ManageEngine

Ransomware

COVID-19 caused mutations and the ultimate guide for protecting your remote workforce

Table of contents

The answers to the future can often be found by delving into the past. To understand the implications of COVID-19 on ransomware and to predict its future course, a thorough understanding of its evolution over the years is crucial.

The genesis

Ransomware is a type of malware that encrypts files in the victim's computer or denies them access to the computer itself until a ransom is paid. It is often disguised as trustworthy files in phishing emails, and once opened, virtually hijacks the victim's computer. Attempting to retrieve this data safely can be futile, as the key to decrypt the files may not be transferred even after the ransom is paid in full.

How it all began: AIDS Trojan attack

The first ransomware attack dates back to 1989. Exploiting the panic surrounding AIDS, this Trojan malware was distributed through infected floppy disks that were labeled "AIDS Information - Introductionary Diskettes" given to attendees at a WHO conference.

Even though there were no significant monetary consequences due to the free decryption tools that were released, this attack managed to change the cybersecurity landscape forever. Ransomware has continued to grip the IT world since then, with estimates of a new business falling victim to an attack every 14 seconds in 2019.

Evolution of ransomware

Over the years, ransomware has mutated significantly. The three elements that are imperative to a successful attack are, a strong encryption tool, the means to anonymously transfer the decryption keys, and ways to collect ransom while remaining untraceable. All these aspects have been reinvented to engineer the ransomware that we know today.

Re-awakening of ransomware

A lack of innovation and internet advancements paused the advance of ransomware until its reawakening in 2004 as GPCode. Spread through emails containing malicious attachments, these attacks were primitive with the encryption algorithm used, and had minimal effects.

Archievus followed that used a more advanced, RSA asymmetric encryption and then came Trojan.Ransom.A that combined aspects of adware. Ransomware began to encompass newer technological developments and strengthened its encryption techniques. Although these attacks were rendered futile by simple antivirus programs, they laid the foundation for a tsunami of future attacks.

Innovation in attack scenarios

The early 2000s saw a boom in scareware, a fake antivirus scam that incorporated ransomware aspects. Next came the first locker ransomware variant, WinLock Trojan. Unlike the previous versions of ransomware, this Trojan locked down the entire system instead of just a few files. Ransomware soon gave this a new creative narrative as Reveton that sent messages to its targets claiming to be from the FBI, notifying them that their computers have been locked due to copyright violations.

These ingenious schemes helped attackers across the globe evolve and innovatively combine methods that previously hindered the success of an attack.

Influence of the Bitcoin era

Throughout the years, the missing puzzle piece that hampered the smooth monetization of ransomware was the lack of a payment process that would let the attacker escape scot-free. The introduction of Bitcoin and other cryptocurrencies closed this gap, and helped perfect future ransomware attacks. The Cryptolocker attack of 2013 that affected countless Windows machines, utilized spear phishing techniques combined with an advanced encryption model like AES-256 to strongarm targets. The new normal became aggressive ransoms with threats to delete files if payments in Bitcoins, were delayed.

Easy and secure ransom collection enabled experimenting with new attack structures, and threat actors seamlessly moved from just targeting Windows computers to Android mobile devices, Linux, and Mac machines.

Ransomware as a Service (RaaS)

The year 2015 brought a huge change in the ransomware trend. Criminals developed samples, released as Ransomware as a Service (RaaS), to monetize it. The developer would receive a cut of the ransomware bounty, but not actually implement any of the dirty work. Even though initial RaaS kits came with hefty price tags of up to $3,000,

increased market competition brought it down, to as low as $39.

RaaS has exponentially increased attack instances as it removed the barrier between highly skilled and amateur hackers, making it easily executable for all.

WannaCry: The attack that shook the world

After various other innovative ransomware, like Chimera, Locky, Petya, etc., the first wormable ransomware, ZCryptor, caused a paradigm shift. ZCryptor spread through computers of the network without depending on spamming schemes.

As a result, in May 2017 the IT world saw its most damaging attack yet. Dubbed WannaCry, this wormable ransomware quickly swept through networks, encrypting the hard drive's of the devices in its way. It involved an exploitation of a vulnerability in the SMB protocol that is used to share files within a network.

Estimates from around the globe claim that WannaCry has cost $4 billion collectively, despite patches for the vulnerability being available prior to its exploit. Following this, attacks like NotPetya, Bad Rabbit, Ryuk, RobinHood, and others soon surfaced proving that ransomware was growing enormously, and constantly absorbing new advancements on the technological front.

The implications of COVID-19

Along with leveraging technological progress, cyber criminals are known to exploit global circumstances to their advantage. COVID-19 has changed the definition of a normal workplace, forcing many enterprises to send their entire workforce home with zero preparedness. This opened a Pandora's box of complexities, many of which are actively being exploited to pioneer cyber attacks. The major factors that contribute are as follows:

Opportunistic ransomware activation

Most people around the globe are often panic-struck and on the lookout for new information regarding the pandemic. Fear and curiosity might cloud their judgment causing them to fall prey for scams that they would normally be wary of. The inhabitants of the IT world are also no strangers to becoming victims of ransomware attacks that exploit dangerous diseases. Threat actors have cashed in ruthlessly on epidemics of the past, such as Ebola and AIDS; COVID 19 is no exception.

Ransomware is taking complete advantage of this crisis. With the pandemic causing a 350 percent hike in phishing websites, opportunities to facilitate attacks are plenty. Multiple accounts of COVID-19 themed phishing email campaigns and malicious applications that directly deliver ransomware have been reported. Attackers are also simply stealing their victim's personal information and holding it for ransom. Some of the schemes that ransomware now uses to entice their victims are:

- Phishing emails claiming to be from trusted organizations containing details about vaccines or other protective measures against the virus
- Emails or compromised websites offering free downloads of tools that can be used for remote work
- Scams offering financial assistance or employment opportunities from fake government organizations
- Malware covertly hiding behind phoney applications that claim to track COVID-19 cases

These opportunistic attacks also targeted industries, such as healthcare and financial services, that are challenged by strict compliance regulations. This often forced very public organizations to pay the ransom instead of opting for other alternatives.

Remote work intensifies vulnerabilities

Ransomware is also fully exploiting organizations worldwide that have made an unavoidable switch to remote work. The 2020 Vulnerability and Threat Trends Report elaborates on how ransomware has seen a whopping 72 percent increase in new samples in just the first half of this year. Poor controls on home IT networks, coupled with the anxiety steeming from uncertainty related to the pandemic can push the workforce to become easy victims to all sorts of ransomware attacks.

Depending on their role, users depend on virtual private networks (VPNs), or the Remote Desktop Protocol (RDP) to stay connected to their organization's network and its resources. If password policies or other settings are weakly configured, brute-force attacks can be used to compromise the RDP. Along with affecting that particular machine, attackers can leverage this breach as a foothold to move laterally through the network and encrypt all the machines in its way.

RDP attacks amid the COVID-19 pandemic have increased 330 percent in the United States, 524 percent in Spain, and 428 percent in Italy. Interestingly, this hike coincided

with when the disease peaked in the respective countries, further proving the opportunistic mentality of ransomware threat actors.

A portion of the workforce also now depend on personal devices to do their office work. This adds a whole new set of endpoints to the network, many with weaker security configurations than preferred by organizations. Even if the user is cautious enough to stay away from obvious signs of ransomware attacks, the same cannot be expected of other users who might share the device or connect to the same router.

In order to steer clear of ransomware attacks, organizations need to take extra caution to maintain proper email security, a remote patch management process, a network security solution and also preserve accurate backups of their data.

High-risk industries susceptible to COVID themed attacks

Ransomware, much like COVID-19, is unbiased while choosing its victims. However, to maximize its gains, attacks are often launched against industries that are already struggling to cope with this crisis. Here are a few of the worst hit industries:

Healthcare and medical suppliers take the worst hit

Hospitals and other health-care organizations are definitely facing the brunt of the virus. To make matters worse, ransomware threat actors have mercilessly chosen to exploit their existing state of helplessness. In fact, according to studies, the number of cyberattacks detected at hospitals in March saw a 60 percent increase in just 30 days.

Even before this disaster, hospitals have been easy targets. Patient's personal information, admit and discharge records, medical history, and claims are critical details that might put lives on the line if compromised or left inaccessible for even a short time. These concerns have multiplied as medical facilities already struggle to cope with the pressure of being overcrowded.To prevent any causalities that might occur due to possible down mes, healthcare industries often decide to pay the ransom. This susceptibility, along with not so secure IT controls are some of the reasons why ransomware threat actors continue to attack the healthcare industry.

An attack not only brings down operations, but also ruins the reputation of healthcare facilities with patients and can even lead to legal disputes. Ransomware perpetrators, in

addition to demanding ransom, also threaten to release patient's medical records publicly. It is imperative for health organizations to enhance their IT security game, in order to concentrate all their energy on saving lives. Here are some a few must-haves:

- Antivirus, along with an email filtering solution that instantly detects and blocks phishing attempts
- Software to check port security to avoid RDP compromise
- An easily retrievable backup of all critical patient records stored independently from the system
- Risk insurance policies that protect healthcare organizations from the implications of an attack
- Strong password policies to prevent brute-force attacks

Economic crunch makes financial services a target

The most prominent aspect that has taken a hit due to this pandemic is the world's economy. Unemployment and loss of business are driving numerous people and organizations into debt. Governments across the globe are trying to aid their citizens by providing them with relief packages until normalcy returns. However, ransomware has taken this adversity and converted it into a medium for their scams.

Multiple accounts of phishing campaigns through emails claiming to contain relief payments or related information has been recorded. Emails and websites containing fake employment offers are also prevalent. All of these malicious sources can install malware on the victim's device through a single click.

Additionally, ransomware threat actors who understand the economic structure and its present state are shifting their targets to industries that can still afford to pay hefty ransoms. This puts banks and other financial services on top of their list. Financial institutions have seen a 238 percent spike in attacks from the beginning of February to the end of April, at the onset of COVID-19.

In addition to the possibility of a big pay-off, banks are often victimized because of the pressure they face to comply with strict data privacy policies. Ransomware attacks can cause disruptions in their operations that can hamper their reputation and also cause effects on the global financial market.

Attacks on public-sector organizations

Public-sector organizations are often poorly funded and have inadequate budgets to support secure hardware and software practices, making them sitting ducks for ransomware attacks. Just like the medical industry, public-sector organizations also deal with crucial data and services that cannot afford to have down times, so they are often desirable targets for ransomware threat actors.

These organizations, unlike their corporate counterparts, are mandated to disclose details of the attacks publicly. Publishing this information can also make them vulnerable to other threat actors who might conspire to conduct copycat attacks. If public-sector organizations were previously prone to becoming victims, the COVID-19 pandemic has made them sure targets. With most of public-sector organizations' workforce shifting to remote work, a lack of ransomware awareness and prevention training has increased the chances of them falling prey.

Moreover, this pandemic has revealed major fault lines in the existing supply and demand chain. Organizations are relying on more per project contractors to satisfy their requirements, opening up a new avenue of attack vectors.

Even highly respected organizations, such as the World Health Organization, have witnessed attacks. The WHO attack was, fortunately, unsuccessful, but it emphasized the need for all sectors to adopt security measures. Proactively investing in defense mechanisms is more economical than remediating damages after an attack.

What does the future of ransomware hold?

Uncertainty is tied with the idea of the world returning to what was previously considered normal. With 67 percent of companies expecting to switch to work from home permanently, or at least for a long time, remote work is here to stay. Clearly along with the organizations, ransomware has also started to adapt and evolve to exploit this transformation. Listed below are a few ways in which ransomware is expected to mutate:

Attacks targeting SaaS platforms

Organizations are shifting most of their technology from on-premises networks to the cloud to make working from home easier. The providers of these technologies have also evolved to offer Software as a Service (SaaS) tools that are built for and housed in the

cloud. This enables the entire remote workforce to function efficiently, as applications that would normally be accessed through web browsers in the office premises can now be accessed through VPNs while at home.

While SaaS platforms are transforming to become a necessity, weaknesses are also being exposed, and ransomware threat actors are recognizing SaaS as a new avenue to exploit.

The conditions imposed by the pandemic have accelerated adoption of the cloud at many organizations. With many offline businesses shutting down, a huge attack surface for ransomware has disappeared, but this has introduced a new generation of ransomware attacks that target cloud data.

Adopting external tools for cloud-to-cloud back up of SaaS data and for 24/7 monitoring of the IT environment can help organizations reduce these attacks.

MSP based attacks

Managed Service Providers (MSPs) remotely manage an organization's IT infrastructure, including its endpoints, servers, firewalls, routers or switches, and Active Directory servers.

Remote work has increased security threats as it forces endpoints to connect to the office network and access their resources from multiple locations.This, along with the hike in cyberattacks, is pushing more and more businesses to opt for an MSP to control their management and security.

However, MSPs have quickly become one of ransomware's favorite targets, as attacking them can enable ransomware to gain access to multiple networks and devices in a single instance. To gain a foothold in the MSP's network, ransomware threat actors first launch an influx of attacks against the services that are commonly used by MSPs. Exploiting vulnerabilities in an MSPs' unpatched servers,and brute-force attacks to gain privileged credentials are also popular attack vectors.

MSPs, because of their client base, offer a vast attack area. While MSPs commit to good cybersecurity practices, they can still fall prey to persistent and continual cyberattacks because they are often small companies and have limited resources compared to larger organizations.

Data theft ransomware

A new class of data-stealing ransomware surfaced in 2018, and is expected to get bigger in the years to come. Considered a "big game hunting ransomware" that targets large enterprises instead of home users, it moves laterally in networks to impact a maximum number of machines.This data-theft ransomware proceeds to copy data into the hacker's servers before encrypting it. The stolen data is held hostage to encourage organizations to meet the attacker's ransom demands. In some cases, attackers also threaten to disclose the information publicly.

This ransomware evolution stemmed from the strong backup processes that organizations adopted over a period, that resulted in them not paying heed to any of the conventional ransomware threats. Attackers started stealing data to counter this and used this type of cyberattack to re-establish fear about ransomware. Maze, REvil, Snatch and Zeppelin are some of the variants of ransomware that exploit this trend.

Along with the organization's reputation, a significant data-theft attack can also break their bank. The General Data Protection and Regulation (GDPR) and California Consumer Privacy Act (CCPA) laws come with hefty fines if violated, often more than the ransom itself. This adds pressure on victims to give in to the hacker's demands when the customer's personally identifiable information (PII) is at stake.

Remote work, the influx of COVID-19 themed attacks, and the financial liabilities that the pandemic has held over organizations make them more vulnerable to such attacks. As Gartner notes, "Privacy is becoming a reason for consumers to purchase a product". Ransomware threat actors, recognizing this trend, will likely try their best to cause a breach.

Affecting OT through IT

The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released an alert about an attack on a pipeline operator. This ransomware entered the company conventionally through the IT network, but then changed route to infiltrate the Operation Technology (OT) network as well.

This new technique of attacks might suggest how ransomware will behave in the future. Unlike the IT network, the OT network is often unprepared to handle cyberattacks due

to the lack of proper backups, antivirus, or other conventional security mechanisms. Major downtimes can be anticipated if attacks aren't identified in the preliminary stages, and this causes many organizations to give in to their attacker's exorbitant demands.

Downtimes in critical regions of the OT department can even cause issues, considering how they are already operating with a minimum workforce.

A guide to combat ransomware while working from home

With ransomware there is no silver bullet that can ensure complete protection, however dutifully following these best practices are beneficial:

Prioritize email security

According to CSO, 94 percent of malware is delivered via email, making an email security solution indispensable in ransomware prevention. Organizations must maintain tools that filter incoming emails and reject those that contain executable attachments. Additionally, email servers should be configured to block addresses of known spammers and malware. To increase the effectiveness of these security measures, the entire remote workforce must also be trained to notice the basic signs of email phishing, such as recognizing emails with suspicious attachments, addresses, or links.

Conduct remote patching

Studies reveal that many of the software vulnerabilities exploited by ransomware have patches that have been around for awhile. Businesses must exert more attention towards adopting a strict patch management practice to ensure that they leave no such gaps. With working from home (WFH) becoming the norm, a dual-functionality patch management tool that enables both on-premise and remote patching is the need of the hour.

Opt for multiple security software

A firewall, antivirus, antimalware and antiransomware software must be used to form a stronghold that enables organizations to detect, remove, and protect against malicious programs, even while working from home.

Maintain reliable back-ups

The effectiveness of an organization's back up mechanism determines the consequences

it faces in the event of an attack. Businesses, irrespective of their size and sector, should regularly backup both their on-premises and offsite data, to protect against any unanticipated loss. Cloud backups are also imperative for helping organizations avoid paying a ransom. Additionally, users can create system restore points that they can return to in case their backup fails. However, this might not be successful with all ransomware variants.

Encrypt and store data

Even with dependable backups, organizations might give in to ransom demands to avoid public disclosure of their sensitive data. To avoid such breaches, organizations can encrypt all their sensitive data and store their keys in separate locations. If a data theft ransomware attack were to occur, the information downloaded by the threat actors would be of no use to them.

Enforce strict password policies

Brute-force attacks are common entry points for ransomware, and they cannot be averted unless organizations have strict password policies in place. With the conditions imposed by WFH, endpoints act as windows to the entire network, and are spread across expanses.The prevalence of various endpoints—desktops, laptops, smartphones, tablets, printers, etc.—shows the complexity of IT infrastructures, and emphasizes the need for strong password policies, now more than ever.

Disable Remote Desktop Protocol

As per studies, RDP was the most common delivery method for ransomware in 2019. With WFH deeming it vital, organizations need to prioritize RDP-related security. Stringent policies must be set to determine who gets to use RDP, and it should be made accessible only through a VPN. Port security must also be emphasized, the ports RDP (3389) and SMB (445) specifically must be left open only to trusted hosts.

Establish Zero-Trust and Least Privilege principles

Organizations must include software that enables them to establish the principles of Zero Trust and Least Privilege (POLP). Most attacks can be prevented by running only trusted applications and blocking the rest. Moreover, as ransomware can only execute with the privileges of the application, or the end-user device through which it enters the network, by restricting privileged access only to necessary applications and users, wormable malware can be isolated at its point of entry.

Restrict unauthorized downloads

As WFH has blurred the lines between professional and personal activities, employees are increasingly using their work gadgets for leisure browsing. Malicious websites or malvertisements pretending to be legit, can facilitate ransomware downloads in just a click. Organizations need to restrict the downloads and ensure that it occurs only from authorized sites. Additionally, vulnerabilities in web plug-ins can also be exploited by ransomware threat actors. Tools specifically built to shield organizations from such risks must also be adopted as part of their defense mechanism.

Exercise USB control

With every employee logging in to work from the comfort of their homes, anyone around them might be able to gain access to their device. Inserting a USB with ransomware into these machines can essentially bring down the entire network. Organizations need to employ a device control solution, to detect, and block all unauthorized devices.

Educate and train users

Organizations are only as strong and secure as their weakest link. Every network user should receive corporate training and awareness about the basic signs of an attack. They must be encouraged to report signs of intrusion they suspect, no matter how simple. The workforce must also be strictly advised against using public Wi-Fi, as it is more susceptible to ransomware.

How ManageEngine can help fortify ransomware defense?

Patch Manager Plus

This all-around patching solution offers automated patch deployment for Windows, macOS, and Linux endpoints, plus patching support for more than 650 third-party updates supporting more than 350 third party applications. Organizations can take advantage of ManageEngine Patch Manager Plus' capabilities to perform remote patch management to ensure that all their software and OS are updated, even for WFH personnel, thereby minimizing a large segment of ransomware's attack vectors.

Vulnerability Manager Plus

ManageEngine Vulnerability Manager Plus is prioritization-focused vulnerability management software for organizations offering built-in patch management. Packed with a myriad of other features, such as vulnerability assessment, zero-day vulnerability mitigation, high-risk software audit, anti-virus audit, port audit, web-server hardening, fire wall audit, password policy management, BitLocker encryption, and management of other security configurations, Vulnerability Manager Plus acts as an comprehensive solution for organizations keen on implementing security best practices.

Application Control Plus

ManageEngine Application Control Plus helps organizations gain a holistic view of their application network, enabling them to establish the principle of Zero Trust by creating rule-based whitelists and blacklists. Advanced features equip organizations to achieve POLP by identifying and eliminating unnecessary admin rights, while simultaneously managing application-specific privileged access. Application Control Plus minimizes the attack opportunities and ensures that even wormable ransomware is stopped at its point of origin.

Device Control Plus

MangeEngine Device Control Plus is an extensive security solution that allows the control, blocking, and monitoring of USB and other peripheral devices from unauthorized access to an organization's sensitive data. It's features, such as file access control, file transfer control, trusted device list, file shadowing, and file tracing, can be used in concert to ensure complete data security. With Device Control Plus, the possibility of ransomware entering through external devices is significantly reduced.

Browser Security Plus

ManageEngine Browser Security Plus is a comprehensive browser security tool that helps organizations of all sizes manage and secure browsers across networks. It enables them to gain visibility on browser usage trends, harden browsers settings, restrict downloads from untrusted sites, control browser extensions and plug-ins, lock down enterprise browsers, and ensure compliance with stipulated browser security standards. With Browser Security Plus, organizations can prevent the chances of ransomware intrusion through browser, by ensuring its unwavering hygiene.

Learn More