White Paper

Understanding Ransomware and Beating it with Cyemptive

May 8, 2021

TODAY'S RANSOMWARE THREAT

In the cybersecurity battleground, ransomware is an especially difficult challenge. Recent attacks that featured "WannaCry," "Petya," "Ryuk," "NetWalker," and their variants have made news headlines for being particularly virulent. Organizations are vulnerable and looking for solutions.

What Is Ransomware?

Ransomware is the general term for malicious software (malware) that encrypts files on a user's computer system and holds them for ransom. It is a specific form of virus software that spreads with the intent of making money for those who control it.

What Does Today's Ransomware Do?

Ransomware encrypts, or scrambles, the vital contents of a computer and holds them for ransom. Usually, the ransom is to be paid with a certain time period, say 72 hours, or the encryption key will be destroyed, rendering the encryption permanent.

Encrypted Payment is usually requested in an online currency such as Bitcoin to an anonymous destination. Most ransomware criminals are true to their word and decrypt the files once the ransom has been paid. Nonetheless, Kaspersky Labs reports that 20% of victims never get their data back.

How Does It Work?

A common misconception is that ransomware encrypts an entire computer system. In reality, to encrypt an entire system would take many hours, and would most likely be detected by a user before it could be completed. In addition, a system that was completely encrypted wouldn't work at all, making it impossible for the virus to deliver the ransom demand, or fulfill the decryption once the ransom has been paid.

In fact, ransomware usually only encrypts some files, and even those not entirely. Encrypting the first portion of a file is sufficient with most file formats to render them inoperable. This is fast, and for most users is functionally equivalent to rendering the entire system unusable.

The software then installs a program to take over the computer, display an ominous message, and offer instructions for paying the ransom. Once paid, the effects are reversed, but in many cases not all traces of the program are removed.

How Does Ransomware Spread?

Ransomware spreads like all computer viruses, most often initially through email attachments. Emails are sent with attractive or misleading subjects and contents that cause users to open the attachments and thereby install the virus. Occasionally malware is installed when a user visits a web site, but this attack method is getting harder and harder as web browsers are made more secure.

More troubling, however, is that many ransomware variants also spread through hidden machine-to-machine connections. The software locates and learns other computers on the local network and installs itself on those machines. In a loosely controlled network, such transmittal can result in the infection of a majority of the computers in a matter of hours. According to a recent Webroot report, fully two-thirds of ransomware infections are delivered in this fashion, hitting even the most careful of users.

This trend toward network transmittal is especially important as many firms, and many users, have become extra vigilant about opening email attachments. Where previously each infection required a mistake by a user, now an entire network is at risk from just one local infection.

What Are Variants?

Like viruses in the natural world, there are many different forms of ransomware viruses. This is made more common by a vigorous black market in virus toolkits that make creating new versions of the software easy.

Ransomware variants became news when the recent WannaCry virus was found to have a “kill switch” in it that promptly disabled it. Soon the creators had built a new version, or variant, that did not have that switch. This variant also quickly spread.

Variants are an issue with any virus as they can wreak havoc with many of the most common detection methods. Many virus and ransomware protection programs rely on being able to recognize the software to defend against it. A new variant can fool the detection software and be allowed to pass.

In Fortinet’s 2020 Global Threat Landscape Report, they found that ransomware has increased sevenfold from July to December 2020.

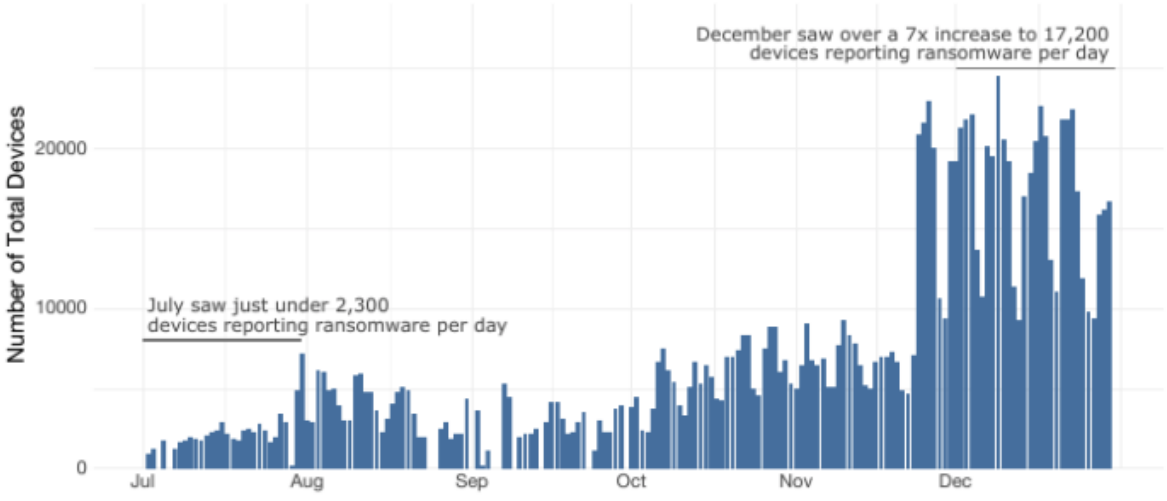


Figure 8: Daily number of devices detecting ransomware variants in 2H 2020.

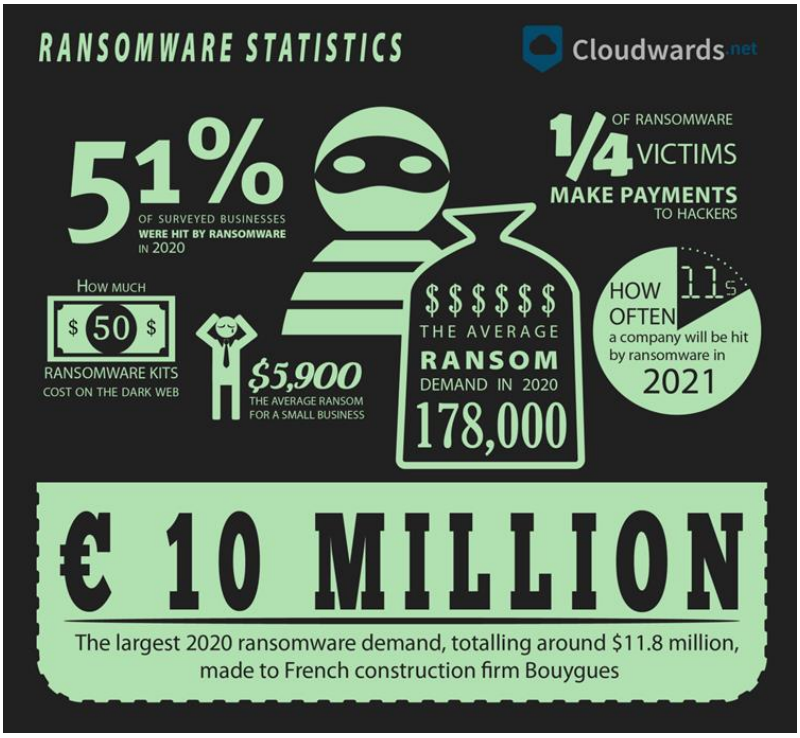
Hackers are developing 300+ variants daily, and according to a March 2021 DataProt.net article, every minute, four companies fall victim to ransomware attacks. These attacks are happening faster than solution providers can identify the ransomware and incorporate into their scanning technologies.

What Does Ransomware Cost?

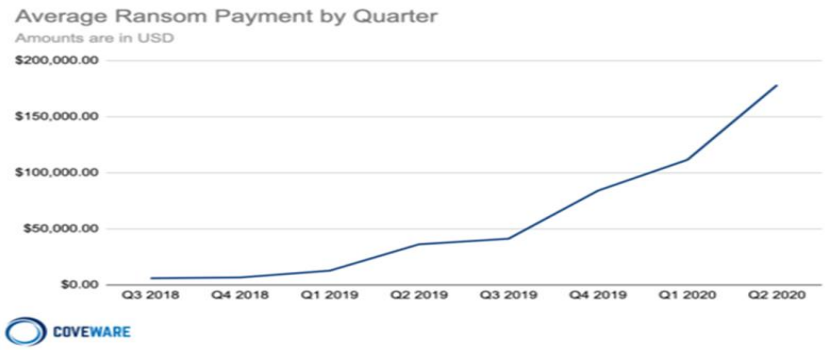
The costs of ransomware to organizations large and small is increasing at an alarming rate. Ransomware has increasingly become the malware of choice, with a recent report from Malwarebytes showing that 6 in 10 viruses are ransomware.

Companies are increasingly at risk, Barkly reports that over 70% of businesses targeted actually being infected. Kaspersky estimates that a company is hit by ransomware every 40 seconds.

According to an article published by Cloudwards.net in March and updated May 6, 2021, ransomware attacks are growing in size and frequency at an alarming rate, threatening businesses around the world.



In another article published by Coveware in August 2020, the average ransom payment in Q2 2020 was $178,254, a 60% leap from the $111,605 average in Q1.



However, both Barkly and Intermedia report that the real true cost is in productivity. The average downtime for a computer hit by ransomware is at least three days, and over 15% are down for more than 10 days.

This downtime impact, especially in time-critical industries such as health care, can be devastating. The National Cyber Security Alliance estimates that 60% of small businesses that suffer a ransomware attack don't survive another six months. For medium size businesses, the costs run to a million dollars, and rise exponentially for enterprises.

All-in-all, ransomware is a huge risk to businesses worldwide, with the cost estimated by GroupIB at over $1 billion in 2019-2020, but the actual damage is likely to be much higher.

In short, ransomware is a risk all companies should take very seriously.

Market Attempts to solve Ransomware

A few leading antivirus scanners have been evaluated to a 99.9% detection rate with a number of false positives and some with significant impact to the system (www.av-comparatives.org). These are controlled, lab tests that simulate an enterprise environment for malware and real-world detection. The same controlled-environment tests also show that ALL tested antivirus software exhibited some degree of scanner compromise by malware up to almost 10%. None of the resulting rates depict or could test Zero-Day exploits or network Zero-Day exploits. These considerations would lower detection significantly and possibly to 0% if severely compromised.

It is difficult to truly determine the actual effectiveness of antivirus scanners with the record numbers of infections reported, malware variants, Zero-Day malware exploits, and an excess of marketing. With the reduced rate of signatures to new variants, ineffectiveness and possible compromise of antivirus scanners, traditional methods must be questioned and scrutinized heavily. Be wary of scanning solutions that do not integrate with a network protection platform. The solutions must provide security boundaries to isolate and eliminate the chance of scanner compromise by the very malware they are looking for in the scans. Consideration should be given to solutions that have higher detection rates like 99.9999% and have little to no impact to the environment.

An Example: If a medium size company is considered, they can easily have 10 Million files. A 98% success rate when scanning files leaves about 200,000 files compromised, at risk, or unscannable. This success rate is unacceptable protection in security-conscious environments.

Common Ransomware Protection

Most software that protects against ransomware relies on detecting the virus and preventing it from installing on the target computer. These products monitor API calls and call it behavioral learning to filter all incoming files to detect the malware and keep it off the system.

Signature Based Detection

The traditional form of detection for viruses, including ransomware, has been a signature-based method. The known variants of the virus are cataloged, and a "signature" – a unique pattern – is identified that can reliably detect each one. Using this signature, every incoming file is scanned for the pattern and the virus is identified.

Each time a new variant is discovered, an update is made available by the cybersecurity company. The client computers must update, usually daily, to include protection from the latest variants. Machines that are not updated, either because their maintenance coverage has lapsed or their software is not updating properly, are vulnerable to each new variant.

It is important to note that a new variant is most often discovered when someone is hit with an attack, recognizes it as a new variant, and reports it to their cybersecurity vendor. New variants often go unreported for some time before they can be cataloged and an updated signature list is produced.

Machine Learned Detection

With the increasing number of variants of viruses in the wild, and the ease at which new ones can be created, cybersecurity companies have realized the futility of signature-based detection. They have, instead, turned to machine-learning and artificial intelligence to identify new variants.

These machine-learning techniques rely on exposing the software to a wide range of viruses and "teaching" it what a virus tends to look like. Then, using the artificial intelligence techniques, they can identify new viruses and variants with a degree of confidence they have never seen before. These still require API driven attacks and cannot detect the self-contained driven attacks.

This new technology is not reliable. These systems are prone to too many false alarms and missed viruses, but they do help augment a signature-based strategy. The cyber protection effectiveness of machine learning, API monitoring, checksums, white lists and signature-based detection is not strong enough to handle the amount of zero days being found in the marketplace. A zero-day attack (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of before it is identified.

Filtration Is Expensive

Even if a signature or machine-learned detection system was 80% effective, it is still an expensive process. Every new file needs to be scanned to see if it has a virus. With large files and ever-growing signature lists, this can take some time. Even with relatively small files, the time delay it takes to scan a file can be frustrating to users and represents a cost in productivity.

In addition, because some files may get into the system through unfiltered means, periodic virus scans of the whole computer must be performed. Usually, these scans are scheduled to be done weekly, and can take from one to several minutes.

Detection By API Monitoring

Most detection technologies today use API monitoring. They review all calls made to a specific API within an Application, Operating System or stack. We call it a signature when they call 3 sequenced API calls. Behavioral learning takes the sequenced calls and calculates all the permutations of the APIs and monitors for anyone requesting any form of sequence other than the signature. In the chart below, we share a 3 API matrix example of how this works. More importantly we will share why this is not the most efficient way of dealing with the issue. As you can see from just 3 APIs, the matrix for monitoring the APIs is manageable. However, eight APIs would have 97,000 permutations! But the reality is in a sample operating system there are over 6,000 APIs and the complexity of the matrix would be overwhelming. In some operating systems, there are 50 to 100 Million lines of code of calling those APIs. This is where and why operating system vendors today haven't solved the problem themselves. The solution would need GBs of RAM and dedicated processing cores to monitor the permutations of all the APIs appropriately, and this is simply not practical. When a cybersecurity company says they use behavioral learning to stop security threats, a relevant question is, "How many APIs are protected?" The typical answer is the "important ones," but most professionals don't know the answer. It really doesn't matter how many, it is impossible to monitor all of them. This is truly we feel the answer to solving the Malware / Ransomware security threats won't be in current thinking or technologies.

3 APIs Permutations		
1	2	3
1	3	2
3	2	1
3	1	2
2	1	3
2	3	1

Sleeper Ransomware Threats

Tomorrow's Ransomware attacks will be much harder to detect and will cause a much bigger impact on organizations. The types of attacks will be more focused on increasing the likelihood of payout. Today's Ransomware attacks have a lower chance of actual payout while payouts with attacks using Sleeper Ransomware will be higher.

Sleeper Ransomware is an encryption attack that doesn't prompt the user for payment right away, but rather it waits (sleeps) for 9 to 18 months while the backups become ruined with encryption as well the production data. The backups become useless and are not able to restore data after the 9 or 18 month

backup timeline. Sleeper Ransomware is the next step in forcing organizations to pay larger amounts of money because the impact has potential to bankrupt companies or governments.

Detecting Sleeper Ransomware is difficult or impossible in today's technology solutions because it doesn't prompt the user nor does it encrypt a large number of files that would instantly trigger "Behavioral analysis" and in turn trigger the sensors. The sleeper encrypts files at a speed much lower than normal ransomware and forces machine learning systems to monitor and track API calls for hours and days. These attacks cause AI-ML systems to use extreme amounts of RAM and processing power to perform weekly analytics to catch such attacks, and therefore significantly degrade system performance.

Sleeper Ransomware could already be rapidly self-replicating across the internet and is set to the sleeping time of 9 to 18 months, waiting for its call to run without knowledge of its existence.

Steganography Sleeper Ransomware Threat

The new and scarier of all attacks is a Steganography Sleeper Ransomware attack. This is where hackers are able to hide fully contained executable files inside of any type of file. These hidden files are un-detectable from any type of antivirus / malware / ransomware scan technology today. The files open normally as requested and look like normal files to the end user. They contain all the elements to execute without calling system level Crypt API calls (enabling encryption within) and the OS doesn't know the files requested will be encrypted. This attack can then encrypt any files within the OS or across operating systems. It also can execute firmware updates to devices on the network looking for and installing Sleeper Ransomware on any type of device with an IP address on it. For example, these devices can also become a replication distribution engine for the Steganography Sleeper Ransomware on every request or every 1000th request, hiding from any type of machine learning security technology. Leveraging its own level of machine learning, gathering data statistics, self-replicating across nodes with file transfer requests.

The same sleeper attack replicates on any type of system where it encrypts files directly without calling APIs and is waiting for the backups to be encrypted as well. This will put the environment into an encrypted controlled state based on the hacker's request. During this time, the hacker now can choose when or if the encryption keys can be deleted.

Once deleted, the hacker could disable many devices on the network and put the environment into an unrecoverable state. Imagine losing data from the past 18 months including all the backups. Imagine if the hacker doesn't care about money because another country or company has paid them to ruin the backups and send the stock price down in a company to causing all the info of the company to be lost for 18 months or more. Imagine if the name of the company attacked was the "NASDAQ" or any other stock market. All transactions in the past 18 months would have been encrypted, locked and made unrecoverable. Banks, insurance companies and other financial organizations losing up to 18 months of data would be a serious attack on any company.

This is a massively destructive technology that is available and is used to attack organizations today. The system architecture can be secretly compromised and any type of digital data or currency can be compromised with this technology.

Cyemptive Ransomware Protection

Cyemptive Technologies takes a completely different approach to Ransomware and encryption protection. Rather than relying on detecting viruses, and trying to keep up with the ever-evolving virus landscape, Cyemptive's encryption protection strategy focuses on the actual effects of encryption attacks and how they spread.

Encryption Detection

The principal threat that ransomware represents is the encryption of your valuable information.

Our scanner does not rely on known signatures or system API monitoring since hacks can occur at any level in an operating system. Rather than trying to learn and stop all the various ways a file can be changed, the Cyemptive Enterprise Scanner uses multiple unique processes and sensors applied to the actual unique "Cyemptive File State" to determine if there is any tampering. Through our revolutionary automated Cyemptive process, we can detect both known and unknown forms of encryption and other tampering such as embedded files.

Even the latest, newest, never-before-seen ransomware fails immediately at its core mission: to encrypt your data. Your information is protected.

In the rare case in which you intended to encrypt information, the Cyemptive Solution offers you the ability to authorize the encryption request, and let the encryption proceed. Yet, by detecting and controlling all encryption, only Cyemptive protects your systems from all malicious encryption activity.

Network Security and Defense-in-Depth

In addition to stopping the effects of ransomware, Cyemptive also stops it from spreading.

Cyemptive's revolutionary Perimeter Fortress (CPF) solution provides Pre-emptive Threat Protection at network perimeters, stops advanced global hackers, handles root level and firmware attacks with ease utilizing CyberSlice© technology, provides the ability to withstand and thwart attacks within seconds and prior to intrusion, and are financially backed by CyberSLA; performance-based SLAs in Minutes/Seconds.

Cyemptive does not offer a single solution, but several solutions that working together provide Defense-in-Depth at multiple layers in an environment leveraging the concept of Zero Trust. The Cyemptive Perimeter Fortress (CPF) is used at different levels in and across datacenters including a built-in state of the art Data Loss Prevention (DLP) solution. Cyemptive Zero Trust Access (CZTA) - resides on CPF for the ultimate in secure remote user connections. The Cyemptive Web Fortress (CWF) provides security at the load balancer, proxy server and web server levels. These Cyemptive solutions together provide the defense in depth approach by combining with intelligence sensors and our unique Zero Trust Blueprints enabling a Zero Trust defense in depth platform.

This network protection works against new malware variants that no one has ever seen before and protects computers running even unpatched or older software. Cyemptive delivers strong integration

from the edge to the web server working together to enable stronger protection than anything else found in the market.

Unparalleled Protection

Cyemptive's scanning technology is disruptive and innovative when combined with other Cyemptive Solutions following Zero Trust blueprints; we preemptively protect environments in an automated defensive and real-time protection process. Solutions that require human intervention cannot scale and cannot keep up with the increasing rate of cyber-attacks.

Summary

Today's ransomware attacks have evolved so that industry solutions have a harder time detecting encryption and file state changes in a reasonable timeframe to prevent actual compromise. For example, Artificial Intelligence and/or API call monitoring technologies monitor known attacks and detect compromises after infiltration.

According to a March 2021 DataProt.net article, hackers are developing 300+ variants daily, and, every minute, four companies fall victim to ransomware attacks. These attacks are happening faster than solution providers can identify the ransomware and incorporate into their scanning technologies, typically weeks or months before they are incorporated into a signature-based detection system or AI based filtering system.

Industry scanners are not finding any embedded libraries-based attacks which bypasses almost all scanning technologies found in the market today. The result is that some ransomware is getting past even the biggest solution providers in the industry.

Cyemptive's scanning technology is disruptive and innovative when combined with other Cyemptive Solutions following Zero Trust blueprints; we preemptively protect environments in an automated defensive and real-time protection process. We employ world-leading security architects, top ethical hackers, and many other employees with expertise other companies do not have. Cyemptive has developed revolutionary, patented and patent-pending technologies to achieve new capabilities around cybersecurity and compliance not seen before.