GLASSWALL

Ransomware:

Innovative Risk Management as a Disincentive

glasswallsolutions.com

GLASSWALL

"Someone once asked Slick Willie Sutton, the bank robber, why he robbed banks. The question might have uncovered a tale of injustice and lifelong revenge. Maybe a banker foreclosed on the old homestead, maybe a banker's daughter spurned Sutton for another.

"'I rob banks because that's where the money is,' he [allegedly] said…."[1]

I. Introduction

Executive Summary

This white paper largely focuses on ransomware as it has been experienced over the last few years. It explores some high-profile incidents, traces the evolution of ransomware campaigns, and offers a couple of approaches to managing risk considering ransomware's apparent trajectory.

Ransomware is not a new phenomenon, although its rise within mainstream attention reached a crescendo in 2017 with two large-scale campaigns. Based on the security community's experience in 2017, initial forecasts for 2018 and beyond suggested sustained, if not increased, ransomware campaigns. Experience over the first half of the year, however, indicates a more nuanced trajectory. Whereas ransomware attacks historically were large in scale, opportunistic and not generally targeted, recent campaigns have touched fewer victims, but with greater target specificity. Ransomware attacks, now clearly entrenched as one of many options in threat actors' arsenals, remains an event of potentially great consequence for victims.

As just one example, SamSam ransomware has been used recently to target transportation and government infrastructures. Following SamSam attacks on Colorado and the City of Atlanta, it was reported in July 2018 that the U.S. network of shipping giant COSCO suffered a ransomware attack. While SC Magazine reports that "[i]t is unclear what type of ransomware was used in the attack," SamSam is suspected as the most likely cause.[2] "The incident took place on July 24 and the company's American IT infrastructure including email servers, telephone network, and company website" were impacted.[3]

---

1 Robert M. Yoder, "Someday They'll Get Slick Willie Sutton," in The Saturday Evening Post (January 20, 1951), Vol. 223, Issue 30. Citing an alleged statement from Willie Sutton who disavowed ever saying it.

2 Robert Abel, "Ransomware attack knocks out shipping giant COSCO's U.S. network," dated July 26, 2018. Available at: <https://www.scmagazine.com/ransomware-attack-knocks-out-cosco-shipping-giants-american-network/article/783584/>.

3 Id.

Also on July 24, ransomware spread through the network of Alaska's Matanuska-Susitna borough, encrypting the "email server, internal systems and disaster recovery servers."[4] This impacted most of Matanuska-Susitna's desktop computers, 120 servers, telephones and a physical access card system. Although antivirus software "spotted one part of the virus on July 17…[it] failed to detect all the components of the malware."[5] Resourceful employees resorted to using typewriters in order to maintain some level of productivity.

These and other examples highlight a few characteristics of ransomware. First, it can quickly spread across an enterprise or across the globe in either a targeted or opportunistic fashion. Second, as with other malware, antivirus solutions will not always detect a particular strain of ransomware, and even when they do, their ability to eliminate the threat may be incomplete. Third, ransomware is now a commodity tool of cyber threat actors, and the barrier to its use is quite low. Finally, ransomware is generally used to convince a victim to part ways with its money, but not always—a threat actor can just as easily use it as destructive malware with no intention of decrypting impacted files.

Certainly ransomware should be taken seriously, but there is no need to subscribe to the "doom and gloom" narrative that one might spin from recent experience. Well-planned risk management strategies, based on proper assessments of organization assets, threats and vulnerabilities, can be applied in support of organizational business or mission goals. The combination of people, processes and innovative technologies can significantly mitigate the risk of ransomware alongside other forms of malware.

Prologue

Whether Willie Sutton truly offered the rejoinder that he robbed banks because they were the locations with the largest, concentrated amounts of money,[6] the underlying logic repeatedly holds true in ongoing efforts to manage cyber risks. Nation state, terrorist and criminal cyber threat actors are smart, organized, and ruthlessly focus their resources where they are most likely to obtain access to the data, processes, money or other targets in which they are interested. This includes the victims themselves and entities with supply chain connections to those victims. It also includes the use of malware and other exploits tied to the most prevalent operating systems and software applications. A survey of ransomware's evolution and its application by threat actors over the last decade certainly follows Sutton's purported logic – they simply go where the money is.

In the world of cybersecurity, one could not escape 2017 without a deep

---

[4] Rozina Sabur, "Alaska town returns to typewriters after ransomware attack shuts down computer network", dated August 1, 2018. Available at: <https://www.telegraph.co.uk/news/2018/08/01/alaska-town-returns-typewriters-ransomware-attack-shuts-computer/>.

[5] Id.

[6] In his autobiography, Sutton claims that he never offered such an answer.

appreciation of the risks presented by ransomware. In May 2017, WannaCry ransomware spread globally and severely impacted organizations, including the National Health Service in the United Kingdom. Shortly thereafter, the NotPetya malware impacted organizations across over 60 countries, hitting Ukrainian transportation, commercial facilities sectors and the national bank particularly hard. Yet these incidents were just the exclamation point on many years of evolution in ransomware. First observed in 1989, the tactics applied by ransomware have changed over the ensuing decades, but since at least 2004 or so, the end goal of ransomware has been to encourage victims to part ways with their money. However, even recent high-profile ransomware campaigns are not necessarily what they appear to be.

II. 2017: A Window into the Business of Cybercrime

By early 2017, the authors and users of ransomware had matured their tools and tradecraft far beyond their initiatives from a decade earlier. In 2017, ransomware, was a prominent tool in the hands of threat actors. And a year later, among the megatrends identified in a February 2018 Ponemon Institute report was the "risk [that] cyber extortion and data breaches will increase in frequency" over the next three years.[8] This is supported by 67% of respondents who 'strongly agreed' or 'agreed' that the "risk of cyber extortion (such as ransomware) will increase in frequency and payout," with 19% judging such cyber extortion to be very frequent in 2018 and 42% expecting it to be very frequent over the next three years. Verizon's 2018 Data Breach Investigations Report presents a similar forecast, noting that while the 2018 report suggests a decrease in malware and hacking events in 2017, this was largely due to the removal of botnet infections from the data and the fact that the report is based on confirmed data breaches and "it is important to keep in mind that attacks that [Verizon] see[s] on the rise, such as ransomware and some financial pretexting, do not require a breach of confidentiality for the attacker to meet their goal."[9] Of course, these sentiments were the product of respondents' own experiences in 2016 and 2017 as well as the visible consequences of two major events in 2017.

---

[7] Ponemon Institute, Research Report, "2018 Study on Global Megatrends in Cybersecurity", p. 1. Available at: <https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf>. Sponsored by Raytheon.

[8] Id., p. 7.

[9] Verizon, "2018 Data Breach Investigations Report". Available at: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>.

GLASSWALL

2017

Early in the morning on May 12, 2017, U.S. authorities began receiving reports from Asia and Europe of a ransomware campaign, which rapidly spread across 150 countries and led to over a quarter of a million infections. Ultimately, it impacted operations at hospitals, automakers, gas stations, railways and shipping companies. Reports suggest that the ransom amount demanded from each victim fell between $300 and $600 in bitcoin, and the perpetrators ultimately only made just over $140,000 according to most reporting, it could have been in the multiple millions if they were more organized. Clearly, the significance of the WannaCry campaign had little connection with the actual dollar amount obtained by those responsible (other cyber incidents netted far more), and much more to do with the speed and breadth of its global spread as well as the impact it had to business operations among critical infrastructure entities.

The sting of ransomware in 2017 felt even more painful due to the NotPetya campaign, which followed shortly on the heels of WannaCry in late June 2017. The NotPetya malware, so named due to its similarity with previously seen Petya ransomware, used a few technical options to spread laterally within an organization and to quickly spread globally. For example, it included the use of previously known vulnerabilities, for which patches were already available, and so-called "living off the land" techniques whereby the malware uses legitimate system tools to achieve its intent.

More advanced than WannaCry, NotPetya encrypted victims' devices and displayed a screen demanding a ransom. Despite this demand and the temporal proximity between WannaCry and NotPetya, there is an important distinction to make between the two. Whereas WannaCry was a rapidly spreading ransomware campaign that netted relatively little revenue, NotPetya was not quite ransomware. It certainly demanded and offered an opportunity for victims to pay a ransom, but the malware and supporting infrastructure were not designed for the threat actors to associate a payment with a particular victim's device through an installation identifier. As such, perpetrators would be unable to decrypt an affected device upon receipt of payment. In reality, it seems that NotPetya was nothing more than destructive malware—a wiper with the ability to spread fast and wide. In February 2018, the White House released a statement that "[i]n June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed 'NotPetya,' quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas."[10]

//

The attack quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas

[10] Id., p. 7.

While WannaCry and NotPetya may not have shared the ability to decrypt a victim's device, they did share an ability to impact a vast array of victims over a short period of time. They also shared another attribute. Unlike prior, well-known ransomware campaigns, WannaCry and NotPetya were both attributed to nation state actors. Whereas the latter was attributed to the Russian military, the former was attributed to the North Korean government. The breadth of the campaigns, the destructive nature of NotPetya and the attribution to nation states placed these two events on a plane far apart from prior, concurrent or subsequent ransomware campaigns.

Forecasts

Consistent with the Ponemon Institute and Verizon forecasts of increased risks from ransomware going forward are survey results reported by Cybersecurity Insiders, which found that "Ransomware is the fastest growing security threat, perceived as a moderate or extreme threat by 80% of cybersecurity professionals. 75% of organizations affected by ransomware experienced up to five attacks in the last 12 months alone, 25% experienced [six] or more attacks. 79% predict ransomware to become a larger threat over the next 12 months."[11]

And these three forecasts did not stand alone at the end of 2017 and beginning of 2018. In his February 2018 "Statement for the Record" related to the "Worldwide Threat Assessment of the U.S. Intelligence Community", the U.S. Director of National Intelligence observed that "[t]he risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war," and that "[r]ansomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations."[12]

SophosLabs noted four 2017 trends that they expected to continue in 2018, including "a ransomware surge fueled by [ransomware-as-a-service (RaaS)] and amplified by the resurgence of worms."[13] Viewed as a lucrative threat, ransomware authors increased the availability of RaaS on the dark web, which makes it accessible to even those with little technical expertise, while also improving the features of their malware, such as improved encryption and antivirus evasion, broader ransom payment options, and applicability beyond the Windows operating system.[14] At least a dozen other forecasts suggested that the experiences of 2017 were expected to continue in 2018 and beyond.

//

Ransomware is the fastest growing security threat

[11] Verizon, "2018 Data Breach Investigations Report". Available at: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>.
[12] Statement from the Press Secretary, The White House (February 15, 2018). Accessed on July 5, 2018 and available at: <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.
[13] SophosLabs, "2018 Malware Forecast", p. 1.
[14] Id., p. 5.

GLASSWALL

III. Ransomware's Evolution

Despite the news coverage and government response around the events of May and June 2017, ransomware was nothing new at that time. Digital Guardian reports that "[a]fter the first documented ransomware attack in 1989, ransomware attacks remained uncommon until the mid-2000s…. Popular during this time were Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive."[15] Other, more recent and commonly encountered ransomware variants include CryptoWall, Teslacrypt, Cerber, CTB-Locker, Cryakl, Scatter, and Locky, and the "total number of users who encountered ransomware between April 2015 and March 2016 rose by 17.7% compared to the previous 12 months (April 2014 to March 2015) – from 1,967,784 to 2,315,931 users around the world."[16] And a paper by the Heritage Foundation found that "[b]etween 2011 and 2016 the number of ransomware attacks grew steadily, with incremental evolutions in sophistication and scale. That all changed in 2017."[17]

Since mid-2017, ransomware campaigns continued. For example, SamSam ransomware emerged in 2016 and continued to be encountered in 2017 and 2018. In March 2018, the City of Atlanta, Georgia suffered a SamSam ransomware attack, and the State of Colorado previously experienced the same ransomware. In early December 2017, Glasswall Solutions protected one of its customers from a new variant of the GlobeImposter ransomware, which demands $1,037 from its victims and was being distributed via email attachments by the Necurs botnet.[18]

Plenty of information is available about earlier and current iterations of ransomware. Without repeating that information, it is best to consider two aspects along the historical trajectory of this threat—(1) types of extortion and ransomware, and (2) actor targets and motivations.

---

[15] Nate Lord, "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time", dated April 6, 2018. Available at: <https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time>.
[16] Kaspersky Lab, "KSN Report: PC ransomware in 2014-2016," dated June 22, 2016. Available at: <https://securelist.com/pc-ransomware-in-2014-2016/75145/>.
[17] Klon Kitchen and Megan Reiss, "Ransomware is Coming. It'll Make You WannaCry,", dated May 8, 2018. Available at: < https://www.heritage.org/technology/commentary/ransomware-coming-itll-make-you-wannacry>.
[18] Glasswall Solutions FileTrust™ Advanced Threat Protection prevented this ransomware incident on day "T", although the antivirus community did not indicate awareness of the ransomware file's hash until day T+1.

Types of Extortion and Ransomware

Symantec provides an analysis of how online extortion and ransomware evolved between 2005 and 2015.[19] Four general categories of extortion and associated ransomware can be used to trace the history of this online threat. These categories include: misleading applications; fake antivirus; lockers; and crypto ransomware. The first category generally presented an end-user with the appearance of a spyware removal or performance optimizing solution available to the user for a fee. Over time, the presence of fake antivirus increased. This category of extortion presented the end-user with alleged scan results, which appeared to detect significant malware infections. Perpetrators scared their victims into purchasing fake antivirus. As the first two categories began to recede in relative prevalence, the activity of locker ransomware increased.

According to Symantec, "[f]rom 2011 to 2012, attackers transitioned from fake antivirus tools to a more disruptive form of extortion. This time, the cybercriminals disabled access and control of the computer, effectively locking up the computer from use."[20] Although locker ransomware has decreased in its relative prevalence, it has not disappeared. However, network defenders and incident response teams sometimes found ways to defeat lockers, leading ransomware authors to expand into crypto ransomware. With a locker, the targeted device may no longer be accessible, but there remains the potential to recover the files stored on its hard drive. However, crypto ransomware encrypts individual files, rendering recovery difficult if not impossible. Interestingly, this final category that emerged over the last three years had a relatively significant presence in 2005, but fell out of favor during the intervening years.[21]

The trend is fairly obvious. Extortionists generally moved from approaches that relied on using a false threat to scare a victim into parting with its money to approaches that presented very real threats to the availability of a victim's computing resources or data. Intended victims could learn to differentiate false from real threats, thereby rendering misleading applications and fake antivirus less lucrative. Cyber criminals, however, followed the logic attributed to Mr. Sutton and increased their use of lockers and crypto ransomware, which led to sustainable profits.

---

[19] Kevin Savage et al., "Security Response: The evolution of ransomware", dated August 6, 2015, pp. 7-11). Available at: < http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf>.
[20] Id., p. 9.
[21] Id., p. 8.

Victims

The victims of ransomware have largely cut across government and private sector organizations, critical infrastructure sectors, small businesses, and home users. Arguably, small businesses and home users were more susceptible to the early categories of misleading applications and fake antivirus. This has little relationship to the sophistication of a business or user and everything to do with decision-making authority. In a small business or home user setting, the person experiencing the extortion is also more likely to be the person in a position to spend money on the security and maintenance of their information technology resources. In larger organizations, the initial victim is more likely—although not always—to defer to an information technology department for handling the issue and making payment. At that point, information security professionals have the opportunity to intervene, recognizing the false threats for what they are.

With respect to lockers and crypto ransomware, however, the advantage of the larger organization falls away. The threats are real and, absent the execution of pre-existing risk management strategies, the pressure to pay a ransom may be very great.

Again, the shift to ransomware types that open up greater opportunities to extort large public and private sector organizations reflects one of the most predictable attributes of unpredictable threat actors—they and their tools will gravitate towards the victims of greatest value to them. The NotPetya experience, although technically not ransomware, shows that value is not always reducible to clear monetary amounts. Especially among nation states, strategic interests can have much more to do with disruption of infrastructure and institutions within competitor nations.

There is no reason to believe that threat actors will abandon their pursuit of victims they value. However, the continued trajectory of ransomware is not as obvious.

GLASSWALL

IV. The Threat Landscape Isn't So Clear: The Latest Observations

The cybersecurity community entered 2018 with well-defined ransomware capabilities and victims. Ransomware tools had evolved in their ability to spread quickly and cause considerable disruption. A debate around whether or not to pay requested ransom amounts co-existed with the increasingly visible events. Whereas law enforcement generally encouraged victims to not pay the ransom, the final decision belonged to the asset owner. Within this context, security professionals predicted that 2018 would see a growth in ransomware.

Yet, by mid-2018, assessments suggested a more nuanced trajectory. In March 2018, a Recorded Future blog noted that over 2017 and into 2018 there actually had been "a steady decline in ransomware campaigns", that ransomware efforts were becoming much more targeted, focusing on specific industries and using a greater number of variants, and that RaaS "would continue to thrive, at least through 2018."[22] Similarly, in April 2018 it was observed that ransomware "is falling into such a steep decline that some of the major families responsible for taking millions from victims have ceased operation….It is a sharp contrast to how ransomware performed during 2017."[23]

This and similar reporting indicates that while ransomware is not expected to disappear as a concern, it is expected to evolve. Less indiscriminate than the campaigns of 2015 through the high-profile campaigns of 2017, threat actors are using ransomware to focus on specific victims. And while the common ransomware families appear to be dying, the ransomware that remains is being presented to victims through the use of larger malware variants. Finally, access to the malware is widely available through RaaS.

This is perhaps as worrisome as the broad ransomware salvos of the last few years. Now, potential victims are likely to be specifically targeted. SamSam ransomware, for example, is now characterized by threat actors scanning for the presence of specific vulnerabilities that can be exploited to achieve an initial infection as an alternative to using phishing emails. And once inside a victim's network, SamSam threat actors "prep[] the victim for full exploitation."[24] In this emerging era of ransomware, a threat actor will have the discipline and focus to tailor its delivery mechanism, such as spear phishing emails with attached malicious files, to achieve a greater probability of exploiting the victim.

//

Ransomware efforts were becoming much more targeted

22 Allan Liska, "5 Ransomware Trends to Watch in 2018", dated March 6, 2018. Available at: < https://www.recordedfuture.com/ransomware-trends-2018/>.
23 Danny Palmer, "Ransomware: Not dead, but evolving nasty new trick", dated April 9, 2018. Available at: < https://www.zdnet.com/article/ransomware-not-dead-but-evolving-nasty-new-tricks/>.
24 Doug Olenic, "SamSam ransomware payments hit $6 million, malware called labor intensive to operate", dated July 31, 2018. Available at: <https://www.scmagazine.com/samsam-ransomware-payments-hit-6-million-malware-called-labor-intensive-to-operate/article/784454/>.

At the same time, increasing varieties of a particular piece of ransomware have the potential to avoid detection and prevention by signature- and heuristic-based intrusion prevention, next-generation firewall and antivirus solutions.

Yet if recent reporting is correct, then most organizations are unlikely to experience ransomware unless they are targeted. From a risk management perspective, an organization needs to understand where it falls in relation to the early 2018 forecasts and the nuanced trajectory suggested more recently. From an organization's perspective, determining the probability of facing ransomware is important. But RaaS, which lowers the bar for those who want to use this threat, and the threat actor-specific determinations of victim value, which suggest a dynamism around whether one is a target at a particular time, suggest that a given probability determination could quickly become stale.

V. How to Manage Risk as Ransomware Evolves ations

If ransomware is seen for what it now is—just one more commoditized tool to achieve cybercriminal and nation state goals of financial gain, disruption or obfuscation—then associated risk management approaches are relatively straightforward. Ransomware risk management fits well within broader risk management efforts. This is evident through a decomposition of the risk. Whether risk is: (1) presented as the common function of a threat interacting with an exploitable vulnerability and a resulting consequence; (2) identified using the Factor Analysis of Information Risk and its focus on quantifiable loss event frequency, loss magnitude and their concomitant threat, vulnerability and loss component measurements; or (3) assessed using any other common methodology; the risk manager's conclusion is clear. Ransomware risk can be mitigated to a level at which remaining risk is either acceptable or fit for transfer. The mitigation techniques are nothing new. An asset owner can choose to mitigate threats (or at least the threat vectors), vulnerabilities, consequences, or a combination thereof. However, as will be discussed, innovations in threat vector mitigation offer tremendous opportunities for broader risk management efforts.

Beginning in reverse order, consequence mitigation strategies include business continuity planning, recovery planning, and the implementation of back-up and recovery solutions such that systems can be reconstituted and data restored based on pre-determined restoration points and maximum downtime targets.

Whether a threat actor wants to extort money in exchange for decrypting files, or whether an actor is focused on disrupting a business or sector, a well-planned, exercised and practiced back-up and recovery strategy will greatly mitigate the consequences. Of course, this approach also could be used to mitigate the consequences from other types of attacks as well as non-malicious human errors and natural disasters that impact an organization's data. As such, it serves as a threat-agnostic, all-hazards risk management solution.

Some ransomware and initial ransomware infection vectors will be designed to exploit known, published vulnerabilities. A vulnerability management program, which likely includes vulnerability detection, patch management and other mitigations, can limit the attack surface available to ransomware. Similarly, configuration management, proper network segmentation, and identity, credential and access management can prevent or otherwise limit ransomware's ability to spread laterally within an organization. Of course, instituting these practices will provide vulnerability mitigation beyond the threat of ransomware.

Finally, the ransomware threat vector can be mitigated. Common approaches include the use of intrusion prevention systems, next-generation firewalls, antivirus and sandboxing solutions. These are all good, if not best, practices. But they should be seen as baseline solutions. More is required. Focusing on the common threat vector of ransomware delivered via a spear phishing email, organizations looking to mitigate the ransomware risk should consider their defensive postures and how to improve them in light of the threat. Generally, email attachments are scanned by traditional, signature-based antivirus solutions at the email gateway and upon execution at enterprise endpoints. Innovations have added heuristic-based antivirus solutions and sandboxing opportunities. Such organizations' success is largely based on prior experience—a combination of previously seen malicious files, malicious behaviors, suspect behaviors, and other attributes of prior attacks. Yet email-based malware continues to effectively compromise individuals and organizations. Increasingly, it is used as a pivot-point from which so-called "file-less" malware can be introduced into an enterprise, presenting its own detection and prevention challenges. And as recently observed, the number of ransomware variants in use appear to be increasing, thereby reducing the chance of successful detection and prevention.

Considering the success of threat actors using phishing emails loaded with ransomware attachments, one can only conclude that while detection is necessary for effective cybersecurity, it is not sufficient. The "SANS 2018 Survey on Endpoint Protection and Response" suggests that "[t]raditional tools are no longer sufficient to detect cyberattacks, the data shows: Antivirus systems only detected endpoint compromise 47% of the time," and that advanced behavior-based detection tools are

GLASSWALL

Considering the success of threat actors using phishing emails loaded with ransomware attachments, one can only conclude that while detection is necessary for effective cybersecurity, it is not sufficient. The "SANS 2018 Survey on Endpoint Protection and Response" suggests that "[t]raditional tools are no longer sufficient to detect cyberattacks, the data shows: Antivirus systems only detected endpoint compromise 47% of the time," and that advanced behavior-based detection tools are being purchased, but not used due to lack of training and bandwidth among already over-worked information security teams.[25] For too long, the cybersecurity community has been trying to solve an increasingly intractable problem—identifying and stopping malicious file attachments before they infect an endpoint or network. Yet, automated assembly-line ransomware generation on an industrial scale, coupled with sandbox-aware or at least sandbox-evading attributes, will continue to defeat detection approaches far too often. The end goal of preventing malicious files from infecting an enterprise remains sound, but it requires solving a simpler problem. Instead of detecting and preventing "known-bad" files, enterprise email security must incorporate technology to simply look for, generate and pass "known-good" files.

Generating and passing "known-good" files can be achieved using deep-file inspection, remediation and sanitization technology (d-FIRST™), which has been maturing for several years and is already available in the cybersecurity marketplace. Glasswall FileTrust™ Advanced Threat Protection is just such a technology. In near real-time, it will compare a file to that file type's standard or specification (e.g., Microsoft Office specifications, ISO 10918 for JPEG, ISO 32000 for a PDF file), regenerate the file in accordance with that specification, and pass the file forward. During the regeneration process, Glasswall FileTrust™ performs two sets of actions. First, it remediates structural deviations from the file type specification. This includes fixing byte-level anomalies, which may be intentionally or unintentionally introduced into the file, but can create unwanted consequences. Second, it sanitizes functional aspects of the file based on an enterprise's security policies. For example, it can remove extensible attributes, such as macros, JavaScript, embedded files and metadata. Sanitization can be applied differently depending on user groups and their business needs.

The d-FIRST™ approach is a departure from traditional security techniques; more to the point, it's approach is the complete opposite of all preceding security solutions. All files are subjected to the process on a least-trust basis, instead of only acting on files that match a known signature or heuristic pattern. The results, however, fill a gap in traditional architectures. For instance, Glasswall Solutions tested 6,000 known and unknown malicious files with a global defense contractor.

A departure from traditional security techniques

[25] Kelly Sheridan, "Less Than Half of Cyberattacks Detected via Antivirus: SANS", dated July 16, 2018. Summarizing the SANS 2018 report and available at: <https://www.darkreading.com/endpoint/less-than-half-of-cyberattacks-detected-via-antivirus-sans/d/d-id/1332309?_mc=NL_DR_EDT_DR_weekly_20180719&cid=NL_DR_EDT_DR_weekly_20180719&elq_mid=85822&elq_cid=25863258>.

GLASSWALL

Initially, only an antivirus solution was deployed. Of the 6,000 malicious files, 3,592 of the files were detected by the antivirus solution—a 40.13% failure rate. Subsequently, a heuristic layer was added by the systems integrator, which reduced the failure rate to 35.58%. Finally, Glasswall FileTrust™ was inserted in place of the signature- and heuristics-based solutions. Each of the 6,000 files was effectively remediated and sanitized because Glasswall FileTrust™ was not looking for known-bad.

In an operational example, a well-known brand that is a Glasswall Solutions customer in the tech sector received 347 million emails over a six-month period, including Microsoft Office, PDF and image files. Four layers of defense were applied to the files, including next generation firewalls, anti-spam and anti-phishing filters, antivirus solutions and a heuristics filter. Fifty-five million of the original files were processed and allowed to pass as 'clean' to Glasswall FileTrust™, the company's final line of defense prior to the email server. The multiple security layers failed to prevent 171 malicious files, almost an average of one file per day. According to the customer, Glasswall FileTrust™ neutralized the threats with no impact to the end-user experience. Glasswall Solutions began querying well-known malware repositories with the hashes of the original 171 malicious files. In some cases, the malware was known to the antivirus community, but the traditional solutions lacked a matching signature and did not interdict those files, similarly, the sandbox layer had been bypassed using new and previously unseen techniques, so it was not looking for that malign behavior. In other instances, not only did Glasswall FileTrust™ protect the customer on day-zero, but it took up to three, seven and even 30 days for the antivirus community to indicate awareness of the malicious files, and longer for the sandbox vendor to develop, test and release its updated software. Of course, with the d-FIRST™ approach this is to be expected. By subjecting all files to the security solution, previously unknown malware will be rendered inert. Customers are not only protected by Glasswall FileTrust™ on day-zero, but they have access to personalized threat intelligence as these are files often specifically directed towards them.

As with consequence and vulnerability mitigation strategies, the deployment of Glasswall FileTrust™ Advanced Threat Protection alongside more traditional solutions is threat-agnostic. Whether an adversary is engaged in a ransomware campaign or attempting to introduce another type of file-based malware into an enterprise, Glasswall FileTrust™ Advanced Threat Protection will neutralize the threat.

It serves an organization well to identify those risk management solutions that can best mitigate the widest set of probable threats, vulnerabilities and consequences. At the same time, not all systems and data are of equal value to the organization or threat actors. Investment and architectural decisions should take this into account, applying security, back-up and recovery solutions based on risk-informed decisions. Glasswall Solutions can support this effort through a no-cost risk assessment, which will demonstrate current security gaps and exposures as they relate to the formatted files entering and exiting an enterprise.

//

Multiple security layers failed to prevent malicious files

GLASSWALL

VI. Conclusion

Ransomware can cause significant losses in terms of extortion payments, the interruption of business operations, and associated cascading consequences. Clearly, some within the security community expect the threat of ransomware to increase in prevalence. Others expect the threat to remain, but evolve in terms of its victims, availability to a broader set of users, and ability to evade traditional security solutions. The events of 2017 confirm that ransomware is no longer the tool of cyber criminals focused solely on financial gain—nation states have their own, unique use-cases for it. No doubt, the direction ransomware will actually take over the next few years is unclear. However, the associated approaches to managing the risk it presents are well-defined.

One need only take a step back and assess cyber threat actors for what they are—value-maximizing individuals and entities. Just like Willie Sutton, they will target the prize—data, money, disruption or other objectives they value—in their efforts. Whether an organization is confronting ransomware, other malware-based attacks, other malicious activity, or non-malicious incidents, a common set of established and emergent risk management practices are available. In the aggregate, the threats driving these incidents will not stop. Smart prevention, response and recovery investments are available to address them in the aggregate.