ManageEngine
FileAudit Plus

WHITEPAPER

Ransomware: History, anatomy, and survival tactics

www.fileauditplus.com

Contents

Ransomware: History, anatomy, and survival tactics

Introduction

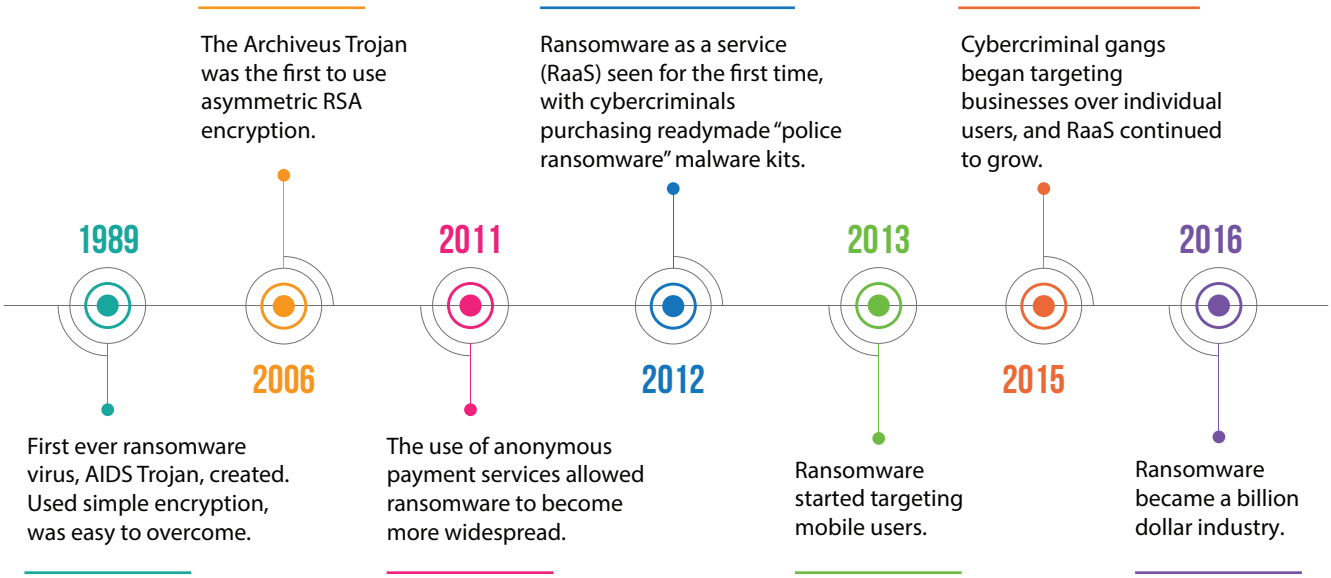
In less than a decade, ransomware—a type of malware—has catapulted itself to the top of cybercriminals' list of preferred attacks. This phenomenon is as noteworthy as it is scary, and has continued to reign supreme in the past few years. Most ransomware follows a straightforward method of operation: get onto a user's machine, encrypt all their files, then demand a ransom to decrypt their files. Although this is a simple game plan, the growing prominence of ransomware arises from constant innovation and evolution, allowing many variants to bring down entire corporate networks within minutes.

This white paper provides an all-around view of ransomware, starting with an exploration of ransomware over time, along with some expected future trends. It then examines how and why ransomware attacks occur, and whom they target. Finally, it explains the best ways for enterprises to prevent ransomware attacks, as well as how to detect and contain an attack if one does occur.

Ransomware: Its past, present, and future

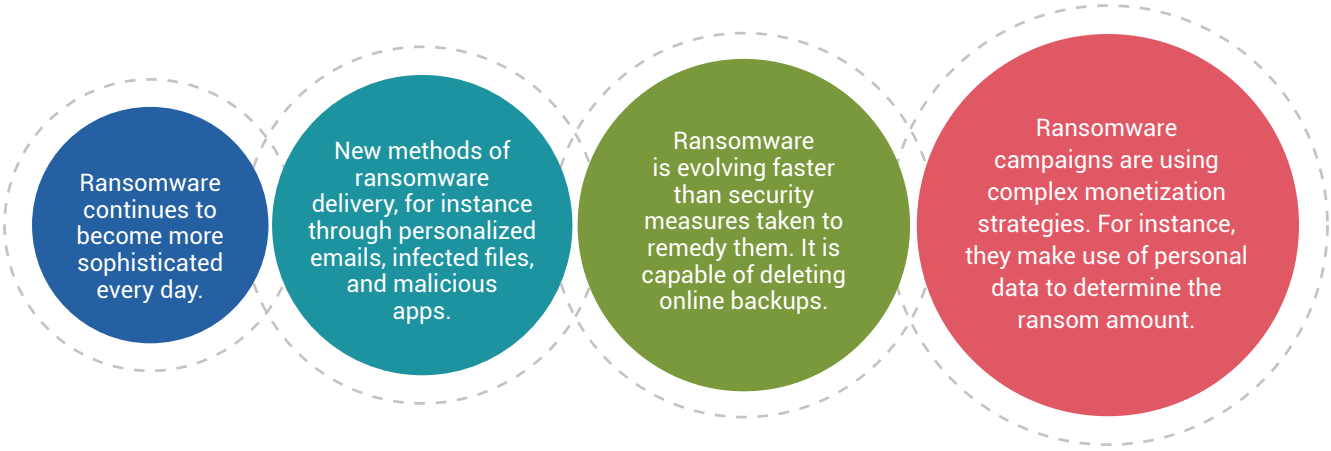
PAST

The evolution of ransomware



PRESENT

Current scenarios



FUTURE

The future of ransomware

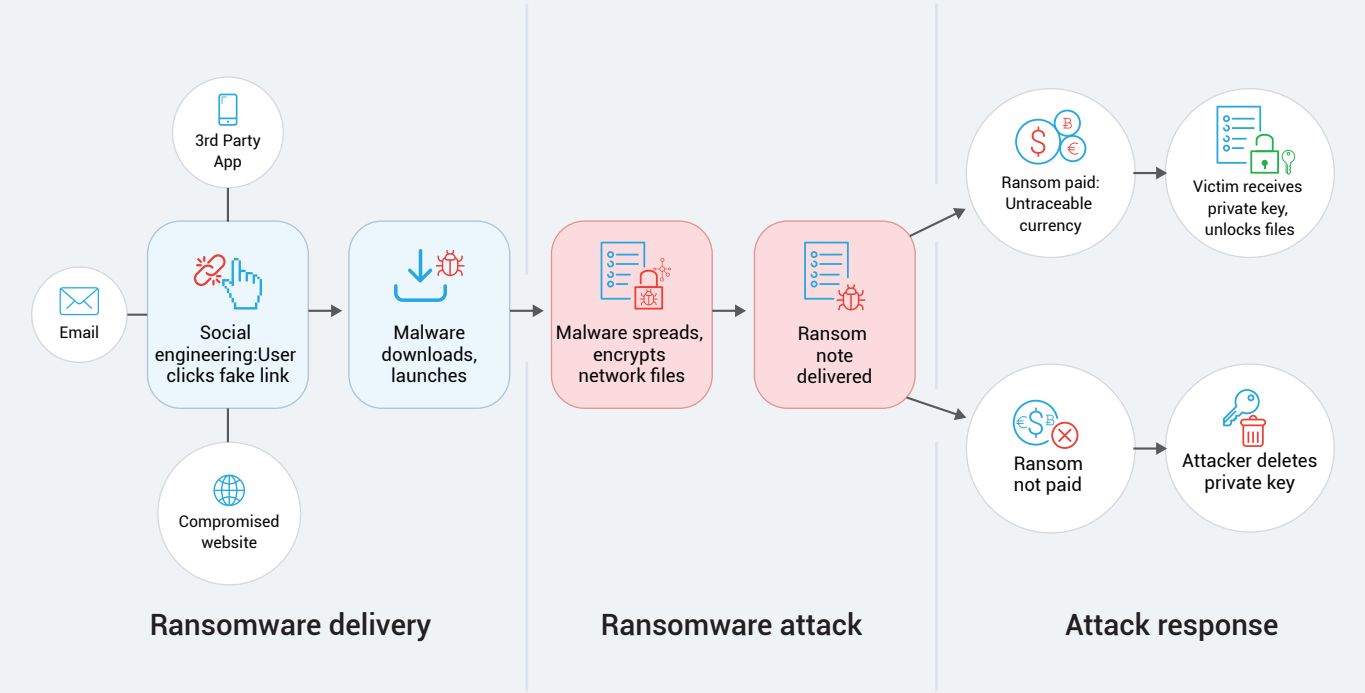
- Ransomware will continue to be cybercriminals' most preferred attack method.
- RaaS will continue to rise, and new types of ransomware may become scarcer.
- There will be an increase in targeted attacks, with individuals with high net worth being high risk targets.
- Internet of things (IoT) devices will be increasingly vulnerable to ransomware. They may be locked down, or their data may be stolen outright.

Ransomware overview

To fully understand ransomware attacks, it's important to familiarize yourself with the building blocks of ransomware attacks, as well as related elements surrounding an attack, such as why attackers prefer ransomware, and whom ransomware targets.

How does ransomware work?

The below diagram depicts the anatomy of a ransomware attack:



Ransomware delivery:

Most ransomware attacks begin with some form of social engineering, where a user is tricked into clicking a malicious attachment or link that contains the malware. These attacks can come in the form of an email, an ad or link on a compromised website, third-party mobile apps, or even malicious macros within other files.

A technique often used today is to customize the content of these emails or webpages with stolen personal information, in order to trick users into downloading the ransomware. Many ransomware files are also disguised as other types of content in an effort to get onto a user's system.

An even scarier trend is how some ransomware files get installed in a background download, without the user's knowledge. In these cases, a visit to a compromised website is sufficient to load ransomware onto a system, and doesn't even require the user to explicitly click on a link. Once the malware is on a system, it automatically launches and the ransomware attack begins.

Ransomware attack:

Once ransomware infects a system, it searches for all the files on that system or all the files of a specific type that it is going to encrypt. This can include files stored on shared folders within a local network—if the infected system has direct access to a corporate file sever, all of an enterprise's data could become encrypted.

Notably, WannaCry and Petya used the EternalBlue network exploit to propagate themselves across systems. In the future, more self-propagating variants are likely to pop up, in an effort to catch as many victims as possible. Self-propagating ransomware allows large portions of an enterprise's network to be brought to a standstill, which increases the odds that the ransom will be paid.

Most ransomware tends to use a combination of symmetric and asymmetric encryption. Asymmetric encryption alone takes too much time, so the files are encrypted using a simpler, symmetric encryption—which generates a random key. This key is then encrypted using an asymmetric method, which uses another private key specific to the victim.

Once ransomware finishes encrypting the files on an infected system, it displays a message demanding ransom. The creators of ransomware typically ask for the ransom to be paid using some digital form of payment. The requested payment method will either be untraceable (such as gift cards or certain cryptocurrencies) or difficult to trace, like Bitcoin (which has been preferred in recent years).

Attack response:

Along with the ransom demand comes instructions on how to pay the ransom and unlock the data. An attack victim has to choose whether to pay the ransom or not. If the victim does not pay the ransom within a stipulated time, the private key needed to decrypt the data is destroyed (either manually by the attacker or

automatically by the ransomware). Without the private key needed to decrypt the data, that data is essentially lost forever. Some ransomware attacks provide an additional time window to pay the ransom, after steeply increasing the ransom amount.

If the victim does pay, the attacker might send them their private key, which they can use to unlock their files. Sadly, there have been plenty of cases where victims pay the ransom but never receive a key to retrieve their data. What's more, paying a ransom may incentivize attackers to develop more ransomware.

More so than relying on chance and hoping an attacker releases a key to decrypt data, recovering data from backup is the best remedy for ransomware. However, if no recent backup is available, many victims choose to pay the ransom despite knowing the risks, in order to have some hope of regaining access to fresh files.

Why do attackers prefer ransomware?

There are several reasons which make ransomware a highly attractive option to attackers:

Number of potential victims:

A well-designed social engineering attack can result in thousands of initial victims. Furthermore, with propagating ransomware variants, each infected system spreading ransomware to other systems, attackers can expect an exponential rise in the number of victims within the first few days.

A Kaspersky survey reported that 42 percent of small and medium-sized businesses were hit by ransomware in 2016. *Source: Kaspersky Security Bulletin, 2016*

High chances of ransom payout:

Data is a highly valuable asset. Especially in the case of business victims, even a day of downtime can prove costly. Combined with compliance concerns, companies tend to look for the quickest resolution possible. This often means they'll choose to pay the ransom rather than face any downtime or the potential blow-out from a data breach.

Low risk of getting caught:

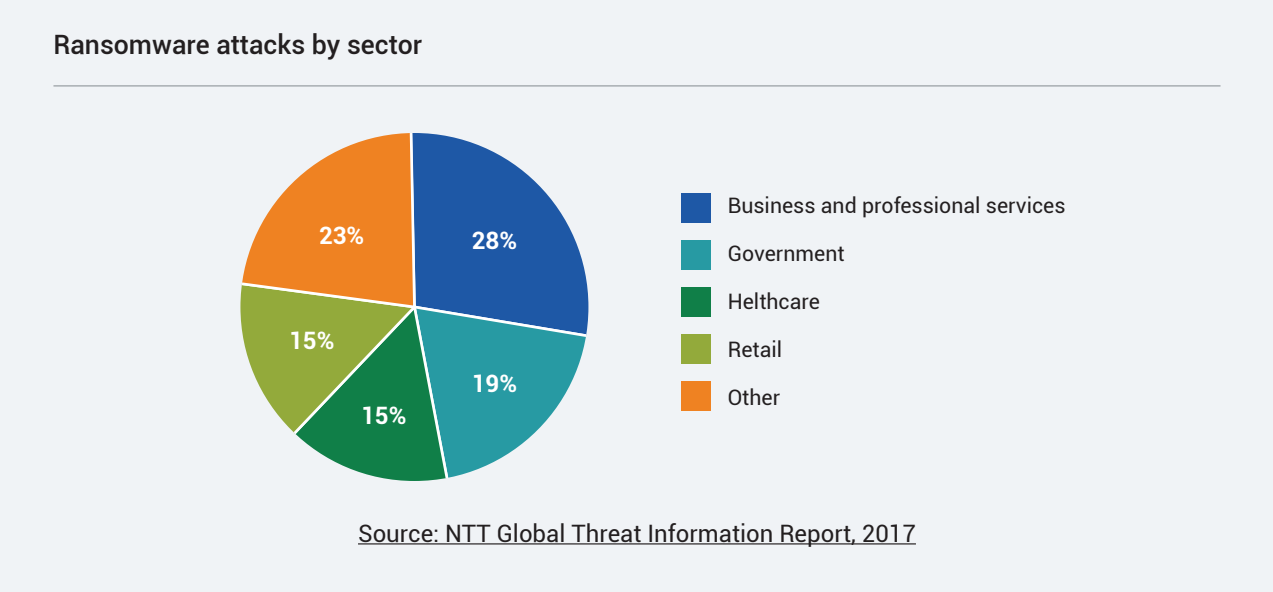
Once a ransomware attack is completed, it is practically impossible to decrypt the files without the corresponding key. The key is only in the attacker's possession (there aren't duplicates) and is delivered to a victim only after they pay the ransom. Since many payments are made using untraceable methods, it is impossible to track the attackers. Many ransomware victims don't even involve the authorities due to the reasons mentioned in this and the previous point. All in all, there is very low risk involved for the attacker.

Low effort required:

It remains relatively easy to launch a ransomware attack today. Ransomware awareness is still catching up at the individual employee level, with several network vulnerabilities left unpatched. Further, the advent of ransomware as a service has enabled even novice attackers to set up complicated and widespread ransomware attacks with ease and quickly reap the benefits.

All of these factors make ransomware a highly lucrative business model for cybercriminals and therefore continues to remain prevalent.

Who does ransomware target?



Source: NTT Global Threat Information Report, 2017

Simply put, all mobile and desktop devices can be affected by ransomware, which makes everyone a potential target. In the early days of ransomware development, social engineering attacks were random and blindly targeted anyone they could reach. Soon after that, they started targeting more corporate users, with small and medium businesses facing these attacks more often before large enterprises started falling prey to them as well.

Overall, as ransomware attacks have become more sophisticated, a larger proportion of attacks have targeted specific sectors, companies, or even selected individuals with high net worths. Those with a higher potential to be targeted by ransomware attacks are characterized by:

- **High value data**
- **Potential for large downtime costs**
- **Lax security measures**
- **Low awareness among employees**

An NTT Security report from 2017 noted that 77 percent of ransomware attacks were found among four sectors: 28 percent were encountered in the business and professional services sector, 19 percent in the government sector, 15 percent in the healthcare sector, and 15 percent in the retail sector. The diversity among these industries highlights the need for better preparedness and security measures against ransomware across all industries.

By the first quarter of 2017, phishing emails carrying ransomware dropped by almost 50 percent, implying that criminals may be turning to other delivery methods.
Source: Proofpoint Threat Report, 2017

Ransomware prevention best practices

Without a key, encryption is basically permanent, making prevention truly the best defense against ransomware. Preventing ransomware involves some very simple practices, the importance of which are—surprisingly—still not widely appreciated among enterprises. These practices are:

- **Educate end users:**
  Regularly train your employees on how to identify and avoid common ransomware pitfalls such as malvertisements or phishing emails. The training needs to be rigorous, as even the most discerning user can fall prey to well designed ransomware bait. Just a single employee's mistake can bring down a large enterprise.

- **Patch vulnerabilities:**
  Companies can go years without patching known vulnerabilities in their systems. This is far from ideal, since criminals know how to use these vulnerabilities to their maximum advantage. Prioritizing patches for network vulnerabilities and regularly updating your operating system, browsers, and other applications will all play an important role in securing your network.

- **Use an intrusion detection system:**
  Have a system in place to detect ransomware attacks in their early stages and stop them in their tracks. Use one of the available solutions to continuously monitor your network and detect signs of anomalous or malicious activity in real time. These solutions can then launch an automated response to stop ransomware from spreading. This is highlighted in the next section.

- **Employ email filtering:**
  Email is one of the most common routes for ransomware to hit any network. Use strong spam filters to detect and block malicious executables, phishing emails, and other methods ransomware is known to use. Along with employee training, this helps prevent ransomware from being downloaded altogether.

- **Whitelist applications:**
  Strictly monitor the download and use of third-party software. Adding acceptable software to your whitelist can help block unauthorized programs from running. If a program containing malware isn't whitelisted, it can't be downloaded onto your network.

- **Provide the least amount of privilege possible:**
  Organizations often provide more access rights to their employees than is needed, for the sake of convenience. This way, things don't have to slow down if and when users require extra permissions during the course of their work. The downside of this is an automatic increase to the potential attack surface for any ransomware attack. Instead, use robust access management to restrict unwarranted access and reduce the number of access points through which malware can enter and spread through your organization.

- **Logically separate networks:**
  Separate various parts of your network, say by department or function, to help control the spread of ransomware. This helps reduce the magnitude of data loss and reduces the cost incurred in the event of an attack.

If any of these prevention strategies fail, the best remedy for ransomware is to just restore the infected system from backup. A strong backup policy guarantees that you always have a recent copy of your data to fall back on. Ensure that you test these backups as well, or you may discover you are unable to recover your data. The popular 3-2-1 backup strategy is a good rule of thumb to use when backing up your data: always have at least 3 copies of your data, use 2 different storage types, and store at least 1 copy off-site. Following this rule helps fight ransomware variants that can delete backups stored online.

Ransomware detection and response

Prevention practices go a long way in keeping ransomware away from your data, but it is important to be prepared for an attack, as attackers discover new ways to infiltrate networks every day. There are several solutions available to fight ransomware, so it is important that you select a solution that can:

- **Work in real time:**
  The time between a ransomware attack striking your network and finishing file encryption is the best—and possibly only—chance you have to fight the attack and contain its damage. Considering most ransomware attacks take only a few minutes to complete, you'll need a solution that responds in real time.

- **Detect ransomware accurately:**
  Some solutions identify ransomware by detecting activity typical of ransomware programs. Once they do, they'll send out real-time alerts. The option to adjust the parameters of these alerts using filters can help improve the accuracy of the alerts.

- **Launch automated responses:**
  Since the response window for ransomware is very short, a manual response will typically not be quick enough. Ransomware solutions should therefore launch an automated response when an attack is suspected. For instance, immediately shutting down the infected system can help stop the spread of ransomware to other devices on your network.

- **Provide detailed analysis:**
  Any attempted ransomware attack can provide a look into possible vulnerabilities in your network. It is important for ransomware solutions to aid in attack analysis, so you can understand how it happened and take steps to prevent the same scenario from occurring in the future.

Using a file server auditing solution to monitor your files in real-time is an ideal way to protect them from ransomware attacks. When these solutions detect a large number of files being modified in a short time frame, they send out real-time notifications, launch an appropriate automated response, and provide you detailed reports that help you gain insights into how the attack occurred.

About FileAudit Plus

FileAudit Plus is real-time Windows file server auditing and analysis software that tracks, monitors, and reports on all accesses and modifications made to your file server environment. It provides detailed analysis on file storage, helps you meet multiple compliance requirements, and generates instant, user-defined email alerts while carrying out automatic predefined responses when potential security threats occur. Its key features include:

- **File access auditing:** Obtain detailed information on the quintessential four W's—who accessed what, when, and from where—for all file and folder access.
- **Storage analyzer:** Analyze storage space to gain critical insights into unstructured data and identify old, stale, or hidden files.
- **Ransomware detection:** Thwart security threats right at their inception using our automated response mechanism and user-defined, instantaneous alerts.
- **File permissions monitoring:** Gain visibility into all file share permissions and generate real-time alerts that signal permission changes made to your sensitive files.
- **File integrity monitoring:** Prevent unauthorized changes to your file server environment through continuous real-time monitoring.
- **Compliance reports:** Ensure compliance with multiple external regulatory standards such as PCI DSS, HIPAA, FISMA, GDPR, SOX, and GLBA.

$ Get Quote Download

Toll Free
+1 844 245 1101

Direct Dialing Number
US : +1-408-916-9891

support@fileauditplus.com

www.fileauditplus.com