6-13-2021

Understanding Ransomware Trajectory to Create an Informed Prediction

Jacob D. Klusnick
Portland State University

Understanding Ransomware Trajectory to Create an Informed Prediction

J. D. Klusnick
Portland State University
Portland, OR 97201 USA
jklusnick@gmail.com

***Abstract*—Ransomware is a form of extortion in which digital files are rendered inaccessible until a ransom payment is made. Modern ransomware emerged in 2006 and its destructive influence has been expanding ever since. In recent years cybercriminals have evolved who they target, what computer systems they target, and how they infect those systems. Meanwhile, cybersecurity experts have modelled ransomware methods allowing them to innovate their defense techniques across three paradigms: recovery, detection, and prevention. Ultimately either ransomware attackers or ransomware defenders will dominate this ongoing conflict. A review of the literature indicates that the ransomware crime wave will likely be mitigated in the coming decades as security tools improve, users become more aware of the threat, and governmental entities step in to enforce punishments.**

Index Terms — Countermeasures, cyberattack, internet security, ransomware

I. Introduction

Ransomware extortion is an emerging type of crime in which victims must pay to regain access to their computer or files. You may have heard of ransomware in the news before. Just last year it was responsible for a shutting-down hundreds of hospitals in one of the largest medical cyberattacks the United States has ever seen [1]. A 2014 ransomware attack has cost Home Depot more than US$200 million in total [2]. Maersk, world leader in container shipping, had to replace 50,000 computers in an attack that has cost the company roughly US$300 million [3]. Cumulatively, ransomware is estimated to cost the globe US$20 billion by 2021 [4]. Undeniably, ransomware has established itself in the few years it's existed, but what does the future hold for ransomware?

For the last fifteen years cybersecurity experts have been fighting an ongoing battle to protect the world from ransomware. Cybercriminals and cybersecurity experts are constantly racing to outpace each other's progress. As ransomware techniques evolve, new security tools evolve to thwart cybercriminals. In response, new ransomware techniques emerge to evade security measures. Eventually one side has to win out; either ransomware will become too difficult to be profitable, or security will be too difficult to be feasible.

The purpose of this literature review is to examine the techniques that have emerged in ransomware attack and defense to inform predictions about the prevalence and severity of this crime in coming years. Drawing methodological trends from the literature allows me to infer the trajectories of both cybercriminals and security researchers. I review scholarly sources, predominantly peer reviewed research articles, but also industry publications, news articles, and topical podcasts to establish the methods by which ransomware attacks are carried out, as well as cybersecurity experts' approaches to ransomware defense. By comparing the progress in these two fields I'll argue that ransomware is a serious threat, but a threat that cybersecurity experts can mitigate and significantly diminish in the future.

II. Background

Ransomware is a subset of malicious software designed to take a victim's computer or data hostage and demand a ransom payment to regain access. The term comes from the combination of the "ransom" the victim is asked to pay and the "software" that takes hold of the computer system. These ransoms tend to be paid in cryptocurrencies such as Bitcoin, however, paying the ransom doesn't guarantee the valuables will be released. When dealing with criminals there is always the possibility they won't hold up their end of the deal. Unfortunately, due to ransomware's newness and online anonymity, these criminals often fall through the cracks of international jurisdiction and go unpunished. Therefore ransomware has become an attractive low-risk criminal venture. Being victimized by one of these attacks is undeniably frightening and challenges users' sense of online security.

Ransomware attacks usually follow a predictable pattern. Below are the basic steps of a standard ransomware attack; delivery, execution, payment, decryption, and liquidation [5].

A. Delivery

The ransomware must be delivered to the victim's system for the attack to begin. 'Delivery' doesn't

necessarily capture the harm occurring here though, and since ransomware is considered a disease this process is also colloquially referred to as 'infection'. The actual payload delivered is called a binary and it's composed of code that determines the actions of the ransomware. Infection methods vary greatly and I will address them in-depth in my "Infection method" section later.

B. Execution

The ransomware binary activates and begins following the instructions that the attack developer set out. As you would expect in a black market execution instructions vary widely, making the creation of an accurate ransomware execution model particularly challenging. Still, ransomware execution can be divided into three generic stages; stealth operations, suspicious activities, and obvious actions [6].

1) *Stealth Operations:* The ransomware must familiarize itself with the victim's system before initiating the attack. Cybercriminals want their ransomware to remain undetected during this initial step to prevent the attack from being interrupted prematurely [7].
2) *Suspicious Activities:* The ransomware initiates the damaging part of the attack without announcing itself, potentially remaining undetected. For locker ransomware this stage would include restricting the user interface, for crypto ransomware it would include encryption [6].
3) *Obvious Actions:* The ransomware announces its attack to the victim and makes its demands known by way of ransom note. At this point the damage has been done to the victim's system so the ransomware is ready to reveal itself [6].

C. Payment

Now that the ransomware has been executed it is time for the victim to decide if they'll pay the ransom. If they choose to, payments are usually made in bitcoin rather than a national currency. Bitcoin is a cryptocurrency, a digital currency created to circumvent any central authority. Whereas national currencies are minted and legally enforced by a government, bitcoins are entirely decentralized [8]. This makes it attractive to criminals because it's unregulated and users remain practically anonymous, providing cybercriminals a method of receiving ransom payments safe from prying eyes [5]. Additionally, transactions are irreversible and bitcoins are universally available for victims to purchase [9]. Oftentimes ransom notes contain instructions for the victim to buy bitcoin from online exchanges then send them to the attacker's wallet address.

D. Decryption

In the most likely case of a crypto-ransomware attack, after the payment has been received the ransomware may decrypt the files automatically or provide the victim with a decryption binary so they can do it manually [6]. Don't forget we're dealing with criminals though, and payment does not guarantee decryption. At this point the victim has already made their payment, so there's little incentive for the attacker to follow through on decryption.

E. Liquidation

Finally, time for the ransomware attacker to reap their rewards! The attacker cashes out their bitcoin in exchange for a national currency. This is the riskiest stage for the criminals because it links the proceeds of their crime to their identity. To mitigate this risk attackers will sometimes attempt to hide their tracks by shuffling ransom payments from different victims [5]. Once the ransom has been liquidated the attack is complete.

Ransomware has but one goal by definition, to exploit the victim. Cybercriminals employ a wide variety of methods to achieve this goal, but not all methods are created equal, and as such some gain popularity while others fall out of favor. An excellent example of this constant evolution is the transition from locker ransomware to cryptographic ransomware as the dominant attack method. Locker and crypto are the two main ransomware types [7], however, cybercriminals are creative and there are no rules to the game they play. These two types do not encompass the entirety of ransomware variety, others exist, but for the purposes of this example they are appropriate.

From approximately 2011 to 2012 locker ransomware was the dominant cyber extortion threat, only a few years after its emergence in 2008 [7]. Locker ransomware is based on the idea of locking the victim out of their computer. That is achieved by taking over the user interface, usually restricting user capabilities so that the computer can only be used to pay the ransom. Generally, locker ransomware only affects the user interface, leaving the users' files unharmed. That allows tech-savvy victims to often fully recover from these attacks by restoring system settings or using security tools [7]. Additionally, if the victim is able to transfer the computer's hard drive to an uninfected computer then no data is lost [10]. Therefore, locker ransomware isn't the most effective ransomware variant. To make up for its weaknesses many locker ransomwares employ social-engineering techniques meant to prey on the victims' fears and emotions to manipulate them into paying the ransom. For example, it's common for locker ransomware to impersonate law enforcement, claiming to have caught the user engaging in illegal activity online, then asking the victim to pay a fine for their indiscretion. While it has the potential to be very effective against simple computers with limited user interface functionality, locker ransomware has its weaknesses against complex computers [7]. For these reasons cybercriminals began transitioning to cryptographic ransomware en masse in 2013 and haven't looked back.

In 2013 crypto ransomware rose to become the dominant cyber extortion threat and continued to explode in

popularity among cybercriminals [7]. By 2016 more than 95% of new ransomware was of the crypto variety [6]. Cryptographic ransomware is based on the idea of locking the victim out of their files, rather than just their computer, and the only person that can unlock that data is the attacker. A cryptograph is a coded message, so this variant of ransomware achieves its goals through encryption, translating valuable files into unreadable gibberish that only the attacker can decrypt. Encryption requires a key -- a string of letters and numbers, like a password -- so when an attacker locks your file with their key that file can only be unlocked with their key. In this way the attacker denies the victim access to their personal files while often leaving computer functionality otherwise untouched. Once struck by a crypto attack a victims only method of recovery is decryption of the affected files, whether that be via ransom or a decryption tool. The penetrating nature of cryptographic ransomware paired with the strength of mathematical encryption makes crypto-ransomware very effective [7]. Due to the ubiquitous nature of crypto ransomware in recent years any future references to ransomware will refer to crypto ransomware unless otherwise specified.

III. Brief Ransomware History

Ransomware is one of the biggest focuses for cybersecurity experts right now [9]. Studying the events that have made ransomware what it is today is helpful in understanding the future of ransomware.

A. 1989

First recorded ransomware, the AIDS Trojan, is deployed at the World Health Organization's International Aids conference via 5¼ inch floppy disks mailed to the conference intentionally mislabeled "AIDS Information – Introductory Diskettes". The first of its kind, the AIDS Trojan didn't actually pose a threat because it used such simple, symmetric cryptography. The ransom was set at $189 USD to be sent to a PO box in Panama. Unlike most ransomware we know who the author was, Joseph L Popp, a biologist now considered the 'father of ransomware' [11]. Clearly ransomware was not a threat at this point, rather, in this era malware was used in pranks and vandalism to gain notoriety [7].

B. 1996

Adam Young and Moti Yung, cryptographers, describe the concept of cryptographic ransomware and name it cryptovirology. They published a groundbreaking paper proposing that cryptography -- traditionally used defensively for privacy, authentication, and security -- could be used offensively for extortion-based attacks. They emphasize that asymmetric encryption is essential to these attacks, and warn that access to cryptographic tools should be well controlled [12]. Unfortunately, that warning fell on deaf ears, setting the stage for ransomware to come.

C. 2005

Young and Yung implement the concept they had described years earlier and once again warn against the threat of ransomware. However, this time they also include some user countermeasures: backup your data, have a strong defense (firewall and antivirus), and only download from trusted sources [13]. This represents the first known crypto-ransomware implementation and established the expectation that cybersecurity experts publish ransomware countermeasures.

D. 2006

The first criminal ransomware to make use of asymmetric encryption emerges, only one year after Yung and Young's proof-of-concept. As they had warned, this represents a massive leap forward in the destructive potential of ransomware and the emergence of effective criminal cryptoransomware. There's some debate over which ransomware virus did it first, but it was either Archiveus Trojan or GPcode. GPcode disguised itself in a malicious job application email attachment and targeted Russian internet users [11]. The author of GPcode continued to improve their ransomware by enhancing the encryption strength, releasing three versions in the span of five days; the third version used encryption that would have taken 30 years for a contemporary computer to crack [14]. Archiveus Trojan required victims to purchase items from an online pharmacy to receive the 30-digit decryption key [11].

E. 2007

Lou & Liao, security researchers, published a paper claiming that users' misuse of computer systems had resulted in privacy violations skyrocketing. In response they began promoting awareness and education of ransomware as a means of ransomware prevention [15]. Importantly, this was the first time researchers in information systems security addressed ransomware.

F. 2008

Gazet, a computer virologist, analyzed three early families of ransomware based on their quality of code, ransomware functionality, and cryptographic strength. He concluded that researchers should continue to monitor ransomware, but at the time it was not mature and complex enough to warrant the attention it was receiving in the media, going as far as to say that it was doomed to failure as a mass extortion scheme [16]. At this point the research community had identified ransomware as a problem, but dismissed its severity without even offering potential solutions.

G. 2009

Bitcoin enters the scene and revolutionizes ransomware, transforming it into an established black market. Up until now, ransoms had to be paid in roundabout ways because untraceable online payment was not an option. For example, victims have paid by mailing prepaid cash-equivalent cards, calling a premium rate phone number, or ordering goods from the attacker's online store [10]. Ransomware attackers were eager to transition to Bitcoin because existing methods were inherently traceable [5].

H. 2013

CryptoLocker is unleashed upon the world and spreads like wildfire. As the name suggests CryptoLocker is a crypto-ransomware; its infection methods include malicious email attachments sent to business professionals and misleading downloads on compromised websites [11]. CryptoLocker went on to infect roughly 500,000 machines and experts estimate CryptoLocker's revenue at US$3 million conservatively and US$27 million on the high end [17]. Once the ransom note had been presented victims were only given three days to pay, after which the decryption key would be deleted or the price would jump dramatically, depending on the version. CryptoLocker demonstrated to cybercriminals and researchers that cryptoransomware was a mature business model characterized by reliable and untraceable payment. Within three months other cybercriminals adopted CryptoLocker's business model and multiple copycat ransomwares began circulating [18]. The impact CryptoLocker had on the ransomware industry is best illustrated by looking at the number of attacks in 2013; 100,000 in January and 600,000 in December [7]. Attacking at such scale put a target on CryptoLocker's back, and within one year security firms had infiltrated the cybercriminal network and set up an online decryption portal which helped keep the percentage of victims that paid the ransom low at 1.3% [17].

I. 2015

A cybersecurity research group publishes a groundbreaking study in the same research area as Gazet. Similar to the previous study but larger, this study reviewed 1,359 ransomware samples from 2006-2014 and found that although a few ransomware samples were sophisticated and threatening, most used superficial techniques [19]. Once again the research community argued that stopping advanced ransomware attacks was simpler than the media was reporting. However, this paper took it one step further. In the process of studying so many ransomware extortion methods they determined that ransomware could theoretically be detected and distinguished from harmless applications by measuring system behavior. This discovery is massively important because it enables researchers to begin detecting ransomware attacks for the first time. Whereas previous research dismissed ransomware as a legitimate threat and stopped there, Kharraz et al. develops a foundational model of ransomware behavior and uses it to advance state-of-the-art defense.

J. 2016

The next year a follow up study was published that implemented the method described in the 2015 paper. By monitoring file accesses and system behavior the research team was able to detect ransomware with a 96.3% accuracy [20]. This is the birth of detection-based defense, an important approach to ransomware defense. Much of the ransomware defense research that has since been published builds upon this study's techniques, or in some way has these authors to thank.

K. 2017

Ransomware has its most notorious year to date with the widespread attack of WannaCry. WannaCry leveraged an exploit created by the National Security Agency (NSA) that had been stolen and leaked by a group known as the Shadow Brokers. The initial infection likely occurred over an unprotected public internet connection, essentially coffee shop Wi-Fi. What made WannaCry especially devastating was its ability to self propagate like a true virus, meaning damage is not only limited to the machine infected but any other machine on that network [21]. In a matter of hours WannaCry infected hundreds of thousands of machines in more than 150 countries, targeting individual users, business organizations, and public agencies. Although not very profitable, WannaCry infamously targeted the United Kingdom's National Health Service which catapulted ransomware into public consciousness [11].

L. 2019

Early in the year a group of cybersecurity researchers published a study of contemporary ransomware and concluded it was rapidly diversifying. The recommendation to counter this diversification was to develop better models of ransomware behavior so defenders can more effectively detect and respond to attacks [6]. At this point the research community had fully embraced the idea that they could offer solutions to combat ransomware. Late in the same year MITRE ATT&CK, a cybersecurity expert curated ransomware model, was published online. ATT&CK stands for Adversarial Techniques, Tactics, & Common Knowledge. As the acronym suggests, the model catalogs ransomware methods and was freely available to any person or organization for the purpose of creating a safer world [22].

As you can gather from this brief timeline, in the last fifteen years defending against ransomware has become a serious challenge that we must not underestimate. Early on ransomware development moved slowly and was often pioneered by security research. Security experts were ahead of the curve until cryptocurrencies gave cybercriminals the tools they needed to criminally abuse academic research anonymously. Ransomware defense has been playing catch-up ever since, but even with ransomware attack on the forefront, development isn't linear. Oftentimes one criminal or group innovates and makes a sporadic leap in ransomware progress that others copy, then that technique becomes widespread and eventually standard practice.

Also, ransomware developers have an inherent head start on large-scale defense efforts for two main reasons. First, even when security measures have been suggested by professionals and the dangers warned against, little preventative action has been taken. Only in recent years have we seen ransomware warnings finally taken seriously by governments and industries, but it's taken financial incentives to make that change. It would appear that only after being burnt are organizations willing to invest the resources necessary to heed the warnings that the stove is hot. Second, as new ransomware attack variants emerge, ransomware defenders need time to develop a suitable defense. Consider the criminal black market that ransomware innovation operates within today. Very little information is available to defense researchers for them to base their techniques upon, besides those observations they make themselves. Similar to a fighter facing a new opponent, defense researchers need to learn the strengths and weaknesses of their foe before making an educated decision on how to fight. Thankfully, in the last few years the fight is swinging in favor of defenders as they collectively share their cumulative knowledge and enjoy greater access to essential resources.

IV. Research Justification

Ransomware is a growing threat to which we are all vulnerable. Despite this fact, the general population isn't adequately knowledgeable about ransomware or how to defend themselves against it, particularly college students [6]. A 2017 study found that despite being a likely target for ransomware attacks, more than half of college students were not familiar with the term 'ransomware' [6]. Cybersecurity experts refer to the three pillars of user-based cybersecurity: awareness, behavior, and culture [23]. In keeping with Portland State University's motto "Let Knowledge Serve The City", I wanted to take the opportunity to spread awareness about this danger to students and faculty and potentially have a positive impact on the cybersecurity of PSU. To this end I have included a list of seven best practices that Internet users can follow to protect themselves from becoming a ransomware victim in the Prevention section.

V. Attack Overview

Ransomware authors have to make many choices when they write their malware. Like most criminals, their primary incentive is to maximize their financial gain. Don't forget, no matter how sophisticated the attack, money doesn't come from the computer, it must come from the victim. The best way to maximize profits is by making the right decisions about what user market to target, what computer system to attack, and how to infect that computer. Like many industries cybercriminals are in competition with one another, and as such they observe each other succeeding or failing they learn from one another and an ecosystem forms that practices Darwinian evolution. Over time this has led to impressive technological innovation by cyber criminals. In this section I'll investigate the decisions ransomware attackers must make, and identify overarching trends in the attacker ecosystem.

A. Users Targeted

Ransomware authors must decide what type of users to attack, essentially who they'd like to extort. As mentioned before, ransomware attacks are fundamentally financially motivated, so choosing which users to target is at its core an economic decision. Originally, attackers did not write their ransomware with a particular type of user in mind, choosing instead to cast a wide net with their attacks [7]. This approach works because of the sheer quantity of Internet users; attackers are collecting relatively small ransoms from many victims. A single ransomware virus could be distributed to millions of users worldwide and only a small fraction of users would need to pay the ransom to make the whole scheme profitable. More recently however, ransomware attackers' preferences seem to have shifted to favor collecting relatively large ransoms from fewer victims. Rather than targeting individuals ransomware authors are now focused more on targeting organizations [9, 18].

For the majority of ransomware's history home users have been victimized by attacks more than organizations. According to Symantec's 2015 whitepaper, ransomware is particularly effective against home users for three key reasons. First, because they're an individual rather than an organization they have the least amount of access to technical assistance. Second, they are the least likely to be fluent with their technology. And third, they are the least likely to be familiar with ransomware. Considering those three key reasons, it's easy to imagine how home user victims can feel helpless, scared, and overwhelmed when they discover they've been attacked. Ransomware attackers know that those emotions improve their odds of collecting a ransom, and as such, manipulate those emotions in a practice known as social engineering [7]. Home users have sentimental attachment to the data being held for ransom because personally important files, information, and documents are at stake. A low ransom may be a small price to pay to regain access to wedding photos, a video game save file, a nearly completed thesis paper, or your medical

records. Stop and think, is there anything on your home system that you couldn't live without?

Nowadays, ransomware attackers mostly target organizations, defined as private businesses and public agencies such as educational institutes, medical institutes, law enforcement entities, etc.. Unlike an individual home user, organizations have access to far greater resources. Those resources enable organizations to hire cyber security professionals that can help implement effective defenses against ransomware attacks and respond to an ongoing attack. Organizations can also purchase ransomware insurance to mitigate the financial risk of a ransomware attack. In fact, 84% of organizations surveyed in a 2020 study had cybersecurity insurance, and 80% of those policies cover ransomware [24]. However, data can still be stolen from the company records and extorted by threatening to release it to the public, which insurance doesn't help with. It may seem like organizations are safe from attacks because of the resources at their disposal, however many businesses rely on their digital systems to perform their service, so a ransomware attack that interrupts their services can put them out of business [7, 25]. In this way a ransomware attack can be fatal for a company in a way it isn't for an individual.

Since roughly 2015 there has been an apparent shift in ransomware attacker's approach. Rather than targeting home users, ransomware authors have transitioned away from residential attacks and are focusing on business and agency attacks [18]. Interestingly, despite what news headlines would lead us to believe, the private sector is attacked more frequently than the public sector; generally, private organizations have no obligation to publicly report attacks and are actually incentivized not to report them. In 2019 alone 45% of public sector organizations reported being attacked by ransomware, less than the global average for any organization type at 51%, and less than the most frequently attacked industry (entertainment) at 60% [24]. Cybersecurity experts believe this trend exists because ransomware attacks are able to extort higher ransoms from a business than they could an individual [9]. According to a 2020 study analyzing business insurance claims, the cost of business interruptions in the form of lost revenue and repair costs often outweigh the ransom being demanded [25]. In our increasingly digitized economy a successful cyber attack can slow or halt all business operations, increasing the pressure felt by a ransomware victim to pay up.

This shift is good news for the average home Internet user but bad news for businesses and agencies. Continuing in this trajectory, in the future you'll be less likely to have your wedding photos ransomed on your home computer, but more likely to have your workplace compromised. This trend emphasizes the importance of cybersecurity training in the workplace, now and in the future, since that's where we see a disproportionately high amount of attacks.

B. Systems Targeted

Ransomware authors must decide what type of computer to infect. Infection is their means of seizing something valuable from the victim, so they want to choose their target strategically. In general, cybercriminals are faced with four main systems: personal computers, mobile devices, servers, and Internet of Things devices [7]. The nature of most ransomware attacks requires that they can access cryptography tools already in the computer's operating system (OS), so they need to be OS specific. Originally, ransomware was only designed to target personal computers, particularly Windows machines. But once mobile devices had been widely adopted by the public that opened the door for ransomware authors to expand their list of targeted systems. In recent years there's been a dramatic shift towards mobile devices like cell phones and tablets, and Internet of Things devices such as security cameras and smart thermostats. Lastly, cloud computing has been consistently replacing on-premise servers and server attacks have followed suit, now targeting public cloud computing services.

Personal computers, particularly those running a Windows OS, have historically been the most heavily targeted system. The reason Windows was so heavily targeted is because Windows computers represent the vast majority of computers in use globally [7]. It made sense for criminals to target Windows at that time because most victims were accessible via Windows, and this was in a time when home users were still being targeted most heavily. When going after an organization attackers also tend to target servers, which often contain valuable data or host important web services. Attackers target servers because they're usually business critical, and organizations risk serious losses if they can't use their servers as detailed in the Users Targeted section. Ransomware attackers were targeting all technologies that were viable to attack in the early days of digitalization, victimizing people and organizations from all angles.

With the invention of smartphones came a new avenue of revenue for ransomware attackers. As smartphones and other mobile devices were widely adopted an increasing percentage of people owned personal computers, only these ones fit in your pocket. Mobile devices from smart watches to phones to tablets became the second most targeted system because of their ubiquity [7]. Ransomware authors pivoted to capitalize on the growing market and unsurprisingly this became a reliable method of targeting individual users.

Mobile devices tend to come in two OSs, either iOS or Android [7]. iOS for Apple devices are pretty safe because Apple has strict rules for app developers and consumers. Dissimilarly, Android is very open source and customizable, making them the primary target for mobile attacks. Also, Android has a larger share of the global market, roughly three quarters of phones use Android, so it makes sense from the perspective of attackers to go after the most victims possible [26]. Evidently, ransomware authors target their attacks wherever they see numerous ransoms to be paid, and therefore profit to be made.

It's been more than a decade since the initial release of the smartphone, and in that time other technologies collectively referred to as Internet of Things (IoT) have emerged and risen to global popularity. IoT devices are electronics that use an Internet connection to transfer data and receive software updates. In 2018 these devices numbered between 18 billion and 35 billion, a significant growth from the estimated 2 billion devices in 2010 [27]. While smartphones are technically IoT devices, there's been a trend towards expanding beyond mobile devices to other IoT devices. One particularly startling cyberattack of this nature, which was carried out by researchers rather than cybercriminals, targeted a Jeep Grand Cherokee. The researchers were able to remotely take control of the vehicle over the Internet, controlling the steering, brakes, radio, air conditioning, essentially everything, leaving the driver powerless [28]. If it's possible for researchers it's possible for cybercriminals, and it's not hard to imagine how a cybercriminal could extort any ransom they please when they can steer you into oncoming traffic. A more recent but equally memorable example, this time perpetrated by genuine cybercriminals, involved extracting a casino's customer database through an unsecured fish tank thermometer [29]. While no ransom was demanded, this attack clearly demonstrates cybercriminals' ability to innovate and find security weaknesses in new technologies.

The trend of innovative extortion continues to this day, as evidenced by the growing presence of public cloud attacks. In the early years of ransomware servers physically existed at the same location as the organization's buildings -- these are known as on-premise servers -- so ransomware attacks targeted on-premise servers. Now however, many organizations have pivoted away from on-premise servers and are opting instead to use a public cloud to store their data, such as Amazon Web Services or Microsoft Azure. According to a 2020 survey of 5,000 information technology (IT) managers across a variety of organizations 59% of cryptoransomware attacks included encrypting data in the public cloud [24]. If that weren't enough, cloud security threats have heightened dramatically with the coronavirus pandemic pushing so many employees to work remotely, forcing the suspension of IT security standards at short notice [25]. A survey conducted after the onset of the pandemic of 250 Chief Information Security Officers at large companies listed cloud usage in the top three threats during the work from home period [25]. Cybercriminals are undeniably opportunistic, and will exploit changes in technology and technology usage to their advantage.

Systems targeted by ransomware started simple but have been expanding to keep up with technological innovation and user behavior, trending most recently towards Internet of Things devices and public cloud services. This demonstrates cybercriminals' willingness to branch out and try new targets. As new technologies continually emerge and are widely adopted, new attack surfaces repeatedly present themselves and cybercriminals are always going to pursue those possibilities. It's up to ransomware defenders to prevent those possibilities from coming to fruition and victimizing individuals and organizations.

C. Infection Method

Once a ransomware author has created their virus it must be distributed to computer systems to create victims and generate revenue. Cybercriminals have many choices when deciding how to infect victims, but traditional choices have taken advantage of human error, or at least human interaction. Techniques are constantly evolving though, and recent developments have circumvented the need for human error. Ransomware infection vectors are trending towards more automated and efficient distribution.

Historically, ransomware authors have relied upon their victims taking action to infect systems. This variety of infection generally takes the form of a malicious email attachment, a malicious website that performs an unsolicited download, or malicious advertisements on an otherwise trustworthy website. Ransomware authors prefer these methods because in most cases it's much easier to trick a user into downloading a file or visiting a website than it is to bypass the user and trick the computer.

The most popular infection method over the last fifteen years has been malicious emails disguised as harmless emails that aim to deceive the recipient into downloading an attachment or clicking a link [6]. Oftentimes the attachment will be the ransomware binary, so once it's downloaded it begins executing and encrypting files. In the case of a malicious link the most likely scenario is that it leads to a malicious website that performs an unsolicited download (known as a "drive-by download"). You've probably been warned about these emails before, they're commonly referred to as phishing emails. According to a 2020 survey of 5,000 IT managers across a variety of organizations 45% of ransomware attacks originated from phishing emails [24]. When cybercriminals send out millions of these emails it's referred to as malspam. Malspam is effective because cybercriminals can get very creative with their emails, using a variety of psychological tactics to convince the recipient to click, such as time sensitive offers. Cybercriminals are targeting the weakest link in security systems -- humans -- when they're engaging in phishing malspam, so the only effective mitigation is user education.

Besides fooling the user with phishing email, cybercriminals have used two main methods to download their binaries onto victims' systems. First, cybercriminals create malicious websites for the sole purpose of performing drive-by downloads. All the user has to do is visit the site for their device to become infected, so attackers redirect traffic to their site. Cybercriminals use exploit kits, ransomware tools packaged together for ease, to redirect users from a legitimate website to a malicious website [9]. In this scenario a user could click a link from a search results page or a phishing email and, through no fault of their own, end up on a malicious website. This technique

requires human action, but not human error, and as such are difficult to mitigate with user education alone. Second, cybercriminals can compromise a trustworthy website by inserting malicious code into advertisements they take out [9]. These advertisements may redirect users that click on the ad to a malicious website, or they may perform a drive-by download without the need for users to even click the ad. This technique is especially effective because cybercriminals can compromise websites with heavy traffic, such as Spotify or The New York Times [30].

Recently however, ransomware authors have been coming up with techniques that eliminate the need for victim action. Older techniques still get plenty of use because they're undeniably effective, but ransomware innovation is headed in the direction of automation. Newer ransomware samples such as WannaCry can automatically self-replicate over the internet network by taking advantage of a Windows OS security flaw, therefore any device connected to the same internet as the infected device is immediately at risk. Admittedly, this technique still relies on user action to initiate, but once that has happened further propagation is user-free. This represents an all new threat level because once one device becomes infected then any data on the network is in peril, gone are the days of one action leading to one infection.

Another growing trend in the ransomware distribution space is the adoption of the Ransomware as a Service (RaaS) affiliate profit sharing scheme. RaaS is a criminal business model where one party creates the ransomware and hires other parties to distribute the ransomware [9]. This model has two main benefits. First, the risk of being caught is shared between the two parties [7]. Ransomware authors insulate themselves from the risks of distribution by interfacing with victims through their affiliates [31]. Affiliates are presumably willing to assume this risk because they get a share of the ransom without writing any ransomware. Second, division of labor allows cybercriminals to specialize and focus on what they do best, whether that be programming or distribution [7]. Many ametuer cybercriminals lack the skills and resources necessary to write code that can outsmart modern cybersecurity defenses, but they are capable of malspam and drive-by downloads [7]. Exploit kits can be purchased for a nominal fee, or even found for free, on the Dark Web and that's all someone needs to begin participating in the cybercriminal ecosystem [9]. RaaS lowers the barrier of entry for cybercriminals, expanding the reach that authors can have [7]. Ransomware is trending towards organized crime, ransomware defenders and law enforcement must incorporate this knowledge into their respective approaches.

D. Attack Conclusion

Ransomware attacks are a growing threat, there's no denying that attackers are continuing to innovate. Attackers have set their sights on organizational cash cows while at the same time finding new ways to victimize individuals. Tried and true methods of infection such as phishing malspam and website redirects are being made easier by the availability of exploit kits and RaaS partnerships. Alongside those methods, newer more efficient ransomware variants that spread like a virus without user interaction are being added to attackers' arsenal. As it stands now, there's a strong financial incentive for attackers to develop new techniques to maximize their revenue from exploiting users, and that's led to serious innovation.

Modern ransomware has been in its heyday since its birth in 2006. It came into a world that was totally unprepared to defend against it and in many ways it still enjoys the element of surprise. Cybercriminals inherently have a head start because when they develop new and creative attack methods it takes time for cybersecurity defenders to engineer and implement defenses. To make matters worse, the attack surface for ransomware authors is rapidly expanding as the world becomes more digitized and interconnected, particularly threatening IoT devices. Meanwhile, cybercriminals are utilizing business models to specialize their labor, allowing for faster development by increasingly powerful authors, and more menacing distribution from a wave of ametuer cybercriminals. For these reasons ransomware isn't going away immediately.

VI. Defense Overview

After reading all about the innovations of attack, ransomware defense is understandably not an easy task, but significant money and energy is being invested in putting an end to ransomware. Academic researchers, government agencies, and private cybersecurity firms all want to help. Even though ransomware attacks are criminal, law enforcement agencies have not historically been equipped to deal with this new kind of crime, in fact they get ransomed too. International attacks don't really fall under any country's legal jurisdiction, so a lot of the responsibility has fallen to researchers trying to keep up with cybercriminals in real time. Ultimately, up to now the burden of stemming the flow of ransomware attacks has fallen to cybersecurity experts.

So how do researchers go about such a monolithic task? Researchers study how ransomware operates then create models from which they devise countermeasures. Ransomware is an underground black market, therefore reputable information is hard to come by. Defending against an unknown threat is near impossible because defenders are working from incomplete information. The more complete cyber security experts' understanding of ransomware attacks, the better equipped they are to thwart those attacks [6]. Once models are created to describe how ransomware attacks work, then researchers can begin to counter those attacks. Without the models they wouldn't know where to start. Essentially, researchers have to witness ransomware attacks to learn how to react to them.

Thankfully, academic researchers and professional experts have been working together to construct generic

models of ransomware attack methods. One such model, created by American not-for-profit, government funded cybersecurity research corporation MITRE, exists to

> "create a comprehensive list of known adversary tactics and techniques used during a cyberattack. Open to government, education, and commercial organizations, it should be able to collect a wide, and hopefully exhaustive, range of attack stages and sequences. MITRE ATT&CK is intended to create a standard taxonomy to make communications between organizations more specific."

Breakthroughs in defenders' understanding of attack techniques have made leaps and bounds in recent years, proving the hypothesis that progress can be made when adequate resources are allocated. For example, in 2019 David Lu, a security researcher and PSU professor, authored a corporate blog post arguing that MITRE ATT&CK is "tremendously valuable [...] to better communicate, collaborate, account for, and reason about the domain in a scientific manner", but at the time the model is inadequately organized and in need of structural improvements [32]. In 2020 MITRE ATT&CK introduced sub-categories to resolve the issues present in the previous iteration of the model. Just one year after Lu's call to action he posted another article praising MITRE for their improvements, stating that the newer model is more usable and provides finer detail [33]. This is a clear example of the collaborative ransomware defense ecosystem rising to the challenge of working to enable iterative improvements quickly. As attack models are fine tuned and updated, ransomware defense trends towards increased security.

Thankfully MITRE is just one of many groups pushing for accurate ransomware models. Efforts from academic researchers have resulted in the creation of Randep, a model of the Windows API functions called by ransomware samples, useful for classifying and predicting ransomware behavior [6]. Private entities have also found success when partnering with academic researchers. A 2018 paper by Google and Chainalysis partnered with University of California San Diego, New York University, and Princeton University, performed the difficult work of tracking ransom payments through the once-anonymous Bitcoin blockchain to construct a model of the ransomware attacker ecosystem [5]. These groups of talented, driven, and bright individuals along with many other groups like them, are working to establish consistent methodologies so our understanding of ransomware attack, and therefore capability to implement ransomware defense, is trending upwards.

Once an understanding of ransomware attacks is established then security experts can begin implementing defenses. Most often this comes in the form of a downloadable tool for your computer, but also includes user education, online resources for victims, and law enforcement response. There are three general approaches to ransomware defense taken by cybersecurity experts. Recovery, meaning the victim is able to fully recover from an attack without paying the ransom. Detection, meaning the attack is detected as it's happening and defended against. Lastly prevention, meaning the attack is proactively mitigated before any damage can be done to the victim's system. In this section I will investigate how ransomware defense has changed over time to inform predictions about ransomware defense in the future.

A. Recovery

Recovery is the most passive defense approach to ransomware defense, based on the idea that the victim is able to regain access to their stolen valuables without paying the ransom. Historically, the cybersecurity community has been willing to invest ample time and energy into ransomware detection and prevention, but less attention is given to methods to recover the stolen files after infection [34]. A variety of techniques exist to help victims recover from successful attacks, ranging from decryption to key escrow systems to simple backups.

Backups offer a straightforward and effective solution to the ransomware threat by providing a recovery point for a victim's system, therefore files can be retrieved without paying a ransom. Although no silver bullet exists that can defeat all forms of ransomware, backups are the closest thing users can get. Keeping a separate copy of the data being ransomed effectively removes all bargaining power from the attacker. Additionally, users that regularly backup their data enjoy peace of mind because they have little reason to fear an attack. Unfortunately, despite the widespread availability of backup technology, many home users haven't implemented an effective backup strategy to successfully recover from a ransomware attack. According to a 2015 survey 25% of home users had never backed up files at home, while 55% backed up some but not all of their files at home. This unsettling statistic indicates that the majority of home users are exposed, to some degree, to ransomware attacks. Additionally, only 25% of home users backed up files at least once a week, meaning that 75% of home users would lose more than a week's worth of files in the event of a ransomware attack [7]. The lack of backups can likely be attributed to a lack of user awareness and education. Therefore, increasing users' understanding of the importance of backups, which ultimately leads to a change in user behavior, represents a trend towards greater recovery rates. Alternatively, decreasing the knowledge or effort required of users to create reliable backups has the same desirable result.

In the early days of ransomware attackers used symmetric encryption, the more basic type of encryption that requires the same key to encrypt and decrypt data [35]. Symmetric encryption is quick to implement but is inherently simple to reverse, so it didn't take long for cybersecurity experts to reverse engineer the malware and provide decryption tools [7]. The first generation of crypto

ransomwares were easily thwarted because cybercriminals' techniques were outmatched by those of cybersecurity experts. However, as Yung and Young had predicted, ransomware techniques improved to leverage asymmetric encryption, the more complex type of encryption that uses two different keys to encrypt and decrypt data. This development hampered researchers' decryption efforts dramatically, but decryption tools were still being published. Oftentimes, once a cybersecurity expert discovers a method of decrypting files damaged by a particular sample of ransomware they'll publish the method online for victims to use.

Utilizing asymmetric encryption made file recovery much more difficult, but researchers have identified a method for recovery from ransomware infections on Windows systems. This method relies on a common weakness in ransomware implementation and the capability of Windows to create shadow copies. Shadow copies are backup copies of the user's system that are saved at regular intervals so in the event of a system failure you can restore the system to a recovery checkpoint [7]. Unfortunately for victims, later generation ransomware samples are advanced enough to delete shadow copies during their attacks, leaving no restoration points with which to recover. Fortunately for victims, according to a 2016 study users can prevent the four most common crypto-ransomwares from deleting their shadow copies by renaming the system tool that handles shadow copies [34]. The researchers used this finding to produce a script that automatically renames the appropriate tool. Once a user has run the script their computer is effectively capable of recovering from a ransomware attack via restoration to a state prior to encryption [34]. A technique that was once a cybercriminal innovation has since been entirely mitigated by researchers in a way that reduces the knowledge demanded of users, further evidence of a trend towards more ransomware recoveries.

Another recovery method is a key escrow system that involves storing recent encryption keys in a secure vault to be used for decryption. In the event of a successful ransomware attack the user's key vault captures the encryption key, making file recovery via decryption a trivial task. One such tool called PayBreak was published in 2017 by a team of researchers in collaboration with MITRE. PayBreak continually monitors the integrity of files on the user's computer, keeping an eye out for telltale ransomware behavior. Since most ransomware attacks rely on cryptography tools in the computer's operating system, PayBreak can reference attack models to know which function calls are suspicious, then store encryption keys as encryption occurs [35]. PayBreak was tested with 107 ransomware samples spanning twelve ransomware families, including two of the most financially devastating families of 2016, and demonstrated 100% file recovery for each attack, effectively defeating the threat of cryptographic ransomware [35]. Although ransomware attackers could change their techniques to evade PayBreak, for example writing their own cryptographic functions rather than using what's available, this tool significantly increases the effort required to pull off an unrecoverable attack. PayBreak eliminates the threat from a huge group of ransomware samples and in doing so forces attackers to employ new and challenging techniques that most have avoided. Best of all, PayBreak's source code was published in 2017 and the tool is freely available to the public [35].

Ransomware recovery methods are steadily improving as defenders develop a stronger understanding of their adversary. System and file backups offer the simplest solution, but a disappointing proportion of Internet users neglect to take this step. In response security experts raise awareness of their importance and computer manufacturers implement automatic backups. When ransomware attackers began targeting the shadow copies researchers found a way to counteract that, simplified the setup, and released it to the public. Alongside that specific remedy, defenders created a more robust defense that covers a wide variety of ransomware variants and isn't easily overcome. This tool, PayBreak, was released to the public free of charge too. Recovery may be a last resort in the domain of ransomware defense, but its ability to help victimized users and keep money out of cybercriminals' pockets is profound. As the proportion of infections that result in recovery rather than ransom increases, the battle against ransomware swings in the direction of defense.

B. Detection

Detection is the oldest approach to ransomware defense, founded on the idea of observing and halting an attack as it happens, greatly reducing the need for recovery efforts. Researchers have established two main methods of attack detection; analyzing the behavior of the computer system to identify anomalies, and luring the ransomware into attacking a decoy file. Both techniques require an accurate and detailed model of ransomware attack techniques to work properly. Behavioral analysis requires an understanding of ransomware encryption patterns to recognize the attack quickly, and decoy files work best with an understanding of how ransomware prioritizes which files it targets. With improvements in attack modeling come improvements in detection techniques as defenders have more information at their disposal. This causal relationship is best illustrated by the newfound capability of detection tools to identify unfamiliar ransomware samples [36]. Additionally, detection's upward trend is evidenced by the decreasing time between infection and detection, and the existence of mitigation strategies for ransomware that's yet to exist [18, 37].

Decoy files are one of the simplest techniques for detecting ransomware attacks. They operate by lying in wait alongside the user's other files and raising a red alarm when they're disturbed, similar to a landmine [18]. Because these files are not intended to be accessed by the user any file activity is assumed to be a ransomware attack. The effectiveness of decoy files as a deception-based detection

technique is reliant on the ransomware's willingness to encrypt a decoy file. As such, researchers study methods to minimize the damage an attack renders to a system before being halted.

In 2017 a team of researchers reverse engineered eleven distinct ransomware samples to understand how they traverse a victim's file system and found that every sample sorted files alphabetically [37]. Based on their research of existing ransomware they developed a defense technique, and even went one step further by developing defense techniques based on their predictions of alternative ordering methods future ransomware authors may use to evade deception-based defenses. To defeat current, decoy-blind ransomware they propose naming decoy files such that they are encrypted first when sorting alphabetically. To defeat future ransomware, which may order files by file size or access time, they propose methods of prioritizing decoy files based on file size and access time. To defeat future ransomware that orders files randomly they propose utilizing a greater quantity of decoy files which statistically results in faster attack detection. Not only did this research team identify methods to mitigate known threats, they also thought several steps ahead in the battle against ransomware authors.

In a 2020 PhD dissertation author Genc takes a hard look at existing deception-based anti-ransomware systems and identifies multiple weaknesses that could be exploited by current decoy-blind and future decoy-aware ransomware. Interestingly, the existence of such decoy-aware ransomware is purely speculative, therefore Genc is identifying a weakness in current defenses and predicting how attackers may take advantage of that. Based on an in-depth literature review of deception-based defense tools, Genc provides advice on which decoy techniques to abandon because they're too easily evaded, and best practices on how to improve current techniques for greater effectiveness against decoy-aware ransomware.

Consider that deception-based detection techniques were first published in 2016, and by 2017 researchers were optimizing their techniques for decoy-blind ransomware, then by 2020 there were strategies that would mitigate attacks from decoy-aware ransomware. Every step of the way, defenders are staying a few steps ahead, working from an understanding of how future ransomware samples will likely operate to mitigate ransomware authors' inherent head start.

Behavioral analysis is another technique for detecting ransomware attacks, this one based on continuously observing system behavior and watching for telltale signs of ransomware. Because ransomware usually tries to encrypt many files quickly, detection tools can identify that an attack has begun when certain aspects of the victim's system become significantly more active [18]. In fact, in 2018 the median time required for ransomware to encrypt an entire file system was only 7.8 minutes [5]. The system behavior observed may include frequency of file system access, frequency of encryption, network connections, and which OS functions are being called, all metrics that will be characteristically affected by active ransomware [9]. When a process begins acting suspicious an automated security tool can terminate it immediately, preventing further damage [18].

Behavioral analysis was the first researched detection technique, pioneered in 2015 by Kharraz et al, and as such has served as a foundational technique of ransomware detection. Kharraz et al. closely studied how existing ransomware manipulates the victim's file system and discovered that the system's input and output requests could be monitored to successfully detect an ongoing attack [19]. This discovery represented a major leap forward in defense capabilities and researchers have been fine tuning the technique ever since.

Later that year HelDroid was published, a security tool that detects ransomware attacks on Android mobile phones [36]. Rather than monitoring the file system for anomalous behavior, HelDroid detects apps that are secretly attempting to lock or encrypt the device [36]. Along with a robust mobile device security tool capable of detecting unknown ransomware samples with nearly zero false-positives, the study also contained common characteristics of mobile ransomware [36].

Another such tool is the Pre-Encryption Detection Algorithm (PEDA) developed by Kok et al. and published in 2020. PEDA builds upon previous detection and prevention research to leverage a two layer detection system capable of identifying known and unknown ransomware [9]. The behavioral analysis layer works using a machine learning model trained on the OS function calls made by the potential ransomware sample. All system calls are recorded until a call to an encryption function is made, at which point the list of extracted calls is fed into the machine learning model to produce the prediction [9]. In order to collect the system calls made without jeopardizing the user's system, PEDA executes the ransomware sample in a secure virtual environment known as a sandbox. To accommodate this paradigm users must manually submit a file to PEDA for ransomware analysis. PEDA is a particularly advanced detection tool capable of detecting ransomware without requiring damage to the user's files, but its general effectiveness is limited by the high computing cost of running a sandbox. PEDA boasts a 10-fold cross-validation recall score of 99.9% proving to be a robust detection system, but more importantly the study identified three system calls used by most ransomware [9]. These three system calls have certainly been incorporated into ransomware models and will continue to inform defense tool developers for years to come.

Ransomware attack detection is undeniably improving. Not only can security tools detect attacks faster than ever before, they can even recognize attacks from never-before-seen ransomware samples [36]. In special cases security tools can even detect ransomware without risking system damage [9]. However, detection as a defense paradigm is inherently reactive, which is not ideal because

the victim must incur some system damage. Attack detection is certainly helpful for minimizing losses and it's better than relying solely on recovery, but it still requires that the ransomware infects the user's system before defenses are enacted. Detection tools essentially limit damage, and they've been allowing less and less damage, but can security tools entirely prevent attacks?

C. Prevention

Prevention is the newest approach to ransomware defense, predicated on the goal of defeating ransomware before it can even attack. There are many approaches to ransomware prevention, ranging from technical prevention to widespread user education to international law enforcement. Cybersecurity researchers would love to be able to prevent system damage aso they have found ways to prevent infection and prevent encryption. Internet users would love to be able to have peace of mind and not pay ransoms therefore user education resources are plentiful. Governments would love to minimize the financial burden of criminal activity on their citizens so they have begun targeting cybercriminal organizations and placing hefty sanctions on ransomware strongholds. Recovery and detection are invaluable in the domain of ransomware defense, but prevention is the gold standard. Thankfully the challenge of ransomware prevention is becoming increasingly realistic and feasible.

Despite the successful development of reactive defense tools, security researchers were aware that defense could still be improved, so some set out to create a system that operates proactively. Their solution was binary analysis, a technique in which the contents of the code in a file are searched for cryptographic operations and compared against known ransomware. Recall that the code responsible for ransomware behavior comes in the form of a binary file, hence the name binary analysis.

In the previous section I discussed the detection layer of PEDA, now I'll discuss the prevention layer of PEDA. PEDA implements binary analysis by first hashing the binary, producing a hash signature. In cryptography hashing is a mathematical one-way function that accepts a file and produces a character signature unique to the file contents [9]. The signature is then compared against a repository of known ransomware signatures. A match here indicates the file is a known ransomware, at which point the user is made aware and the file is quarantined [9]. The binary analysis layer executes prior to the detection layer because identifying a known ransomware sample eliminates the need to interpret the system calls, the attack has already been prevented. If the hash isn't recognized, and then the detection layer classifies the file as ransomware, then the signature is added to the repository of known ransomware signatures. This self updating system helps to keep the repository of known ransomware signatures current. Binary analysis is fast and efficient, but lacks the ability to identify unknown ransomwares and therefore cannot prevent their attacks. However, since most ransomware attacks stem from a small number of ransomware families, binary analysis goes a long way towards preventing most attacks. Where once users were completely vulnerable, we now have a technique that can prevent damage from ransomware that's been seen before. This is a massive step in the right direction, but emerging cybercriminal techniques such as obfuscation of the binary may allow attacks to slip by unprevented [18]. To counter this never ending battle researchers continue to anticipate cybercriminal innovations by developing innovations of their own.

Whereas binary analysis prevents a ransomware infection, innovative methods continuously emerge that prevent ransomware encryption. In 2019 a team of researchers developed a novel method that prevents file encryption by randomly and continuously changing file extensions that the ransomware tries to encrypt [31]. The authors refer to this as the Moving Target Defense method and claim it can prevent encryption despite changes in attack techniques because it provides protection at such a fundamental level [31]. When tested against ransomware samples from four families the tool was able to protect important files from 99% of the samples, all while maintaining a small computational footprint, meaning no noticeable performance degradation [31]. The widespread adoption of a tool this robust would put a huge dent in ransomware attackers' profits, and the development of such a tool represents a positive trend in ransomware prevention. Another example of prevention innovation is a tool published in 2020 called NoCry which prevents encryption by controlling which programs have access to OS cryptography functions [18]. Rather than monitoring these function calls and detecting suspicious encryption patterns, NoCry only allows trustworthy programs to use the functions necessary for encrypting files, taking the step from detection to prevention using a similar technique. NoCry was developed from a prior tool in the same paper called UShallNotPass that leveraged the same prevention technique, but when developing NoCry the author made improvements to make the tool more secure, effective, and efficient. Testing NoCry against hundreds of ransomware samples yielded a 97% encryption prevention rate and UShallNotPass even protected the system from NotPetya, a feat no prior defense tool could accomplish [18]. By iteratively improving prevention techniques and coming up with creative approaches the problem of ransomware encryption prevention can effectively be solved.

Luckily for security researchers they're not the only ones interested in defending against ransomware attacks, governments and law enforcement agencies are finally fighting too. For roughly the first decade of contemporary ransomware's existence law enforcement has been disappointingly inactive, but it's not entirely their fault. Most law enforcement agencies operate within a geographic region where they have jurisdiction, but since ransomware attacks happen online and often originate in a different geographic region than where users are victimized, attackers

are beyond the reach of any single jurisdiction [7]. To make matters even more difficult cybercriminals use pseudo-anonymous payment methods and launder ransoms through multiple geographic and legal jurisdictions so tracking the money is difficult [7]. Thankfully, in 2018 a groundbreaking paper was published that deanonymized bitcoin laundering and presented a detailed examination of the ransomware ecosystem from victim bitcoin purchase all the way to attacker cash-out over a two year period [5]. Using a combination of real victims, intentional ransomware infections, ransomware source code, network traffic, and a large Bitcoin address database the research team learned that ransomware operators tend to cash out ransoms at a Russian bitcoin exchange called BTC-e [5]. In fact, 95% of all ransomware payments made between the start of 2014 and the middle of 2017 were converted to a fiat currency through BTC-e [38]. Armed with this knowledge the Northern District of California's Department of Justice investigated and charged the operator of BTC-e, 37 year old Russian national Alexander Vinnik, with one count of operation of an unlicensed money service business, one count of conspiracy to commit money laundering, two counts of engaging in unlawful monetary transactions, and seventeen counts of money laundering [39]. In December of 2020 after multiple extraditions Vinnik was sentenced to five years in a French prison [40]. The paper that exposed Vinnik was the first of its kind, but after seeing the real world impact that a Bitcoin audit can have I expect to see more of this in the future.

Law enforcement efforts have gone beyond targeting individual cybercriminals in recent months, indicating a trend in the government's willingness to prevent ransomware. On April 15th, 2021 President Joe Biden signed an executive order placing economic sanctions on Russia in response to their involvement in the SolarWinds cyber attack [41]. The attack began in December of 2020 and took advantage of a weakness in the IT software SolarWinds to compromise 18,000 customers, nine federal agencies, and 100 private organizations [41]. While this executive order is just a first step it represents a positive trend for three main reasons. First, Biden's administration has made it clear that further cyber attacks are unacceptable and it's prepared to "impose substantial and lasting costs" if cyber attacks continue. Second, this executive order grants the US government additional powers it hasn't had in the past. Third, the North Atlantic Treaty Organization (NATO) has stated its support for the executive order and "stands in solidarity with the United States" [41]. Considering all of these factors it's evident that the US government, as well as governments abroad, are equipping themselves to combat ransomware that originates outside of their jurisdiction. By taking action now governments are preventing future ransomware attacks.

With the authority and resources of governmental bodies ransomware defense capabilities leap forward, but ll, there is still no substitution for effective user education as a prevention method. Along with endpoint security, cybersecurity experts cite user education as the most important method of fighting ransomware [6]. Awareness, behavior, and culture are considered the pillars of cybersecurity and experts can strengthen these pillars by disseminating their knowledge through training [23]. As discussed earlier, phishing emails are one of the most popular and effective attack vectors because they target the weak link in the security chain, the human user [42]. Information Security Awareness Training (ISAT) can help employees protect their organizations by not falling victim to social engineering attacks such as phishing emails. Implementing an effective ISAT program is not an easy task, but there are extensive resources for ISAT at organizations' disposal; successful programs tend to conduct routine training year-round and identify the specific needs of the organization [42]. Once an organization tries a few approaches and figures out what works best for them the program can mature allowing the organization to benefit from an immense return on investment as their overall security improves. A review of security literature has shown significant organizational security improvements due to behavior changes from ISAT programs [42]. Moving forward, organizations are likely to invest in ISAT programs because it is financially sensible, and that increasing demand for effective ISAT will foster a strong security industry and mature the overall defense ecosystem.

Ransomware awareness can still be improved without the need for costly ISAT programs though. The cybersecurity community has agreed on best practices for organizations and individual users. Many of the organizational practices require information security administration and pertain to large interconnected systems, but individual best practices are attainable for most Internet users. From a review of the literature these are seven security practices that you can implement to prevent becoming a victim of a ransomware attack [7, 43, 44]:

- Regularly back up data offline and check on it. Backups may be the best recovery method
- Since users are targeted focus on awareness of ransomware and training on information security principles and techniques
- Update the operating system, software, and firmware, especially when vulnerabilities are discovered
- Install anti-virus and anti-malware tools. Make sure they scan regularly and update automatically
- Try not to open or reply to spam emails. Do not click on links or open attachments unless you can verify the sender
- Exercise caution when using a public Wi-Fi network. Use network protection such as a Virtual Private Network (VPN)
- Disable network file sharing and deactivate unused wireless connection ports such as Bluetooth or infrared

D. Defense Conclusion

Ransomware defense effectiveness is trending upwards across all three defense paradigms as increasing attention and resources are devoted to them. For roughly fifteen years security researchers had no choice but to react to attacks and analyze their methods. But within the last few years detailed, comprehensive models have finally become available allowing security experts to work proactively and improve reactive methods. Defenders wouldn't have been able to understand their adversary without behavioral analysis laying the groundwork for developing attack models with far reaching benefits, such as the effectiveness of key escrow systems. Decoy file defenses are also getting better at detecting attacks with minimal damage, and research in this area has even outpaced real-world ransomware threats. Still, file backups are perhaps the most effective way to thwart ransomware, and attackers have few options for countering this simple defense method.

Proactive defense is where efforts are primarily focused now, and the methods emerging from this approach are the key to turning the tides in the ransomware battle. Binary analysis tools have the ability to prevent known ransomware threats with no risk to the user's system, and new tools using novel methods can even outperform that. NoCry controls access to the system's encryption functions to defeat unknown ransomware threats and the Moving Target Defense methods continuously changes file extensions to achieve the same outcome. New and innovative security tools such as these are published every year that build upon recent research, meaning that defense progress is accelerating. For example, PEDA combines two defense techniques to create a multilayered, self-updating security tool. What will next year's cybersecurity journals bring?

Aside from technical solutions to prevent ransomware the cybersecurity community has learned how to map and expose the cybercriminal black market, allowing the US government to step in and perform its newfound anti-ransomware duties. Ever improving ISAT programs are enabling stronger protection for organizations and will continue to mature as more organizational customers adopt this preventative measure. In the neverending battle against ransomware best practices and defense tools are the shield, and law enforcement is the sword.

VII. Conclusion

Ransomware will probably never disappear entirely, but with dedicated defense efforts it can be mitigated until it hardly remains. Over time attackers have shifted which users they target, which systems they target, and how they infect victims. New and creative attack methods will always be emerging, but defenders are getting better at understanding and mitigating their threat. Every approach to ransomware defense, recovery, detection, and especially prevention, has seen promising development in recent years. Defenders will continue to refine attack models and implement tools based on that understanding, until eventually attacking is no longer worth the risk or cost, and then ransomware's threat will be diminished.

Realistically, the threat of ransomware may need to get worse before it can get better. Whenever attackers successfully collect a ransom payment they're also sowing the seeds of their own demise because they're incentivizing stronger defenses. Even money lost from damage to infected computer systems, that ransomware attackers never receive, is mounting motivation for Internet users to invest the resources necessary in ransomware defense. Every dollar of damage that ransomware attackers inflict increases the target on their back.

In response to the demand for ransomware defense academic researchers and private cybersecurity firms, alongside massive law enforcement resources, have begun to turn the tide. Preventative methods will enable defenders to overtake attack progress in the future. Surely there will be seen and unforeseen challenges, but as time goes on the collaborative nature of defense research will overpower the competitive nature of attack. Ultimately attack innovations are motivated by profit, therefore ransomware developers are always in anonymous competition with one another. Even collaborative cybercriminal schemes like Ransomware as a Service will soon be dismantled by defender's new ability to track payments. Conversely, defenders accumulate their knowledge and share it because they're united by a common enemy. That's why defense will continue to accelerate until ransomware attacking isn't worth the risk or cost anymore. It's a war of attrition and at that point cybercriminals will move on to the next best profitable crime fad, and then ransomware's threat will be diminished. I don't expect it to disappear entirely, but it will be relegated to niche attacks, only a shell of what the ransomware crime wave once was.

References

[1] K. Collier, “Major hospital system hit with cyberattack, potentially largest in U.S. history,” *NBCNews.com*, 28-Sep-2020. [Online]. Available: https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254. [Accessed: 31-Jan-2021].

[2] B. Winterford, “Ransom payouts spell trouble for insurers,” risky.biz, 01-Dec-2020. [Online]. Available: https://risky.biz/newsletter36/. [Accessed: 31-Jan-2021].

[3] M. A. Mos and M. M. Chowdhury, “The Growing Influence of Ransomware,” *2020 IEEE International Conference on Electro Information Technology (EIT)*, 2020.

[4] S. Morgan, “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021,” Cybercrime Magazine, 21-Oct-2019. [Online]. Available: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. [Accessed: 24-Apr-2021].

[5] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, K. McRoberts, E. Bursztein, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, “Tracking Ransomware End-to-end,” 2018 IEEE Symposium on Security and Privacy, pp. 618–631, 2018.

[6] G. Hull, H. John, and B. Arief, “Ransomware deployment methods and analysis: views from a predictive model and human responses,” Crime Science, vol. 8, no. 1, 2019.

[7] K. Savage, P. Coogan, and H. Lau, *The evolution of ransomware*. Symantec, 2015.

[8] J. Frankenfield, “Bitcoin,” Investopedia, 30-Jan-2021. [Online]. Available: https://www.investopedia.com/terms/b/bitcoin.asp. [Accessed: 28-Jan-2021].

[9] S. Kok, A. Abdullah, and N. Jhanjhi, “Early detection of crypto-ransomware using pre-encryption detection algorithm,” Journal of King Saud University - Computer and Information Sciences, 2020.

[10] Richardson, Ronny and North, Max M., "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276. https://digitalcommons.kennesaw.edu/facpubs/4276

[11] S. Sjouwerman, “Ransomware,” KnowBe4, 2015. [Online]. Available: https://www.knowbe4.com/ransomware#ransomwaretimeline. [Accessed: 31-Jan-2021].

[12] A. L. Young and Moti Yung, "Cryptovirology: extortion-based security threats and countermeasures," Proceedings 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1996, pp. 129-140, doi: 10.1109/SECPRI.1996.502676.

[13] A. L. Young and M. Yung, “An Implementation of Cryptoviral Extortion Using Microsoft’s Crypto API,” *Cryptovirology*, 2005. [Online]. Available: http://www.cryptovirology.com/. [Accessed: 01-Feb-2021].

[14] D. Nazarov and O. Emelyanova, “Blackmailer: the story of Gpcode,” Securelist, 26-Jun-2006. [Online]. Available: https://securelist.com/blackmailer-the-story-of-gpcode/36089/. [Accessed: 25-Jan-2021].

[15] Luo, Robert & Liao, Qinyu. (2007). Awareness Education as the Key to Ransomware Prevention. Information Systems Security. 16. 195-202. 10.1080/10658980701576412.

[16] A. Gazet, “Comparative analysis of various ransomware virii,” Journal in Computer Virology, vol. 6, no. 1, pp. 77–90, Jul. 2008.

[17] M. Ward, “Cryptolocker victims to get files back for free,” BBC News, 06-Aug-2014. [Online]. Available: https://www.bbc.com/news/technology-28661463. [Accessed: 26-Jan-2021].

[18] Z. A. Genç, “Analysis, Detection, and Prevention of Cryptographic Ransomware,” dissertation, University of Luxembourg Library, 2020.

[19] Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. (2015) Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, vol 9148. Springer, Cham. https://doi-org.proxy.lib.pdx.edu/10.1007/978-3-319-20550-2_1

[20] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware,” 25th USENIX Security Symposium, pp. 757–772, Aug. 2016.

[21] S. Sjouwerman, “WannaCry Ransomware Attack Uses NSA 0-Day Exploits To Go On Worldwide Rampage,” KnowBe4, 12-May-2017. [Online]. Available: https://blog.knowbe4.com/ransomware-attack-uses-nsa-0-day-exploits-to-go-on-worldwide-rampage. [Accessed: 27-Jan-2021].

[22] “Changelog,” MITRE ATT&CK®, 23-Mar-2021. [Online]. Available: https://attack.mitre.org/resources/changelog.html. [Accessed: 10-Apr-2021]. Webpage updated periodically.

[23] J. Barker, A. Davis, B. Hallas, and Mahon Ciarán Mc, Cyber security ABCs: delivering awareness, behaviours and culture change. London: BCS, 2020.

[24] “sophos-the-state-of-ransomware-2020-wp.” Sophos, Abingdon, May-2020.

[25] G. Dobie and J. Whitehead, “AGCS-Cyber-Risk-Trends-2020.” Allianz Global Corporate & Specialty SE, Munich, Oct-2020.

[26] “Mobile Operating System Market Share Worldwide,” StatCounter Global Stats. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide. [Accessed: 22-Apr-2021].

[27] S. Strba, "Internet of Things Security: Ongoing Threats and Proposed Solutions" (2018). University Honors Theses. Paper 572. https://doi.org/10.15760/honors.579
[28] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway-With Me in It,” Wired, 21-Jun-2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 24-Apr-2021].
[29] G. Marks, “A Casino Gets Hacked Through a Fish-Tank Thermometer,” Entrepreneur, 01-Jun-2021. [Online]. Available: https://www.entrepreneur.com/article/368943. [Accessed: 22-Apr-2021].
[30] “What is Malvertising: Examples & How It Differs From Ad Malware: Imperva,” Learning Center, 29-Dec-2019. [Online]. Available: https://www.imperva.com/learn/application-security/malvertising/. [Accessed: 22-Apr-2021].
[31] S. Lee, H. K. Kim, and K. Kim, “Ransomware protection using the moving target defense perspective,” Computers & Electrical Engineering, vol. 78, pp. 288–299, Sep. 2019.
[32] D. Lu, “ATT&CK Structure Part I: A Taxonomy of Adversarial Behavior,” The State of Security, 27-Jun-2019. [Online]. Available: https://www.tripwire.com/state-of-security/mitre-framework/attck-structure-taxonomy-adversarial-behavior/. [Accessed: 30-Apr-2021].
[33] D. Lu, “MITRE ATT&CK Framework - July 2020 Update: Sub-Techniques,” The State of Security, 09-Jul-2020. [Online]. Available: https://www.tripwire.com/state-of-security/mitre-framework/mitre-attck-update-sub-techniques-july-2020/. [Accessed: 30-Apr-2021].
[34] M. Wecksten, J. Frick, A. Sjostrom, and E. Jarpe, “A novel method for recovery from Crypto Ransomware infections,” 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1354–1358, 2016.
[35] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “PayBreak,” Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017.
[36] Andronio N., Zanero S., Maggi F. (2015) HelDroid: Dissecting and Detecting Mobile Ransomware. In: Bos H., Monrose F., Blanc G. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2015. Lecture Notes in Computer Science, vol 9404. Springer, Cham. https://doi-org.proxy.lib.pdx.edu/10.1007/978-3-319-26362-5_18
[37] Jeonghwan Lee, Jinwoo Lee, and Jiman Hong. ‘How to Make Efficient Decoy Files for Ransomware Detection?’ In: Proc. of Int. Conf. on Research in Adaptive and Convergent Systems. RACS ’17. Krakow, Poland: ACM, 2017, pp. 208–212
[38] C. Cimpanu, “95% of All Ransomware Payments Were Cashed out via BTC-e Platform,” BleepingComputer, 27-Jul-2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/95-percent-of-all-ransomware-payments-were-cashed-out-via-btc-e-platform/. [Accessed: 09-May-2021].
[39] “Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox,” The United States Department of Justice, 27-Jul-2017. [Online]. Available: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged. [Accessed: 09-May-2021].
[40] C. Cimpanu, “BTC-e founder sentenced to five years in prison for laundering ransomware funds,” ZDNet, 07-Dec-2020. [Online]. Available: https://www.zdnet.com/article/btc-e-founder-sentenced-to-five-years-in-prison-for-laundering-ransomware-funds/. [Accessed: 09-May-2021].
[41] M. Chalfant and M. Miller, “Biden administration sanctions Russia for SolarWinds hack, election interference,” The Hill, 15-Apr-2021. [Online]. Available: https://thehill.com/homenews/administration/548367-biden-administration-unveils-sweeping-sanctions-on-russia. [Accessed: 09-May-2021].
[42] F. Labib, “Qualities of Impactful Cyber Security Awareness Training,” University Honors Theses, May 2019. https://doi.org/10.15760/honors.698
[43] “Internet Crime Complaint Center (IC3): High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations,” Internet Crime Complaint Center (IC3) | High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations. [Online]. Available: https://www.ic3.gov/Media/Y2019/PSA191002. [Accessed: 09-May-2021].
[44] S. Mohurle, M. Patil, “A brief study of Wannacry Threat: Ransomware Attack 2017,” International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017, 1938-1940