RANSOMWARE

A Growing Threat

Anjali Kulkarni and Joseph M. Burton

Ransomware, a method of electronically attacking corporations and individuals by holding their data hostage, has gained massive popularity amongst hackers in the last several years. Ransomware is the first form of malware to present the threats of both the destruction of important data and the economic harm the loss of that data can create. Ransomware attacks will continue to increase in scope and severity in years to come, necessitating continuous vigilance.

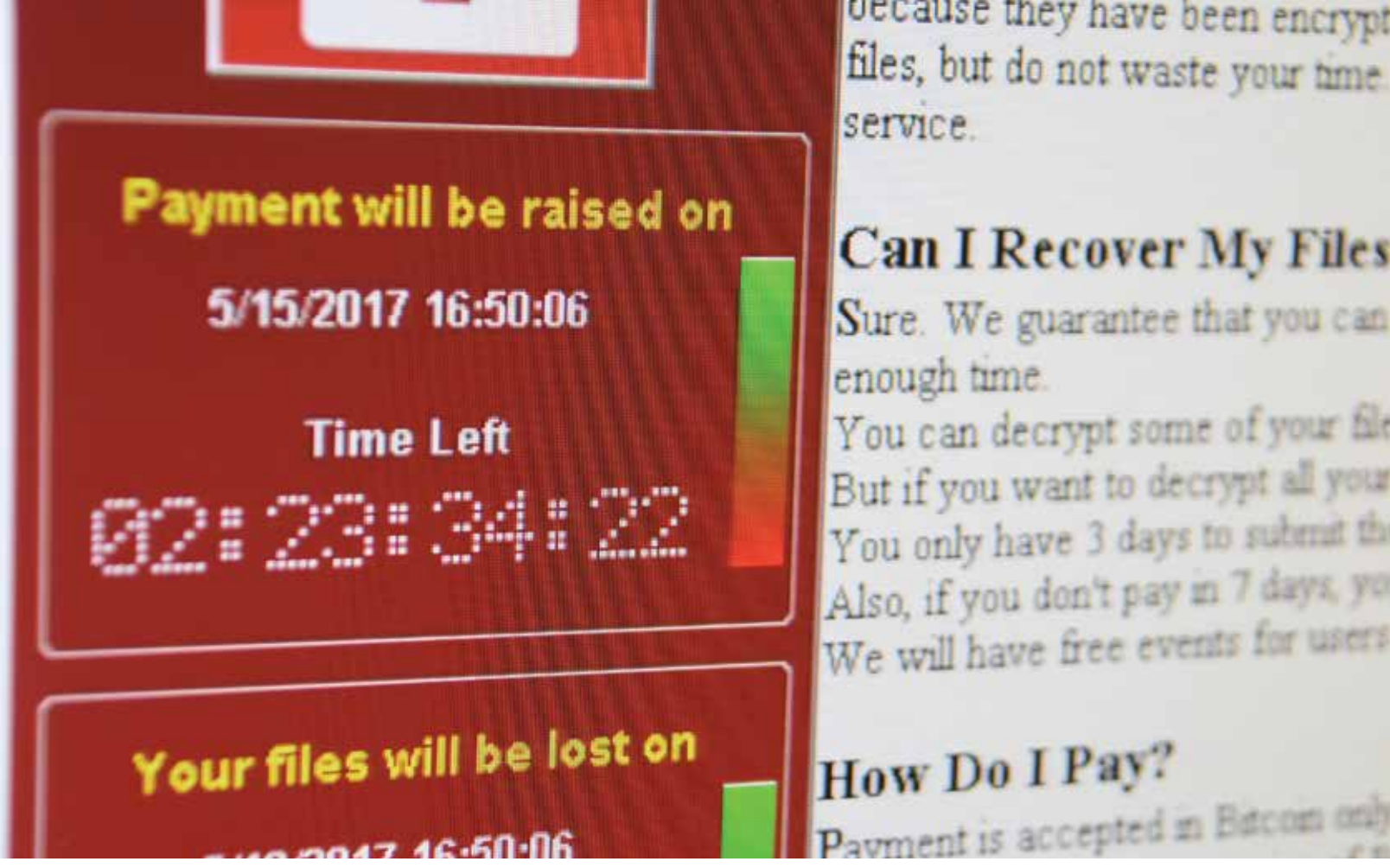
In essence, ransomware acts by taking data that is of value to an entity but not deleting it. The ransomware acts as a figurative glass wall, allowing the owner of the data to physically possess that data but not access it. This is accomplished by implanting a virus on the owner's hard drive, usually by means of an infected link in an email or other innocuous-looking document. Once the link is clicked, the ransomware works by encrypting the entire storage system. The hackers then threaten to destroy the data unless a ransom is paid.

2017 saw some of the worst ransomware attacks to date, escalating exponentially in size and gravity over previous years. According to a study by the Kaspersky Lab, over 479 million attacks occurred from online sources during the first quarter of 2017, up by over 250 percent from years past. These attacks ranged across countries and industries, and plagued corporations of all sizes.

2017 Ransomware Attacks

In May 2017, an international ransomware outbreak occurred in the form of WannaCry, a self-replicating computer virus that took advantage of a vulnerability in the Microsoft Windows program, infiltrating systems large and small. WannaCry infected over 300,000 computer systems in 150 countries, from China to Britain to the United States, including those of Britain's National Health Service. The virus asked for payment of 300 dollars in bitcoin digital currency for each compromised system, and threatened to erase the data in question within seven days. The attackers were paid approximately 130,000 dollars from various sources in bitcoin as a result.

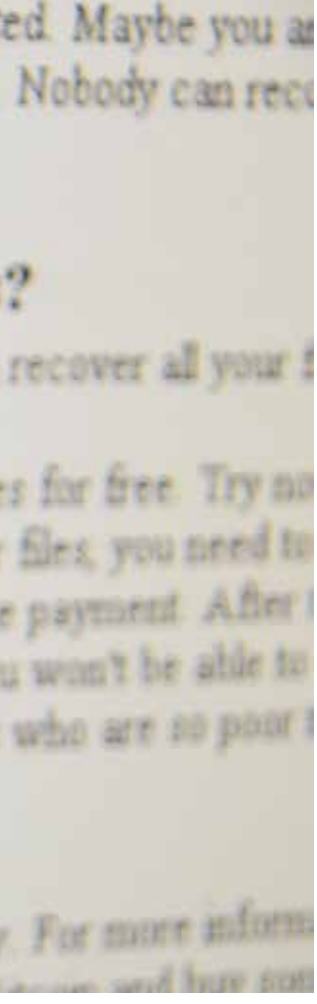
Ironically, Microsoft had released a patch to rectify the vulnerability exploited by WannaCry in March of 2017,



several months prior to the attack. The patch was part of 'automatic updates' for systems using Windows 10, but did not work on systems running older versions of the Windows system. Microsoft eventually released patches for the older systems, but not until WannaCry had caused serious damage on an international scale. WannaCry remained active for the majority of 2017, and has only recently started to decline in frequency.

In early June of 2017, another self-replicating computer virus known as NotPetya swept the international community, spreading itself from computer to computer in major networks by using a modified version of the WannaCry virus. NotPetya operated by seeking to gain administrative access on vulnerable systems and subsequently use that access to move to and encrypt data on other systems on the network. It appears that NotPetya exploited a vulnerability in the accounting software used by 80 percent of businesses in the Ukraine, creating a backdoor that allowed it to infiltrate systems when users conducted routine software updates. As it spread, NotPetya caused serious harm globally, economically damaging several international corporations. A unique aspect of NotPetya was the fact that despite requesting 300 U.S. dollars in bitcoin to release the information, NotPetya was programmed to permanently destroy the information it captured and never allow data owners to reclaim access, even after payment.

One major corporation severely affected by NotPetya was the Danish transport and energy firm Maersk, the world's largest container shipping business. NotPetya caused the shutdown of Maersk's information technology systems across multiple sites for five days, leaving employees to communicate



RANSOMWARE: 2017 IN NUMBERS

3 *massive outbreaks: WannaCry in May; Expetr in June; BadRabbit in October*

700,000 *victims of Wannacry worldwide*

1 IN 6 *businesses who paid ransom never recovered data*

65% *of businesses hit in 2017 lost access to a significant amount of data*

34% *of those affected took a week or more to restore full access*

Source: Kapersky Lab

via WhatsApp on their private phones. Maersk, which is responsible for approximately 15 percent of the world's shipping network, was forced to stop operations at over 70 shipping terminals internationally. This attack cost Maersk between an estimated 200 and 300 million dollars due to the negative impact on their business volume, creating a significant deficit in its profit margin for the third quarter of 2017.

Ransomware and Law Firms

Ransomware attacks have the potential to be especially detrimental to law firms, which rely heavily on electronically stored information in their daily business practices. This was exemplified by the havoc wreaked by NotPetya on the global offices of DLA Piper, an international firm with more than 3,600 attorneys, in June 2017. The attack originated in the firm's Madrid, Spain office and rapidly spread across its international network, including phone systems and the firm's web portal. The firm directed all employees to shut down computers as a precaution, and advised them to refrain from connecting to the firm's network at all costs. For several days, all DLA Piper's operations were at a standstill, with attorneys and staff having to conduct business via cell phone and texting. A week later, the firm was still recovering from the attack, bringing back informational services online in a graduated fashion to avoid corruption of data. Insurance brokers estimated that the fallout from the attack would cost the firm millions.

Ransomware attacks on law firms in the past several years have not discriminated based upon size. In May of 2016, a ransomware virus infected the ten-attorney Rhode Island firm of Moses Alfonso Ryan after one of its attorneys opened

a malware-encrypted email attachment. Moses Alfonso Ryan then lost all access to the documents and information stored on its network. Over the next several months, Moses Alfonso Ryan engaged in unsuccessful efforts to remedy the virus, eventually contacting and paying the ransom demand of the hackers via bitcoin in June of 2016. The firm then obtained an initial decryption key from the hackers, only to find out the key didn't work. Moses Alfonso Ryan made subsequent contact with the hackers, having to renegotiate a ransom price and paying a second ransom demand. The firm obtained a second decryption key, which served to finally allow Moses Alfonso Ryan to access its servers and network after almost three months of complete inability to gain entry. In June of 2017, the firm filed a lawsuit against its insurance company for the 700,000 dollars in lost billings caused by the attack.

RaaS on the Rise

Unfortunately, the forecast for 2018 does not indicate any relief from costly ransomware attacks, which look to be the most profitable hacker business model yet conceived. Ransomware is now offered as an online service for hackers on the dark web. Ransomware as a Service ("RaaS") is allowing the distribution of ransomware with increased frequency. This business model is expected to grow in popularity in the coming year. One of the most popular RaaS programs is Cerber, which works by encrypting the files of infected uses whether or not the infected computer system is connected to the internet. Cerber infestations accounted for over forty percent of ransomware attacks in 2017. Another distributor, Satan, showcases the RaaS distributor business model very simply—it mimics that of any other online service, allowing users to join for free and pay based upon profits. Satan's homepage tells hackers that they must sign up for an account, and that any bitcoin paid to them by ransomware victims will be credited to that account. Satan keeps 30 percent of the victim's payment as a form of payment, letting the purchaser retain the other 70 percent. RaaS distribution makes basic ransomware more widely available to non-sophisticated hackers on the dark net, increasing its spread and potential profitability.

With the threat of ransomware growing in frequency and severity, both corporate entities and individuals must be strategic in the handling of their data. This is especially true of that data which, if compromised, would impede or stop the conduct of business on a daily basis. There is a bright side, however, in that there are several simple things which can be done to protect against ransomware. The first, as illustrated by WannaCry, is to keep your software up to date. The second, which appears obvious, is to install antivirus software on all business computer systems. The third is to backup all data on separate backup drives which are not immediately connected to the primary system, thereby removing any access issues if the primary system is affected. Ransomware is rapidly evolving, but being consistently aware of threats and remaining prepared are the best protections corporate entities and individuals alike can take to avoid their data being compromised.

Anjali Kulkarni is a CIPP certified trial associate at Duane Morris in San Francisco with experience in handling cyber privacy and security related cases.

Joseph M. Burton is a partner at Duane Morris specializing in cybersecurity and digital evidence matters.