SecureAge

SecureAge Technology 2019 Ransomware Protection Report

SecureAPlus Whitepaper

Table of Contents

Introduction

From its simple beginnings as a virus distributed through thousands of diskettes[i], the threat of Ransomware has grown by leaps and bounds in the three-decades since its introduction. What was mostly an annoyance created with the liberal use of symmetric cryptography, easily rectified by readily available decryption tools, is now a $1 billion revenue stream for cyber criminals[ii]. It is a worldwide digital epidemic that continues to make headlines for its effective means to extort money from large corporations down to the average computer user.

The year 2016 saw the meteoric rise of Ransomware with some reports pegging successful infections to have grown by 6,000%[iii], an exponential rate that is credited to the 400% increase in variants on that year alone. It is making cyber criminals so much money that it has sparked the introduction of Ransomware-as-a-Service (RaaS) - a worrying trend that lets any aspiring hacker to invest in the distribution of ransomware and get a slice of the illegal profits to be made.

Internationally, the economic impact of Ransomware attacks is far from understated, a 2018 research conducted by Cybersecurity Ventures has led its estimation for Ransomware damages from all around the world could cost more than $8 billion in 2018[iv], that's up from $5 billion in 2017. Making matters worse, this number is expected to go up to $11.5 billion by the end of 2019[v].

While the growth of ransomware and the number of attack incidents have been superseded by cryptojackers or cryptominers in 2018[vi], ransomware remains a more dominant financially-motivated malware attack with businesses losing $2,500 on average[vii] while also paying as much as $50,000 to decrypt their data.

With the threat of Ransomware looming on every corner of the digital age, the difference between business-as-usual and a successful attack lies on a keen understanding of the problem and the necessary tools to avoid or thwart an attack.

About Ransomware

Ransomware is essentially malware that encrypts a user's data without their consent with the intent of extorting money in exchange for restoring access by providing a means to decrypt the data.

What sets it apart from its malware contemporaries, except the period when it covertly encrypts data, is that ransomware does its best to make its presence known to the victim. Some even going so far as to permeate as many elements of what's left operational after the infection and guiding the user through the entire process of paying the ransom. This behavior is in stark contrast to malware that thrives on remaining undetected such as spyware, bots and Advanced Persistent Threats (APT).

Why is ransomware so effective?

With so much revenue to be had, it is clear why enterprising hackers have been jumping on the ransomware bandwagon. But beyond what's in it for cybercriminals, understanding the other side of the spectrum and delving deeper as to what makes ransomware so successful provides for a right frame of mind to combat the threat.

Here are the four reasons as to why ransomware attacks are so successful:

1. Modern Encryption Algorithms Used are Unbreakable

The rules of encryption applied to cybersecurity apply to ransomware as well. Without the key, victims of new ransomware would require significant resources even to come close to cracking encryption algorithms.

2. Designed with Speed in Mind

A 2016 study by Barkly showed that typical ransomware could encrypt 1,000 files in less than a minute. Even the most ideal cybersecurity infrastructure would take several minutes to react against any form of unprecedented security event like a ransomware attack.

3. A Certain Level of Trust in Delivery of Decryption of Files

The prevalence of cryptocurrency allows ransomware attackers to collect payment from victims safely. While not all attackers deliver on their promise, the relative safety enables attackers to release keys often enough to preserve the crooked business model.

4. Employment of Fear & Urgency Inducing Tactics

The notoriety of ransomware is earned from tactics that it employs to create a sense of imminent loss and urgency – clear deadlines, countdowns, and increasing ransom demand are its most effective tools to coax victims to pay up.

By understanding how it victimizes its targets, proper precautions can be implemented to daily practices as well as determining an appropriate set of tools that will empower users against Ransomware.

What are its sources of infection?

By the end of 2019, a business will get attacked by ransomware every 14 seconds. This number doesn't include attacks on individual users, which occurs even more frequently. For the most part, the delivery of ransomware follows the standard malware playbook, and 91% of these cyber attacks begin with spear-phishing emails[viii].

However, the people behind ransomware also come up with clever ways of getting their payload delivered and propagating.

A more recent and clever way of getting into people's devices was vxCrypter[ix]. The variant cleared up space on its victim's PC, effectively improving performance and increasing encryption speed.

Besides by way of infection, Ransomware developers have also made themselves readily available to enterprising hackers through channels that sell ransomware as a service (RaaS).

Ransomware attacks are also becoming more targeted. While there have been fewer incidents reported compared to prior years, part of the reason may be more about the shift from targeting more substantial businesses, that have better security measures in place, to smaller ones - about 71% of successful ransomware attacks in 2018 were on small to medium-sized companies[x].

How much can ransomware cost victims?

The average ransomware demand in 2017 is $1,077, which is almost four times or a 266% increase from the ransom in 2016 ($294)[xi]. This has since been cut in half in 2018 with demands now averaging $522. Despite being lower, it seems to have been a result of the market correcting itself – a lower demand increases the chances of the victims paying the ransom[xii].

In a study by IBM in late 2016, they found that nearly half of their business executive respondents have experienced a ransomware attack in their workplace with 70% of them claiming that their respective companies have paid to resolve the attack. The study also found that half paid over $10,000, and 20% spent more than $40,000. This response might be because it often costs small to medium-sized businesses to lose $8,500 for every hour their data remains encrypted by ransomware.

It's also not all about the ransom. Companies hit by ransomware incur costs of the downtime caused by these ransomware attacks. Norsk Hydro, an aluminum producer, refused to pay the ransom and has resorted to restoring their data from backups which have reportedly caused them $40,000,000 in damages.

GandCrab: The Most Prevalent Ransomware of Recent History

Perhaps the most prevalent ransomware of recent memory would be those propagated by the people behind GandCrab. It operated a ransomware-as-a-service business model to reproduce quickly – continuously spawning multiple variants and subversions to overcome any remedy that cybersecurity vendors could come up.

The operators even went so far as to take advantage of fraudulent data recovery firms[xiii] to rope victims into spending more on recovering their data. One distinguishing factor of this strain of ransomware is its use of the privacy-centric Dash cryptocurrency with the typical Bitcoin.

After just over a year of operations, the strain has caused over $2,000,000,000 in ransomware payments to the users of the service and reportedly netting the authors of the ransomware and service around $150,000,000 – enough incentive for them to announce the retirement of the service itself[xiv].

Notable Mentions

Besides the dominance of GandCrab infections over 2018, there's also another worrying trend of ransomware strains designed for highly targeted attacks against large organizations that have very low tolerances for downtime. These usually necessitate payment of the ransom regardless of higher demand. The two most recent examples of this are Samsam, Ryuk, and LockerGoga – all of which boast an average ransom several times that of typical ransomware.

	Released	Extorted Money	Avg. Ransom	Primary Attack Vector
Cryptolocker	2013	$3,000,000	$460	Botnet
Cryptowall	2014	$100,000,000	$500	Email
CryptXXX	2016	$73,000,000	$500	Trojan Malware
Locky	2016	$220,000,000	$1,200	Botnet
WannaCry	2017	$140,000	$300	Compromised Website
Cerber	2016	$54,000,000	$500	Ransomware as a Service
GandCrab	2018	$2,000,000,000	$1,170	Ransomware as a Service
Samsam	2018	$6,000,000	$25,000	Targeted Attack
Ryuk	2018	$3,700,000	$286,557	Targeted Attack

Source: CSO Online, ZDNet[xv]

In an annual repor, Cybersecurity Ventures estimates that yearly ransomware damages alone may reach $20,000,000 globally by the year 2021 to make it the fastest growing type of cybercrime yet[xvi].

How to Fight Against Ransomware Threats

The threat of ransomware is genuine. In 2018, at least 77% of organizations that were infected by ransomware were using up-to-date protection mechanisms[xvii]. Proper practices should be observed by every individual to a multinational corporation, in the event of an infection as well as establishing the appropriate preventive measures to ensure coverage against potential future incidents.

As ransomware developers continually find creative ways of attacking their victims, IT security professionals are expected to be one step ahead to anticipate the threat, prevent it from doing any harm, and have the means to decisively identify and exterminate the threat.

Anticipate

Education & Best Practices

User awareness and education are probably the most important preventive measures against the threat of ransomware. Cultivating a cybersecurity centric corporate culture minimizes the risk of a successful attack.

A recent study by Malwarebytes reveals that 53% of those surveyed believe that education and training are a high priority when it comes to ransomware prevention[xviii].

In knowing the threat and what is at stake, employees can exhibit the correct response in the event of potential risk or an actual breach in security.

Furthermore, laying out an incident response plan for such cases will ensure that affected organizations can minimize damage and immediate recovery of critical systems. Having an incident response plan also helps with preventing any further infections that may potentially be introduced by an existing or previous infection.

Application Whitelisting

Whitelisting techniques have been a vital component of enterprise IT security systems for years. It lets organizations create a list of discrete entities such as email addresses, port numbers, processes, and applications that are certain to be safe – usually those that are crucial to daily operations.

Application Whitelisting, in particular, prevents any unapproved applications from running without proper authorization. The approach proved useful for high-risk environments where it is crucial to be fully secure rather than having the flexibility of running a more extensive array of applications. Since then, Application Whitelisting has been a vital component of system baselining for the enterprise.

For ransomware to infect a system and encrypt files, it needs to run its code. By nature of its introduction to a system, it is highly unlikely that ransomware or its malicious components are on the whitelist as part of a baseline system leading to at least a detection of a non-whitelisted application trying to run.

With its vital role in protecting systems against advanced threats, recent versions of Windows now have application whitelisting features built-in through AppLocker, while Mac OS utilizes this to some extent by only allowing Mac App Store applications to run by default, and specific versions of Linux have AppArmor that works in the same vein.

Updated Software & Anti-Malware

Vulnerabilities of outdated installed software are usually the gateway for malware, not just ransomware, to infect systems. Software developers patch generally known vulnerabilities with the latest version, so keeping those up to date is one-way effective way of preventing systems from being compromised.

Having an anti-malware solution with real-time protection helps with preventing known threats from infecting devices while in use is vital. These software solutions should also be continuously updated to ensure that they have the latest library of threats at their disposal and are ready to react whenever these come into contact with their systems.

Offsite Backup

One of the most critical characteristics of ransomware is its ability to infect as much data as possible within a short time. This ability to infect persists beyond the initially infected device and may spill over to other endpoints, including storage servers.

Keeping regular backups of critical files on storage media disconnected from your networks is vital to keeping them safe against an accidental ransomware outbreak. Having frequent on-premise data backup to a known good state is crucial for organizations that heavily rely on victimized data, such as in the case of healthcare.

Taking this a step further by keeping additional regular backups offsite, in other words outside the premises of normal operations, provides an extra level of safety for critical data.

Prevent

Application Control

Application Control is mainly a security practice that restricts or outright blocks any unauthorized applications from executing. Combined with Application Whitelisting which maintains the list of trusted files and applications, it becomes the most effective means of preventing any known or unknown threat such as ransomware from ever infecting a system without the knowledge of its users.

This concept of a block-first approach essentially puts the user, or in the case of organizations the IT administrator, total control on what can and cannot run on their endpoints without worrying about actively looking out for newer and unknown threats.

By having a baseline list of what is safe and allowable (the whitelist), any unexpected threats are prevented from executing and will not be able to harm the system as long as Application Control is in force.

For all its capabilities, ransomware is still an application that needs to execute to be able to start encrypting files. Ransomware (or any malware for that matter) that cannot run is unable to encrypt a system.

This constraint makes application control one of the most effective ways to prevent ransomware or any unknown threat from being able to infect systems.

Command Line Scan/Protection

The command line is an integral part of an operating system. It is probably one of the most direct ways of accessing vital functions and is often a vulnerability exploited by malware. In the case of ransomware, there are some variants that gain access to an infected system's Master Boot Record (MBR)[xix] to alter Windows startup behavior as well as delete file backups that Windows creates.

Command line-based attacks may also be a precursor for a ransomware attack. By taking the form of a script, a file-less attack vector may render systems that rely on file-based attacks from detecting it in time and preventing it from either infecting or spreading.

Command line protection operates similarly to Application Whitelisting in that it plays a role in system baselining by creating, enforcing, and updating a set of rules that only allow recognized commands to run, thereby preventing advanced ransomware from exploiting this attack vector.

Firewall

A critical component of a ransomware attack is its ability to vulnerable networks to both communicate with its source to store the key used to encrypt its victim's files and also to propagate to other devices in the network.

A high-performance firewall, therefore, plays a vital role in securing the enterprise environment against ransomware attacks. In the event of successful entry of ransomware in a system, one of the first things it does is to contact its command and control server to generate the cryptographic keys[xx], without it, the encryption cannot proceed. A well configured next-generation firewall should be able to detect this suspicious network activity and stop it, effectively preventing the ransomware attack. The same applies to the suspicious network activity that happens when ransomware tries to spread through the network.

Sandboxing

Sandboxing, that is creating a temporarily closed environment where files are allowed to run but are unable to affect critical systems, is another way of preventing ransomware and malware in general from infecting endpoints. This, in conjunction with antivirus/anti-malware and behavioral-based security solutions, can detect and isolate ransomware threats.

However, recent advances in ransomware development can also account for this whereby ransomware will not unpack its payload if it recognizes that it is being sandboxed and observed by security systems. These variants only unpack their payload once they detect that they are on a legitimate system.

Security experts from Minerva Labs have found a way to exploit this advanced ransomware behavior by developing a way to trick the ransomware into thinking it is perpetually in a sandbox environment and thus preventing ransomware from executing entirely[xxi].

Examine and Exterminate

Known-Threat Detection

Traditional anti-malware engines remain a very relevant component for detecting known threats. They are typically ineffective against zero-day threats due to their reliance on signatures for detection, which is unavailable for fresh viruses and malware. However, their strength lies in their sheer reliability in diagnosing known ones that have been analyzed by thousands of analysts from various vendors around the world.

The leading anti-malware vendors would also have an extensive library of known ransomware; some have even designed specific ransomware prevention engines that are separate from their primary anti-malware solution.

A well-designed anti-malware engine would have the capability to detect and eliminate known ransomware based on their signature. Modern incarnations of anti-malware engines also have behavior monitoring capabilities and flag potential threats if it exhibits known malicious behavior during execution. This behavior, however, poses a risk to a system if behavioral detection fails, without the help of a sandboxing component to contain potential threats.

Unknown Threat Detection

The threat of malware has been continuously evolving. Relying on a signature and behavioral-based approach may no longer be sufficient. Ransomware developers have been putting in place techniques that allow them to avoid traditional methods of detection and prevention, some even going so far as to behave differently if they detect that they are in a sandboxed environment[xxii].

Furthermore, a 2017 enterprise risk index study[xxiii] found that only about half of all file-based attacks are submitted to malware repositories with only 20% of those accounting to signatures recognized by anti-malware solutions. These findings indicate that on a best-case scenario, 9 out of 10 times, solutions designed for known-threat detection are unable to identify malware when it is initially released.

The advent of Artificial Intelligence has introduced anti-malware applications of the technology. By leveraging big data, AI-driven anti-malware engines can identify ransomware threats without the need for signatures. By relying solely on its capability to analyze a file to immediately determine if its malignant or benign, AI-driven anti-malware engines are better positioned and are more reliable for detecting zero-day threats.

The capability to detect zero-day attacks to combat ransomware is critical – 76% of successful attacks on organization endpoints in 2018 were zero-day[xxiv]. With projections showing that there will be a ransomware attack on businesses every 14 seconds or just over 6,000 attacks daily in 2019, about 30% of them will be zero-day or about 2,000 ransomware variants daily.

Ransomware Protection with SecureAPlus

In 2015, the overall annual cost of global cybercrime was estimated to be at $3 trillion and is expected to double that by the year 2021. This trend is spurred upon by the increasing risks brought upon by the rapidly evolving strains of ransomware which experts have pegged to have caused $1 billion in damages in 2016.

As ransomware continues to be successful, owing to its capability to capitalize on the vulnerabilities of both society's digital infrastructure and mindset, individual and organizations alike require a cybersecurity solution that addresses these vulnerabilities by defending against the emerging threats of today and tomorrow.

The multi-layered approach of SecureAPlus to endpoint security is designed to be able to anticipate threats, prevent damage, and decisively identify and exterminate threats.

Creating an enterprise endpoint security baseline has always been the foundation of a secure system. Larger organizations have a wide variety of applications that need to be approved and tested before being added to an application whitelist so finding the right application control and whitelisting solution that accounts for these rapid changes is essential for larger deployments.

SecureAPlus makes this process more intuitive than ever by having a smart and automatic system of creating the initial application whitelist. IT security professionals can simply install SecureAPlus on their baseline machine, make use of the powerful automation in initially setting up the application whitelist, utilize the different specialized application control modes to further improve the whitelist whilst putting the baseline endpoint into intended end-user use cases, then ultimately exporting and rolling the whitelist out as part of their security policy.

Besides Application Whitelisting, the inclusion of command line and process protection features further enhances the level of security that is easy to deploy on enterprise endpoints.

While firewall and sandboxing are undoubtedly great additions to a layered security approach, what SecureAPlus adds to the table when it comes to the threat prevention layer is with its implementation of Application Control. Unlike other security solutions, application control stops potential threats, including zero-day ransomware, from executing as long as it is not on the whitelist.

However, a common issue that enterprise application control implementations face is that there is a considerable demand for curating and maintaining an application whitelist to exert application control without impacting productivity. SecureAPlus solve this by not only allowing IT administrators to update the whitelist on the fly, but also creates an active feedback loop between end-user and administrator to review, examine and update either the central or a specific endpoint's whitelist.

Finally, SecureAPlus provides organizations. Specifically, it's IT security administrators with the most comprehensive sources for identifying both known and unknown threats. The Universal AV puts together multiple anti-virus engines to diagnose a potential threat against a combined library of known threats. The AI-driven APEX engine, on the other hand, is positioned ahead of the competition with its predictive capabilities. As such, it excels at identifying ransomware mutants that were previously unseen and unknown. With both features combined, while maintaining a small process footprint, IT security administrators always have ready-access to the right data to make informed decisions to allow or exterminate a potential threat with conviction.

Conclusion

In 2015, the overall annual cost of global cybercrime was estimated to be at $3 trillion and is expected to double that by the year 2021. This trend is spurred upon by the increasing risks brought upon by the rapidly evolving strains of ransomware which experts have pegged to have caused $1 billion in damages back in 2016 – a figure now dwarfed by a single strain of malware (GandCrab).

As ransomware continues to be successful, owing to its capability to capitalize on the vulnerabilities of both society's digital infrastructure and mindset, individual and organizations alike require solutions that not only respond to the growing threat but also be one or two steps ahead of them.

While solutions built to react, and withstand a ransomware attack such as anti-virus, anti-malware, immediate backup, and recovery systems are essential to every organization, it is also equally or even more necessary to invest in solutions that safeguard the integrity of your systems against both known and unknown ransomware attacks.

SecureAge Technology's SecureAPlus provides a one-stop solution that not only covers detection of known threats but also against unknown threats through its unique implementation of combining an AI-driven native anti-malware engine, multiple cloud anti-virus engines with application control and whitelisting.

This range of detection essentially allows it to have one of the broadest coverage of known threats protecting endpoints in real-time and an effective means of identifying unknown threats from day one without slowing down system performance due.

Furthermore, it effectively blocks unknown threats with its intuitive way of creating and maintaining whitelists that are either unique to its endpoints or can be managed via a dedicated management console within the organization or remotely through a cloud management console – a necessary and useful feature for small and large organizations.

Finally, it accounts for advanced vectors of attack, such as fileless malware. While such threats can bypass the defenses offered by traditional file-based antiviruses, they are stopped cold in their tracks by SecureAPlus' block-first approach and command line protection.

In all, SecureAPlus exemplifies SecureAge Technology's multi-pronged approach to cybersecurity. With multiple layers of defense built in, SecureAPlus is perfectly positioned to anticipate, prevent, and exterminate the threats of today and tomorrow.

References

[i]http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html#slide2

[ii]http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html

[iii]http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html

[iv]https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/

[v]https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

[vi]https://www.techrepublic.com/article/cryptomining-replaces-ransomware-as-2018s-top-cybersecurity-threat/

[vii]https://www.comparitech.com/antivirus/ransomware-statistics/

[viii]https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

[ix]https://fossbytes.com/vxcrypter-ransomware-performance/

[x]https://healthitsecurity.com/news/71-of-ransomware-attacks-targeted-small-businesses-in-2018

[xi]https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0426_01

[xii]http://invenioit.com/security/2018-ransomware-statistics/

[xiii]https://www.coveware.com/blog/2018/12/11/beware-of-dishonest-ransomware-recovery-firms

[xiv]https://nakedsecurity.sophos.com/2019/06/04/gandcrab-ransomware-service-shuts-up-shop/

[xv]https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

[xvi]https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[xvii]https://safeatlast.co/blog/ransomware-statistics/

[xviii]https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Singapore.pdf

[xix]https://www.enigmasoftware.com/commandlineransomware-removal/

[xx]https://www.backblaze.com/blog/complete-guide-ransomware/

[xxi]https://www.forbes.com/sites/edmundingham/2016/03/12/israel-cyber-tech-startup-minerva-labs-prevention-without-detection-is-possible/#187b21ac7382

[xxii]https://www.securityweek.com/karmen-ransomware-deletes-decryptor-if-sandbox-detected

[xxiii]https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_Whitepaper_EnterpriseRiskIndex_FINAL%20%282%29.pdf

[xxiv]https://www.votiro.com/2018-the-four-zero-day-attack-stats-and-trends/

Website www.secureage.com
Contact protect@secureage.com

SecureAge

Singapore 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
United Kingdom 74 Mackie Avenue, Brighton, BNI 8RB, Company No. 11734665
Japan 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
North America 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA