becoming more and more prolific," says Hayter.

Humble Beginnings

The phenomenon has been around in some form other at least since the late 80s, when the AIDS trojan demanded users send $189 to a Panamanian post office box, lest their "conscience may haunt [them] for the rest of [their] life...and [their PC would] will stop functioning normally." Things have grown exponentially since

those early shady days of the PC Cyborg Corporation. In a report issued late last year, McAfee found a huge jump of late, from 257,357 new ransomware samples in the first half of 2014, to 380,652 in the second half. By the first half of 2015, that number jumped 5.3 times to over 2 million.

The security company added that the rapid growth is likely to continue, due in no small part to the relatively new trend of "Ransomware-as-a-service." Between the hundreds of millions of dollars extorted from smaller targets and the increasing focus on corporations and institutions, ransomware has proven to be an extremely lucrative business model — and one with decidedly less risk of bodily harm and capture than more traditional crime.

"Cyber criminals have figured out that they can make money more easily than with drug deals," says Hayter. "They're turning to cybercrime for their income. And then they can use that income to do more development and get into other forms of crime — or just make more money and buy more Ferraris."

A perhaps unexpected turn in the ransomware game is that hackers are adopting some traditional business tactics, like customer service. Simone's mother, for

example, was able to negotiate with the ransom seekers, who agreed to accept the final $25 a little after the deadline without doubling the ransom.

People "won't pay the ransom if they think they're f**ked anyway," Simone says. "It's e-commerce. They've taken all of the lessons of e-commerce from legitimate businesses and applied it to ransomware."

As McAfee notes, hackers have also developed custom malware solutions built to spec for potential ransomers — a sort of black-market version of Squarespace, if you will.

"You pay a certain amount," explains Hayter, "you get the ransomware, you customize it to yourself, you direct the payments where to want to direct them, you get 24/7 customer support for your ransomware product."

Part of the malware's business expansion model has involved the targeting of new platforms. Once largely the realm of Windows PCs, security analysts have been aware of the presence of Android variants for a number of years. This March also marked the first known instance of a ransomware attack on Mac users, as KeRanger demanded users pay one bitcoin ($400) to rescue files locked down after the installation of BitTorrent software, Transmission.

•

Two-Factor Authentication: Who Has It and How to Set It Up

"It's a sign that the criminals are seeing that there is some value in making Mac malware," explains Hayter. "In the past, the Mac just wasn't an attractive target because there wasn't the profit margin there. Now that [hackers] got through once, I think Apple is going to do a better job protecting the walled garden."

Apple was able to quickly address the issue by revoking the software's app development certificate and updating its malware protection, but it's hard not to see this first breach as a sign of more ominous things to come.

But for all their concerns, the security experts we spoke with are hopeful. "In the 40 years that malware has been around, we've found ways to defeat families of malware," says Hayter. "Catching up with the bad guys has always been the problem. They always seem to be one step ahead. But I think there's hope on the way in a very short amount of time. The anti-malware industry cannot wait. This is a rush job. This is an emergency."