Ransomware Payment: Legality, Logistics, and Proof of Life

Part One: Background and Reality | by John Reed Stark

Ransomware is a type of malicious software that infects a computer and restricts users' access to certain data, systems and/or files until a ransom is paid. Ransomware can come in many forms and iterations and like any other virus or infection, ransomware can evolve and transmogrify to counter cyber-defenses and remediation. Although only a fraction of ransomware attacks are actually reported to federal authorities, the U.S. Department of Justice reports over 4,000 ransomware attacks occur daily.

A ransomware victim company's files are rarely exfiltrated by a ransomware attacker, rather the attacker encrypts the files so a victim company cannot access them. Then the hacker offers to sell the encryption key to the victim, typically payable in an anonymizing online crypto-currency such as Bitcoin. The usual ransomware demand comes with a deadline -- after which time, the ransomware attacker threatens that the key will be destroyed or will expire, rendering the kidnapped files forever inaccessible. In many cases the ransom note that hijacks the victim's screen is accompanied by a digital clock ominously ticking down the minutes and seconds from 72 hours. When the timer expires, the ransom demand usually goes up or even doubles – or the data is permanently locked and henceforth unrecoverable.

Bitcoin and other convertible crypto-currencies have become the keystone to current ransomware schemes, rendering the transactions practically untraceable and well suited for criminal transactions. Unlike the sequence of events during a common kidnapping scenario, where the exchange of money arguably places criminals in their most vulnerable position, virtual kidnapping of ransomware actually facilitates anonymity throughout the Bitcoin transaction process.

First published on the Nasdaq Governance Clearinghouse

RANSOMWARE GROWTH

According to a recent study by IBM, spam emails loaded with ransomware increased 6,000 percent in 2016 compared with 2015, comprising almost 40 percent of all spam messages in 2016. Another report, from cybersecurity firm Symantec, cited 460,000 ransomware attempts in 2016, up 36% from 2015, with the average payment demand ballooning from $294 to $1,077, a 266% increase. Ransomware attacks have grown almost exponentially for several reasons:

- The ransomware business model works, with the FBI stating that ransomware is on pace to be a one billion dollar source of income for cybercriminals in 2017;
- Ransomware start-up costs are cheap. Ransomware software is readily and easily available – and is extraordinarily inexpensive. Ransomware is available for rent, for purchase or even in kits for building. Indeed, 60 percent of the Internet's top sites sell ransomware; and
- Ransomware schemes are typically successful. One recent study found that 70 percent of business victims paid the hackers to get their data back. Of those who paid, 50 percent paid more than $10,000 and 20 percent paid more than $40,000.

Ransomware attacks target the most vulnerable part of a company's computer networks: people. The primary attack vector for ransomware is an employee who has clicked on a file or a link he or she should not have clicked. That employee may be:

- an accidental insider (e.g. an inattentive employee infiltrated due to inadvertent behaviors or broken business processes);
- a compromised insider (e.g. a targeted employee via social engineering and infiltrated due to malware infections or stolen credentials); or
- a malicious insider (e.g. a so-called bad leaver or criminal insider who infiltrated via corporate espionage and sabotage).

Ransomware is sometimes embedded in seemingly legitimate downloads such as software updates or resume files. Fake Adobe Flash updates are a notorious Trojan horse for delivering ransomware because Flash is such a ubiquitous add-on to most Internet browsers. Once inside a network, some ransomware can seed itself to additional computers or other devices via SMS messages or a user's contact list.

What makes ransomware countermeasures challenging is the evolution of ransomware variants. There has been a tremendous increase in ransomware strains – reaching almost epidemic proportions. Indeed, new ransomware strains are now being created to tap into the mobile user base – which can impact both personal and business information – dramatically expanding the ransomware threat landscape, and diversifying and expanding their platforms, capabilities and techniques in order to accrue more targets.

Per recent reports, in the third quarter of 2011, about 60,000 new variants of ransomware were detected. That number doubled to over 200,000 in 2012 and quadrupled to over 700,000 variants from 2014 to the first quarter of 2015. In the first quarter of 2016, security firm Kaspersky Lab revealed 2,900 new "modifications" of existing ransomware, a 14% increase from the last quarter, and a 30% increase from the previous quarter.

As the *Internet of Things* begins to establish a foothold in daily life, ransomware growth seems poised to become more severe and more widespread. Market forecaster Gartner expects 6.4 billion connected devices will surround us in the home and workplace this year, a $30 billion market by the year 2020. This growing network of Internet-connected household devices, from Samsung refrigerators to Nest thermostats, will undoubtedly render individuals and corporations increasingly vulnerable to ransomware attacks.

RECENT RANSOMWARE ATTACKS

While ransomware has beleaguered victim companies for much of the last decade, a recent global spate of ransomware attacks has prompted intense media coverage and worldwide apprehension and concern.

For instance, in April 2017, a ransomware group known as *Shadow Brokers* coopted a ransomware exploit (nicknamed *Eternal Blue*) from the U.S. National Security Agency, and took advantage of a Windows vulnerability, targeting a wave of hospitals. The ransomware extortion demands impacted more than just corporate operations and secrets; suddenly, a cyber-attack impacted the lives of sick hospital patients, prompting an almost international hysteria.

The vulnerability, patchable for new Microsoft systems but not necessarily for older systems upon which many hospitals were running, was dubbed "WannaCry" or "WannaCrypt" ransomware, and according to Europol, claimed over 200,000 victims in over 150 countries.

A few months later in June 2017, Honda Motor Company fell victim to WannaCry ransomware and was forced to halt vehicle production after finding WannaCry ransomware in its plant computer network. Specifically, Honda's Sayama Plant in northwest Tokyo has a daily output of roughly 1,000 vehicles, ranging from Accord to Odyssey models, but was closed down after the ransomware was discovered. While production eventually continued, the data breach continues to prove the lasting effects of WannaCry.

Similarly, in late June 2017, another strain of ransomware hit at least six countries, including and primarily Ukraine, where it was blamed for a large and coordinated attack on key parts of the nation's infrastructure, from government agencies and electric grids to stores and banks. According to Microsoft, this outbreak, referred to as NotPetya – aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya and Diskcoder.C – resulted in "a less widespread attack" than WannaCry, aka WannaCrypt.

As a result of NotPetya ransomware, ATM's in the Ukraine apparently stopped working; workers were forced to manually monitor radiation at the old Chernobyl nuclear plant when their computers failed; and data security personnel at companies around the world – from Maersk, the Danish shipping conglomerate, to Merck, the drug giant in the United States – were reportedly scrambling to respond. Even an Australian factory for the chocolate giant Cadbury was affected.

Though more sophisticated than WannaCry and employing the same Eternal Blue server message block exploit, NotPetya's global impact was reportedly blunted by its own limited attack capabilities (e.g. by a default setting, the infected system reboots after 60 minutes, and the malware does not persist after the reboot). "This means that the threat can only do lateral movement and exploitation of other machines during this limited time," Microsoft says. "This reduced the reach of the attack."

WINTER IS COMING

Upon his capture in 1934, the legendary bank robber Willie Sutton was asked by FBI agents, *why do you rob banks, Willie?* Sutton replied, *because that's where the money is*. The same goes for ransomware attackers except that instead of banks, Hollywood is now where the money is. Hollywood hoards in its coffers a virtual treasure trove of online assets and possessions.

As major movie and television studios have moved their operations online and as video streaming has become commonplace, Hollywood's entertainment properties have become increasingly vulnerable to ransomware attack and cyber-criminal exfiltration. With streaming services like Netflix and Hulu leading the way, the global entertainment industry is now worth around $2 trillion, equivalent to the combined value of the world's top 10 banks. HBO by itself generates over $6 billion in revenue, creating an especially alluring opportunity for online attackers.

Thus not surprisingly, albeit via a more traditional method of extortion, HBO became the latest cyber-attack victim, when online attackers apparently exfiltrated more than 1.5 terabytes of data from inside HBO's network, including upcoming episodes of shows like *Ballers and Room 104* and thousands of internal documents. But the headline-grabbing crown jewel of the HBO cyber-attack was reportedly the theft of episodes, scripts, etc. from the wildly popular HBO series, *Game of Thrones*.

In an extortion video sent to HBO, obtained by Mashable, the purported attackers used white text on a black background to threaten further disclosures if HBO failed to pay "our 6 month salary in Bitcoin," which the attackers implied to be at least $6 million. "We often launch two major operations in a year and our annual income is about 12–15 million dollars. We are serious enough to do our business," the ransom note to HBO read. "We don't play with you so, you in return, don't play with us. You only have 3 days to make decision so decide wisely." HBO is apparently the attackers' 17th target, and the attackers claim only three have failed to pay up.

Interestingly, the real damage to HBO may end up having little to do with *Game of Thrones*. The exfiltrated data reportedly also included a month's worth of HBO emails as well as the apparent contact list of HBO chief executive Richard Leper, which reportedly also contained the personal phone numbers of a litany of HBO series actors. As evidence of the damage, Google was served with a *Defense Contract Management Agency (DCMA) Takedown Notice*, which revealed that the HBO attackers also leaked "masses of copyrighted items including documents, images, videos and sound."

As an aside, a so-called *DMCA Takedown Notice* is a tool utilized in accordance with Title II of the Digital Millennium Copyright Act ("DMCA"). The DMCA Takedown Notice essentially exempts certain online service providers from liability for copyright infringing acts by its users, provided it meets certain conditions, such as being responsive to copyright holders when given notice of infringement on the network the service provider controls (such as a *DCMA Takedown Notice*). A *DMCA Takedown Notice* can be a cost-effective, quick, and powerful means of compelling online service providers to remove material that infringes copyright, such as a *Game of Thrones* episode. Given the proliferation of online piracy, the *DMCA Takedown Notice* provides entertainment companies like HBO a forceful tool to protect their rights.

Whether the hackers accessed any of HBO's intimate (or perhaps ugly) secrets contained in its stolen email and documents may present the ultimate challenge for the entertainment behemoth. Many of the more than 50 internal documents released were labelled "confidential", including a spreadsheet of legal claims against HBO; job offer letters to several top executives; slides discussing future technology plans; and a list of 37,977 emails called "Richard's Contact list", an apparent reference to Plepler. Plepler confirmed the attack, stating ominously, "The problem before us is unfortunately all too familiar in the world we now find ourselves a part of."

The HBO attack bears some striking similarities to the 2014 Sony cyber-attack, when attackers believed to be linked to North Korea breached Sony's computer network. In the Sony cyber-attack, the attackers released tens of thousands of internal emails, as well as the social security numbers of thousands of employees, which led to a multimillion-dollar settlement for Sony employees and the resignations of several key executives, including famed Sony studio head Amy Pascal.

The Sony attack also may have shared similar coding traits to other WannaCry ransomware attacks. While coding details of the HBO attack remain under forensic investigation, it is possible that the HBO attackers utilized a WannaCry related strain of ransomware malware or another type of ransomware. According to recent data from McAfee, of the nearly 100 million more incidents of malware in the first quarter of 2016, the vast majority were types of ransomware. In the first quarter of 2017, McAfee found 9,597,233 cases of ransomware, a huge uptick from the first quarter of 2016, when the security firm found 6,029,206 incidents of ransomware.

LAW ENFORCEMENT AND RANSOMWARE: THE OFFICIAL VIEW

The official line from federal law enforcement with respect to Ransomware is: *Report the Incident and Don't Pay*. Specifically, the FBI warns:

"The FBI doesn't support paying a ransom in response to a ransomware attack… Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. [B]y paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

The FBI also warns that paying ransomware does not guarantee that a victim company will obtain from the attacker a working key to rescue their data. The FBI is aware of cases where either the attackers fail to hand over the correct decryption key or are unwilling to comply with the original ransomware demands after payment is received. According to Trend Micro research, nearly 33 percent of firms that pay the ransom when attacked by ransomware fail to get their data back. The FBI also urges ransomware victims to report ransomware attacks immediately and seek help from the FBI in handling the situation.

Along similar lines, during an emergency meeting to address the WannaCry ransomware attacks, Tom Bossert, Homeland Security Advisor to President Donald Trump, discussed the perils of ransomware payment, and warned that victims could still lose access to files even after making a payment:

"Well, the U.S. government doesn't make a recommendation on paying ransom, I would provide a strong caution. You're dealing with people who are obviously not scrupulous, so making a payment does not mean you are going to get your data back."

LAW ENFORCEMENT AND RANSOMWARE: THE UNOFFICIAL VIEW

In some public settings, the FBI has warned that, without paying a ransom, victim companies may not be able to unlock their kidnapped data from ransomware attackers who use Cryptolocker, Cryptowall and other potent malware strains.

"The ransomware is that good," said Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI's CYBER and Counterintelligence Program in its Boston office. "To be honest, we often advise people to just pay the ransom … The amount of money made by these criminals is enormous and that's because the overwhelming majority of institutions just pay the ransom."

Indeed, the Ponemon Institute reported in a 2016 study that 48% of businesses victimized by ransomware paid the ransom (average ransomware payment being $2,500), while a similar IBM security study found that 70% of business victims paid the ransom during that same period.

Even some law enforcement officials themselves have decided to cut their losses by paying off the purveyors of ransomware. For instance, in the Massachusetts townships of Tewksbury and Swansea, ransomware attackers made off with $500 and $750 bounties, respectively. Elsewhere, police departments in the Chicago suburbs of Midlothian and Dickson County, Tenn., also paid ransom amounts to ransomware attackers. That even law enforcement officials have opted to cut their losses by succumbing to, and paying off, ransomware attackers demonstrates how oddly commonplace ransomware payments have become.

*John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also worked for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and for five years as managing director of a global data breach response firm, including three years heading its Washington, D.C. office. Mr. Stark is the author of, "The Cybersecurity Due Diligence Handbook," available as an eBook on Amazon, iBooks and other booksellers.