

How Timus SASE Protects Against Ransomware Attacks

Using Zero Trust to defend against ransomware

timus
ZERO TRUST NETWORK PROTECTION

Introduction

As computers and the internet became indispensable parts of our social and business lives, new types of technological crimes have emerged. Cybercrime and ransomware attacks are becoming increasingly prevalent and constitute a mounting threat. This type of malware, which leaves the victim's data locked or encrypted, followed by a ransom demand and a threat to leak compromised data, can cause untold damage.

Indeed, global damage from ransomware has skyrocketed from $325 million in 2015 to $20 billion in 2021. By 2031, this number is projected to reach a staggering $265 billion, while a ransomware attack will likely occur every two seconds – up from every 11 seconds in 2021.

Global damage from ransomware attacks is expected to reach a staggering $265 billion by 2031.

Understanding the nature of ransomware attacks and their consequences is the first step in planning for both prevention and recovery. Any organization – despite its best efforts to prepare and preempt – can fall victim to potentially destructive ransomware attacks.

This white paper provides a basic introduction to ransomware attacks and explains how Timus protects against them.

In 2021, a ransomware attack occurred every 11 seconds. In 2031, they will likely occur every 2 seconds.

© Timus Networks, Inc. 2025. All Rights Reserved.

Contents

What is a Ransomware Attack? 4

Stages of a Typical Ransomware Attack 6

Overall Costs of a Ransomware Attack 8

How Timus SASE Protects Against Ransomware Attacks 9

Conclusion 11

© Timus Networks, Inc. 2025. All Rights Reserved.

What is a Ransomware Attack?

Definition

Ransomware is a form of malicious software (malware) that leaves the victim's data locked or encrypted. Attackers typically demand a ransom from the victim in return for the decryption keys needed to restore the compromised data. The key allows the user to access the files and systems encrypted by the malware.

With ransomware becoming one of the biggest threats facing businesses and individuals today, it's no surprise that attacks are becoming more sophisticated, harder to prevent, and increasingly destructive. In recent years, the danger posed by the phenomenon has increased exponentially, with criminals targeting brand reputation by leaking confidential data. Attackers employ this tactic as an "insurance policy" if the victim's data is fully backed-up and the victim refuses to pay the ransom. According to surveys, 70% of all ransomware attacks in 2020 involved a threat to leak exfiltrated data. Along with the risk of losing data, victims can find themselves subject to serious dilemmas when ransomware groups sell stolen data on cybercriminal forums on the dark web.

Infamous Attacks

In 1996, ransomware was referred to as "cryptoviral extortion," a concept introduced by Columbia University's Moti Yung and Adam Young. The pair created a virus containing a hypothetical attacker's public key while encrypting a hypothetical victim's files. The malware then prompted the victim to send asymmetric ciphertext to the attacker to decipher and return the decryption key – in return, of course, for a hefty fee.

GP Code



Since 1996, ransomware has taken numerous forms, but the first significant attack was 2004's infamous GP Code, which was replicated via phishing emails.

Reveton



In 2012, Reveton entered the picture. This time, the means of transmission were outdated plugins. Reveton relied on symmetric cryptography.

CryptoLocker



One of the most high-profile ransomware attacks of 2013/14 was CryptoLocker, which affected over 500 thousand computers. The ransomware used required payment in cryptocurrency. It, too, used phishing emails to spread by way of attachments made to look like FedEx and UPS tracking notifications.

2017's "WannaCry" ransomware attack caused an estimated $4 billion in damage worldwide.

© Timus Networks, Inc. 2025. All Rights Reserved.

Petya 

Petya, which appeared in 2016, also blocked the boot sector of compromised systems while simultaneously encrypting certain files. This prevented users from accessing their computers unless they entered an access code – in return for which they were expected to pay.

WannaCry 

The most notorious example of a ransomware attack was the 2017 WannaCry outbreak, which infected 230 thousand computers in over 150 countries in only four days. WannaCry, which was only stopped by a kill switch, caused an estimated $4 billion worth of damage worldwide.

NotPetya 

Also, in 2017, NotPetya, which borrowed tactics from namesake Petya, enmeshed thousands of business and public institutions in a global cyber-net. However, this software version did not provide victims with recovery keys. Although it infected networks in multiple countries, many researchers now believe it was intended to mask a cyberattack on Ukrainian institutions.

Bad Rabbit 

Bad Rabbit was yet another ransomware incident that occurred in 2017. A cousin of NotPetya, it spread via a fake Flash Player update, mainly targeting media companies in Russia and Ukraine.

Ryuk 

Ryuk, which is thought to be derived from the Hermes virus, was first encountered in 2017. However, the majority of its devastating effects weren't felt until the last quarter of 2019, when it jeopardized many companies' data.

2021 saw a 92.7% increase in ransomware attacks compared to 2020.

Sodinokibi (REvil) 

The same year saw the appearance of the ransomware known as Sodinokibi (also known as REvil). This particular variant was characterized by its advanced evasion capacity and wide range of countermeasures for avoiding detection. REvil struck numerous targets across the globe, causing widespread – and in many cases costly – disruptions.

NetWalker and CLOP were two major ransomware to appear in 2020, and attacks continued apace into 2021. According to surveys, ransomware attacks rose by 92.7% year-on-year in 2020.

So far, the most prolific ransomware gangs so far in 2022 have been Conti and LockBit. As of April, the two groups together have been responsible for more than 1,500 attacks worldwide. Both groups target mid to large-sized enterprises, from which they demand a ransom amount based on the organization's perceived ability to pay. Conti's average ransom demand has been $520,559; LockBit's has been $185,432.

Conti and LockBit alone were responsible for more than 1,500 attacks to have occurred so far in 2022.

© Timus Networks, Inc. 2025. All Rights Reserved.

Stages of a Typical Ransomware Attack

Typically, ransomware attacks begin with the initial compromise of an environment. This is usually accomplished by tricking a victim into downloading a malicious file, exploiting remote desktop protocol (RDP), or running a malicious script in memory to search for exposed privileged credentials. The next stage includes lateral movement and data exfiltration. The attack concludes with encrypting data stores and finally demanding a ransom.

1. Infiltrating the victim's environment

The first stage of an attack is where the attacker sets up the ransomware to infiltrate the victim's system. The attacker can do this by employing:

- Scan-and-exploit attacks against a vulnerable internet-facing system
- Stolen (or guessed) credentials to log in via remote-access solution
- A pre-existing malware infection delivered through phishing or other means

With a 63% exploitation rate for internet-facing devices (VPNs, appliances, web-based management platforms, email servers, etc.), these represent the most common means of infiltration. The second most common is credential abuse using brute-force attacks, stolen credentials, and password spraying, reaching a percentage of 23.

As the number of users in your organization increases, the risk of a targeted attack – like phishing, malicious websites, or combinations thereof – also increases. Note that it only takes one user to make a mistake and inadvertently execute the ransomware code.

Note that it only takes one user to make a mistake and inadvertently execute the ransomware code.

2. Installing malware

Once it infiltrates, the ransomware sets up a communication line back to the attacker, through which additional malware can be deployed. Some processes may look legitimate, but they will run from unusual locations in the file structure. The ransomware could be lying dormant – without arousing any suspicion – for days or even months.

© Timus Networks, Inc. 2025. All Rights Reserved.

3. Moving laterally

To access as much data as possible, cybercriminals use malware and restore connections to move laterally across other systems within the organization. To do this, attackers can use native operating-system tools or open-source penetration testing tools and certain live-off-the-land techniques to escalate privileges.

4. Terminating security and monitoring processes

Many ransomware variants also target backup systems to prevent victims from restoring their data. This is a unique feature of ransomware. It attacks backup copies in the victim's system, often deleting them to ensure that backup copies can't be used to recover lost data. Most other fraudulent software does not eliminate backup files. Another typical move by attackers is to disable system-restore features, which the operating system can theoretically enable.

5. Exfiltrating data

Increased network access allows attackers to target critical data for exfiltration and encryption. Command-and-control (C&C) server channels used for communication can be employed to exfiltrate data from compromised organizations. Data exfiltration plays a major role in most name-and-shame ransomware operations. Threatening to leak stolen data also gives attackers additional blackmail opportunities.

6. Encrypting data stores

Once backup files are deleted, and the exfiltration is complete, the malware starts performing a secure key exchange. Communication with a C&C server isn't necessary for encryption. The encryption keys in the local system are established, and the malware will begin encrypting files.

Different ransomware variants use different encryption methods, ranging from encrypting the master boot record of a file system to encrypting individual files – or even entire virtual machines.

7. Demanding a ransom

The last step involves the attacker demanding online payment, usually in a cryptocurrency like Bitcoin. This stage can also include threats to leak data or name-and-shame scenarios. The media is informed that your organization could not ensure the security of its data – and that of its customers.

The attacker can make contact through an anonymous email address, demanding that the victim follow certain instructions on an anonymous web page to make payment. Generally, companies will be given a few days to make the payment, failing which the ransom demand can be expected to increase. However, even if the ransom is paid, there's no guarantee that the victim will ever recover their data.

© Timus Networks, Inc. 2025. All Rights Reserved.

Overall Costs of Ransomware Attacks

Apart from the obvious ransom payment, ransomware attacks can have many adverse consequences, including business continuity problems, compliance issues, penalties, and reputational damage, which can translate into serious financial losses. In some cases, they can even lead to bankruptcy.

While the average cost of a ransomware attack was below $100 in 2006, it skyrocketed to an estimated $4.6 million in 2021 – a year that saw many attacks in which vast amounts of data were compromised. However, the cost can potentially run into tens of millions of dollars when all the long-term implications are also considered.

Another survey conducted with 5,400 IT decision-makers in 30 countries found that the average ransom paid by mid-sized organizations stood at about $170,000 in 2021. At the same time, the average cost of resolving a ransomware attack (including costs related to downtime, people time, device cost, network cost, lost opportunities and the ransom) stood at some $1.85 million.

The effects of ransomware attacks can include loss of customers, employees and reputation.

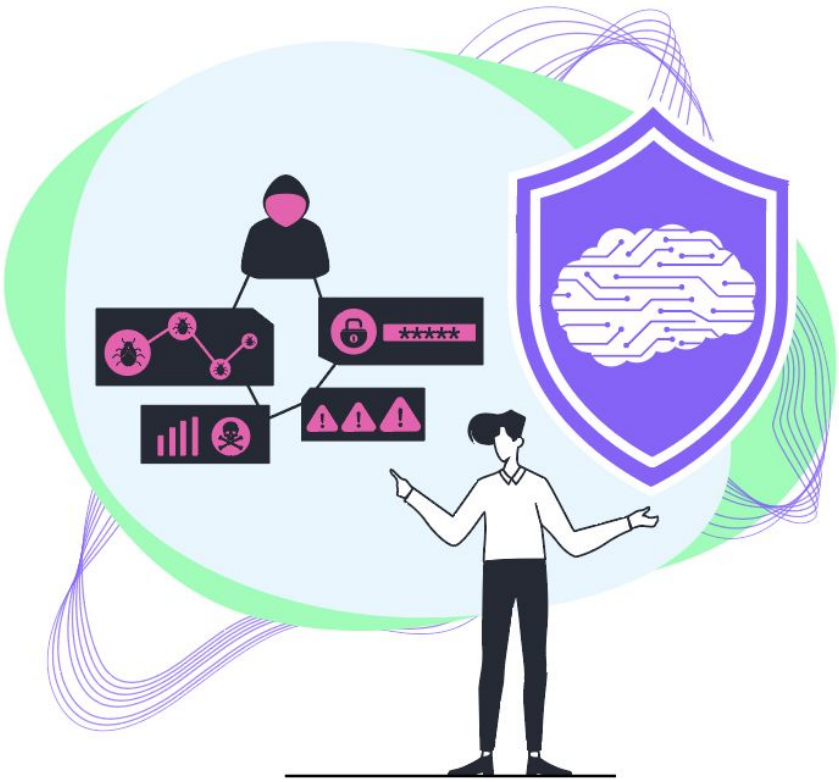
Long-term effects can include damaged brand reputation, loss of key employees, and loss of customers, clients and strategic partners (along with the cost of acquiring new ones), all of which can jeopardize an organization's viability.

© Timus Networks, Inc. 2025. All Rights Reserved.

How Timus SASE Protects Against Ransomware Attacks

Today's increasingly sophisticated cyber threats require integrated threat-prevention solutions by which traffic flows, identities, and user activities can be tracked and controlled in a coordinated manner.

Most of today's network defenses are mainly focused on the perimeter and are too soft for internal traffic. As a result, they tend to be overly permissive when allowing systems within the internal network to communicate with each other. This approach doesn't meet the needs of the modern distributed organization, where users, devices and applications are everywhere.



Zero trust is a holistic approach that assumes that no user or application should be inherently trusted. It begins with the assumption that everything in the network is hostile or compromised and that trust can only be established based on the user's identity and context. Zero trust most effectively works where security is delivered through the cloud, closer to where business assets and user activities are now centered.

Timus provides a zero trust network access platform with integrated threat-prevention engines to protect your company from potential attacks. Detailed threat visibility on the Timus platform is critical for dealing with incidents as quickly as possible.

© Timus Networks, Inc. 2025. All Rights Reserved.

Timus SASE protects against ransomware attacks in the following ways:

1. Reduce the attack surface

- Applications, user and device identities must be hidden from the outside world. They must never be visible or discoverable from the public internet.
- Never permit inbound connections to email or web servers located within a network. Once attackers can see them, they'll be able to find and exploit vulnerabilities on those machines.
- Establish "default deny" policies that allow communication only with allowed destinations.

2. Prevent initial compromise

- You should have an integrated platform like Timus that combines anti-malware, secure web gateway and intrusion prevention systems to protect your network from threats by blocking access to websites that host malicious content.
- Enforce least-privilege access controls based on the user's identity, limiting the data and functionality that can be accessed in case of a breach.
- Use a platform like Timus as a SAML identity provider to enforce granular controls over your cloud applications. An added benefit is that you'll have visibility into what's known as "shadow IT," or unsanctioned cloud app usage.

3. Block lateral movement

- Leverage a zero trust network access platform like Timus that grants access to specific applications instead of the whole network. This is the cornerstone of the micro-segmentation approach, which limits access to applications and resources so that attackers that breach a single device can't cause damage to the whole network.
- Ensure that all connections to your resources are taking place through a zero trust platform like Timus so that all traffic, regardless of user, location, or device type, adheres to all corporate policies. Timus ensures security when accessing corporate resources, regardless of whether these resources are internal, external, or third-party SaaS.
- IT monitoring is a difficult task to manage effectively. Continuous monitoring of network and user activity with Timus Intelligent Insights Engine lets you see which users are trying to access which resources on local or cloud networks. It also provides vital information on potential threats, anomalous behavior, and active security events.



© Timus Networks, Inc. 2025. All Rights Reserved.

Conclusion

Network and system security has become a hot topic of concern since the emergence of the COVID-19 pandemic. Although the pandemic has moved the world toward greater technological innovation and online collaboration, cyber threats also increased significantly. The number of malicious emails rose by some 600% during the pandemic, and that's just one way cybercriminals can infiltrate your organization's environment. Ransomware attackers are always looking for new opportunities to breach your security. These opportunities are generally afforded by new technologies and use cases like work-from-anywhere, Internet of Things (IoT), cloud computing, and Artificial Intelligence (AI).

There was 600% rise in the number of malicious emails during the pandemic.

While the techniques used by ransomware operators can be overwhelming, it is relatively easy to detect and mitigate ransomware attacks in their early stages as long as proper security controls are in place. Migrating away from legacy networking systems, moving towards zero trust cloud security platforms, and educating employees about ransomware attacks (85% of all breaches involve the human element) are other measures that should be taken.

Don't let your organization fall victim to ransomware. Timus provides a comprehensive foundation for your ransomware prevention strategy. Visit timusnetworks.com to better understand how we can protect your organization from ransomware and other cyber threats.

85% of all breaches involve the human element.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.