UNMASKING RANSOMWARE

Why it Exists, How it Works, and How K7 Security Protects You

K7 SECURITY

Contents

Executive Summary

Ransomware is the world's most alarming digital menace. It is the cyber attacker's weapon of choice that can rapidly spread across the world and bring major cities to a standstill. Ransomware attacks do not discriminate between home users and large organisations, or between platforms or devices. Everyone everywhere is vulnerable to ransomware.

The rise of relatively anonymous cryptocurrency has made ransomware attacks easy to monetise, and ransom demands are rising. A university and a web hosting firm paid over **$1 million each** to recover access to their data. Higher ransoms may have been paid but not publicly disclosed. A recent ransomware attack on the world's largest electronics manufacturer was accompanied by a **$34 million** ransom demand. The recovery cost imposed by the attack can be very steep as well; an American city was expected to incur a cost of **$18 million** following a ransomware attack and the world's largest shipping company suffered a **$300 million** loss due to ransomware.

A cyber threat of such magnitude poses an existential threat to any organisation and necessitates the creation and maintenance of strong cyber defences. This whitepaper has been prepared based on K7 Security's extensive experience and proven results in helping companies operating in diverse industries defend their operations against ransomware. Topics discussed include

- Factors that contribute to the increase in ransomware attacks
- The consequences that follow ransomware attacks
- Ransomware on different platforms
- How ransomware spreads
- How ransomware can be prevented

We conclude this whitepaper with a detailed discussion on the features and technology in K7 Security's solutions that protect organisations against ransomware.

Introduction

An entire city scrambles to protect itself from malware. It doesn't seem possible for a computer virus to bring an entire city to its knees, outside of a science fiction movie, but that's what the SamSam virus did to the city of Atlanta in the USA.

The attack on Atlanta was carried out by ransomware – a form of cyber attack where victims are prevented from accessing their own data, usually by locking the device or encrypting the data on the device, and have to pay a ransom to the attacker to regain access to their data.

Ransomware is clearly a very alarming threat. Any cyber assault that can disrupt a large, modern city is not to be taken lightly and can have very severe consequences for individuals, businesses, and governments.

Types of Ransomware

Ransomware can be classified into two categories based on what it attempts to encrypt:

1. **Traditional Ransomware** – Data on the device is encrypted and a ransom is demanded to restore data access

2. **MBR Ransomware** – The Master Boot Record (MBR) is encrypted to prevent the operating system from loading and a ransom is demanded to allow the device to boot. The device needs to be restarted (the malware will usually attempt to force a restart) for the ransomware to take hold of the device

Both types of ransomware deploy malware on the device that acts to prevent the victim from accessing their data. Ransomware attacks can spread through software vulnerabilities, phishing, bogus updates, compromised RDP sessions, and even drive-by downloads; they may or may not need human intervention to infect devices or propagate.

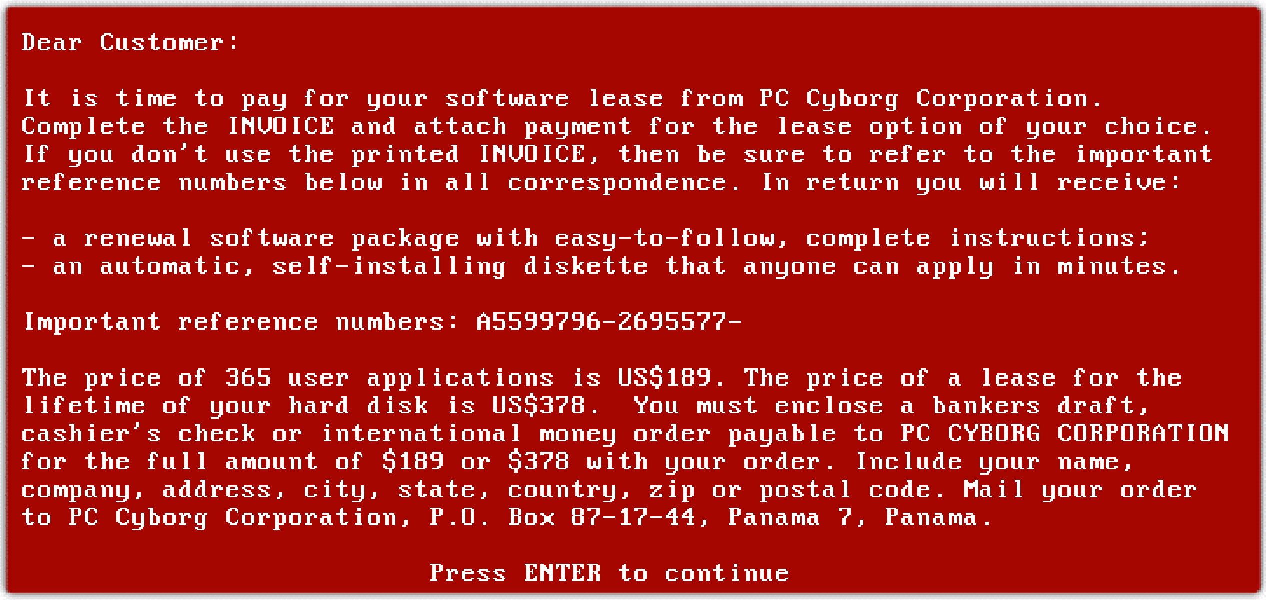
Ransom DDoS

Threat actors have now begun to launch Distributed Denial of Service (DDoS) attacks against an organisation and demand a ransom to call off the attack. These attacks are monetised like ransomware attacks and can be just as devastating to an organisation (e.g., a ransom DDoS attack against an e-commerce website during a festival shopping season can affect a significant portion of its annual revenue) but they are not ransomware attacks as they originate, deploy, and function entirely outside the organisation and do not involve a malware component inside the victim's IT infrastructure.

Ransom DDoS attacks are conventional DDoS attacks with an associated ransom demand. This whitepaper does not examine such attacks.

The History of Ransomware

Ransomware is at least 30 years old. The first recorded instance was in 1989 when Dr. Joseph Popp, an evolutionary biologist and WHO consultant, unleashed the AIDS Trojan by mailing floppy disks called 'AIDS Information Introductory Diskette' which contained the malware, and asked victims to send $189 to a post office box in Panama.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```

Figure 1: AIDS Trojan Payment Notice. Image Source: Wikipedia

Dr. Popp claimed that he created the ransomware to raise funds for AIDS research. His Trojan was not very sophisticated and the encryption could be reversed without payment. We cannot say the same about modern ransomware: they are not created with such noble motives, and decryption may be impossible. Effective prevention is therefore better than attempting a cure.

The Business of Ransomware

Ransomware is financially motivated cyber crime but its business model is different from other cyber attacks. Conventional data theft is motivated by the value of the data to others – the hacker wishes to sell the information on the dark web to other criminals. Therefore such attacks are aimed at organisations that have data that is valuable to others. Medical records and credit card information make hospitals and large businesses popular targets.

Ransomware, on the other hand, doesn't require the data to have value to a third party; it only needs the data to have value to the victim. Since just about every digital device user has data that is of some value to them, even if it is just photographs of special moments, it makes every digital user and service a potentially profitable target for a ransomware attack.

Why Ransomware Attacks Are Increasing

Ransomware attacks are rapidly increasing because of 3 factors:

1. Incentive
2. Opportunity
3. Availability

Incentive

We have already discussed the incentive for ransomware – everyone has data that is valuable, at least to themselves. Threat actors have now discovered an additional incentive to launch ransomware attacks: they threaten to release the victim's data if the ransom is not paid. This increases the probability that the ransom will be paid even if the victim organisation can recover from the ransomware attack without a decryption key (by restoring data backups) due to the fear of a data breach.

Opportunity

There are 3 factors that that drive ransomware opportunity:

1. **Data Explosion** – The growth in mobile devices and affordable internet had led to a staggering growth in digital services and data generated. eTaal estimates more than 64 Billion e-transactions in India in 2020 – and this is just transactions; the number will go much higher when combined with other digital records. Internationally, 234,000 photos are uploaded to Facebook and 500 minutes of video to YouTube every minute. The more data that is generated, the greater the ransomware opportunity

2. **24/7 Connectivity** – Mobile phones have affordable and fast mobile internet connectivity and wired broadband networks' speed and availability keep increasing, which helps the propagation of cyberthreats. The WannaCry ransomware took just 4 days to spread across 116 countries

3. **Cryptocurrency** – Ransomware depends on the payment of ransom through digital fund transfer. Conventional electronic payments are highly traceable but cryptocurrency transactions have greater anonymity and privacy, which enables the monetisation of ransomware

The imminent 5G rollout and the increasing adoption of IoT in commercial applications and in our daily lives will increase the volume, variety, and velocity of data, thereby increasing the incentive and opportunity for ransomware.

Availability

Ransomware creators have now joined the SaaS world and provide Ransomware-as-a-Service (RaaS) that allow criminals with limited technical knowledge to launch sophisticated attacks. RaaS offerings mimic legitimate SaaS offerings and even offer convenient dashboards to monitor attacks, and are advertised on the dark web much like legal software is advertised on the surface web.

The separation of ransomware creator and ransomware attacker roles has resulted in an increase in ransomware attacks due to the division of labour: legitimate businesses have profited from the benefits of specialisation that follow the division of labour, and illicit businesses are now adopting similar practices.

The Consequences of Ransomware

Ransomware has a direct impact on infected devices, rendering them unusable. It also has an indirect impact where other devices, and even networks, have to be shut down to prevent the spread of ransomware. This implies that all the operations at a facility may come to a standstill in the event of a ransomware attack, with severe consequences on an organisation's profitability and reputation.

Cyber attacks are usually associated with the loss of time, energy, money, and data but not life. That changed when a hospital in Germany was crippled by a ransomware attack and was forced to redirect a patient to another hospital, with the delay in treatment leading to her death. Healthcare facilities are often targeted by threat actors precisely because such consequences are possible, making them more likely to pay the ransom quickly.

Ransomware can cripple city and state administration. The American cities of Atlanta and Baltimore were both severely affected by ransomware, with Baltimore estimated to incur a cost of $18.2 million due to the attack. The state of Colorado declared a state emergency following a ransomware attack.

Global shipping giant A.P. Moller - Maersk, representing almost a fifth of the world's shipping capacity, estimated a $300 million loss from the NotPetya ransomware attack and had to reinstall 4,000 servers, 45,000 PCs, and 2,500 applications in ten days and fly a hard disk from Ghana to London to recover from the attack.

In India, operations at one of the terminals of the Jawaharlal Nehru Port Trust that handles 4,500 containers per day were disrupted by the NotPetya ransomware, and WannaCry affected the corporate affairs ministry's MCA21 portal and the Andhra Pradesh police.

Who Can Be Attacked By Ransomware?

We have listed prominent ransomware attacks that affected large entities, but that does not mean that only large organisations are the target of ransomware attacks. We have already discussed why a successful ransomware attack only requires the data to have value to the victim, and therefore any organisation can be targeted by ransomware.

A hotel in Austria paid about €1,600 in ransom and moved back to traditional locks after a ransomware attack crippled the hotel's smart locks and prevented guests from entering their rooms. A small town of just 12,000 in the US paid $460,000 to regain control of its systems.

The size or prominence of the organisation does not affect the probability of a ransomware attack. Any organisation, and even individuals, can be attacked by ransomware.

Do Some Platforms Escape Ransomware Attacks?

Canon issued a firmware update to prevent ransomware infection in its DSLRs, which could be potentially used to extort ransom from news and event photographers. No platform is safe if even a camera's firmware is vulnerable. Any of the common operating systems we are likely to use can be attacked by ransomware.

Windows

Windows is one of the most used operating systems in the world, especially in the enterprise space, and consequently many ransomware variants target Windows. Both the WannCry and NotPetya ransomware spread through a vulnerability in Windows but they only affected unpatched Windows systems. Microsoft had already discovered the vulnerability and released a patch but many users and organisations had not installed the patch, allowing the ransomware to spread and cause havoc across the world.

Mac

Macs may not challenge Windows for market share, but they are not immune to ransomware. K7 Labs was the first discoverer of the EvilQuest ransomware that specifically targeted devices running macOS.

Android

Android is as ubiquitous in the mobile world as Windows is for desktops, and has been targeted by ransomware for several years now. Some Android ransomware now even include machine learning to tailor the attack to the victim's device. The widespread use of Android and the large number of Android devices that either do not receive updates or receive very few updates from the OEM imply that ransomware on Android devices is likely to increase. It should be noted that Android is not limited to mobile devices and smart TVs have also been attacked by ransomware.

iOS

iOS devices are targeted by crude extortion attempts that are more scareware than ransomware, but such ransom-demanding attacks do exist. Similar to many forms of Android ransomware, these attacks do not encrypt data on the device but merely prevent access to some device functionality and require payment to restore access.

Linux

Linux's desktop market share is miniscule even when compared to macOS, but it has a significant presence in the server market which makes it an attractive target for malware developers who have created several ransomware variants for Linux-based operating systems.

Should You Pay The Ransom?

No. It is tempting to pay the ransom and restore normal operations quickly to stem the haemorrhage of funds and customers that follows a crippling cyberattack. Insurance against ransomware attacks is also being offered to meet the cost of paying the ransom. However, paying the ransom is a counterproductive strategy because

- **The attacker may not release the decryption key** – There is no guarantee that the attacker will provide a decryption key to unlock the data encrypted by ransomware once the ransom is paid. In fact, there is no guarantee that the attacker even has a decryption key or is in a position to send you the key if they have it

- **Paying the ransom indicates that you are a lucrative target** – The hotel that had its locks crippled by ransomware did pay a ransom, but suffered 4 ransomware attacks in 2 months. An American hospital paid the ransom but the attacker then demanded more ransom. Paying the ransom informs the attacker that they can monetise attacks against you, and they will try again

- **Paying the ransom increases ransomware development and attacks** – When threat actors make money from ransomware, it incentives them to develop more ransomware and launch more ransomware attacks across the world which makes countering ransomware more difficult and expensive

Penalties Against Ransomware Payments

The US Department of the Treasury has issued an advisory against paying ransom to threat actors or their associates who have links to sanctioned entities or regions and may levy penalties for violations. India does not have such penalties yet, but they may be imposed in future as we also wish to avoid adversaries funding their attacks on Indians though attacks on Indians. Indian organisations with American customers may also fall under American jurisdiction with respect to their operations there and will wish to avoid such penalties.

We have established that paying a ransom to a threat actor is not advisable. We will now discuss other, more effective measures you can pursue against ransomware attacks.

Stopping Ransomware

Since avoiding ransomware is better than paying a ransom, we must first understand how ransomware spreads to be able to develop effective countermeasures.

How Ransomware Spreads

With Human Intervention

Through Trojans that are distributed through email, phishing, USB devices, and compromised software

Without Human Intervention

Through vulnerabilities present in computer systems and networks

With Human Intervention

This requires a user to perform an action that downloads a Trojan and activates its payload. This may include

- Opening a malicious attachment from a trusted sender whose email account has been compromised
- Clicking on a malicious link in a phishing email or message (chat/social media)
- Using an infected USB storage device
- Enabling Remote Desktop Protocol without adequate precautions
- Using pirated software

- Clicking on malicious advertisements
- Visiting malicious websites

These actions are usually performed inadvertently but they may also be performed deliberately by a disgruntled employee.

Without Human Intervention

Once an attack is initialised, ransomware may spread across an organisation through the corporate network, and across organisations and even continents without human intervention. WannaCry and NotPetya, two of the largest ransomware attacks of all time, both spread without interaction with users.

Preventing Ransomware

We can avoid ransomware attacks by countering how they spread with and without human intervention. This requires a defense-in-depth approach, including

Policy Initiatives	Technology Solutions	Training and Awareness
To specify cybersecurity goals and the means to achieve them	To protect devices and networks	To protect users

Policy Initiatives

A cyber security policy defines what the cyber secure organisation looks like, and the roles, responsibilities, standards, requirements, permitted use, and penalties required to implement that vision. This is essential for closing the many doors that a threat actor can use to infiltrate your organisation, such as lax password hygiene. Your policy should address:

Roles & Responsibilities	Permitted Use	Standards	Lifecycle Management	Penalties
Who does What and When, and who is responsible for enforcement	How organisational IT assets may be used	Cyber security standards such as password strength and encryption technologies	Hardware, Software, and User lifecycle management	Penalties for non-compliance

Roles & Responsibilities

Any form of access to your organisation's IT infrastructure has to be regulated. Ransomware can easily take hold in and spread through an organisation where many users have administrative privileges. Therefore the cyber security policy should lay down guidelines for determining user roles and privileges and stipulate how such access is monitored. A maker-checker-approver system should be followed and Identity and Access Management solutions can be utilised to prevent inappropriate access being granted and abuse of access legitimately obtained.

The cyber security policy should also define a hierarchy of responsibilities at different organisational levels to ensure that the cyber security policy is enforced in day-to-day operations.

Permitted Use

Plugging in an infected USB drive, or visiting a drive-by download-enabled attack site, may be all it takes to cripple your operations. Therefore, regulating permitted use is important to preventing ransomware infections. Specifically, every user should have the least privileges required to carry out their responsibilities. Some senior personnel may require greater latitude in permitted use but no one should have unfettered privileges as ransomware does not care if it is an intern or a CEO who is visiting the malicious site, and therefore some security measures will need to apply equally to everyone.

Standards

The policy should define the cyber security standards of the organisation. These can include password strength, multi-factor authentication, cyber security requirements in procurement of hardware and software, and infrastructure segmentation. The Assessing Security Requirements for Controlled Unclassified Information document published by National Institutes of Standards and Technology (NIST) can be utilised as a starting point to determine the controls and safeguards appropriate for your institution.

Lifecycle Management

Every device, application, and user has a lifecycle in the context of your organisation that needs to be managed to ensure that entry, implementation, or access does not compromise cyber security. This should specifically include

- **Hardware Lifecycle Management** – Firmware in hardware can be compromised to deliver ransomware. The manufacturer's commitment to providing frequent security updates should be confirmed before procuring hardware

- **Software Lifecycle Management** – Similar to hardware lifecycle management, the provision of frequent security updates and patches should be considered when procuring software

- **User Lifecycle Managemen**t – Former employees' data and network access privileges should be revoked immediately on exit and current employees should be granted access based on the principle of least privilege to prevent both inadvertent and intentional ransomware infections

Penalties

The cyber security policy will merely exist on paper unless there is a mechanism to enforce it and ensure compliance. This necessarily requires penalties both for non-compliance on the part of users and non-enforcement on the part of leaders. Your organisation can decide on appropriate penalties for your users based on the consequences that may result from non-compliance, but strict enforcement of penalties are essential to encourage compliance. We have earlier discussed how highly destructive ransomware spread across the world through unpatched Windows machines. It is tragic that the simple and easy precaution of applying patches as soon as they become available was not followed by so many organisations. Penalties ensure that your organisation is not one of them.

The use of Remote Desktop Protocol (RDP) is a critical area where the cyber security policy can have a significant impact on preventing ransomware attacks. Threat actors exploit vulnerabilities in RDP implementation to gain remote access to an organisation's endpoints, from where they can launch and spread ransomware. The cyber security policy should regulate the circumstances under which remote access can be granted, the standards to be followed (such as password strength and avoiding default ports), revocation of remote access privileges as soon as they are no longer required, and penalties for non-compliance.

Technology Solutions

Digital technology has 2 facets, in the context of ransomware, and both should be secured against attacks.

Endpoint Protection

Protection of computing devices

Network Protection

Protection of networks, networking devices, and networked devices

Endpoint Protection

Endpoints (desktops, laptops, and servers) are used by employees to carry out responsibilities or facilitate business operations. The wide variety of tasks and tools associated with endpoints create many opportunities for threat actors to launch attacks. Enterprise endpoint security, like K7 Endpoint Security, will protect endpoints by countering many of the ways ransomware spreads that we previously discussed.

Ransomware Vector	Endpoint Protection
Malicious attachment	All email attachments are automatically scanned for threats before they are opened
Phishing email	Malicious links in phishing emails are blocked
Infected USB storage device	USB storage devices can be blocked, or automatically scanned for malware when connected
Pirated software	Installation of unauthorised applications can be blocked
Malicious websites	Unsafe websites can be identified and blocked

In addition to protection against ransomware propagation methods, endpoint protection systems can provide direct protection against ransomware that makes its way to an endpoint. We will examine such direct protection later in this whitepaper under the discussion on how K7 Security protects against ransomware.

It is critical to note here that every device that accesses the organisation's network or data must be protected, including equipment that is leased or belongs to a vendor. We have referred to Colorado declaring a state emergency following a ransomware attack. The attack occurred because a temporary server was installed for testing without being provisioned for security because it was temporary. Attackers discovered the server immediately and were able to guess its password through 40,000 attempts because it permitted unlimited failed logins. One unsecured endpoint resulted in recovery expenditure of $1.7 million. The lesson from this incident is clear: the entire organisation is at risk if even a single device is left unsecured for a short duration of time.

Network Protection

Ransomware can enter an organisation by compromising a networking device, or use the network to spread across endpoints without requiring networking devices to be compromised.

Compromising Networking Devices

Networking devices can be compromised by

- **Exploiting Vulnerabilities** – Firmware in a networking device may contain vulnerabilities that allow a threat actor to perform remote code execution and deploy ransomware. Your organisation can protect against such vulnerabilities by
    - Procuring networking devices from OEMs that provide patches and security updates through the lifetime of the product
    - Applying such patches and updates as soon as they become available. This requires maintaining an inventory of networking devices and their patch/update status
    - Upgrading networking devices as soon as they reach end-of-support even if their networking capabilities are unimpaired
- **Exploiting Insecure Configuration** – Networking devices that use default credentials or otherwise violate security best practices can be compromised by an attacker. Secure configuration is device-specific and such configuration should be performed in consultation with the vendor or with experts familiar with the device

It should be noted that many devices used in commercial and industrial establishments are not computing devices but are still networked (often identified as smart or IoT devices). These devices can be compromised like networking devices and require similar protection against exploits and insecure configuration.

Using the Network to Spread Malware

Threat actors do not need to compromise networking devices to affect an organisation, and may instead use the network to spread the ransomware to all the devices connected to the network (similar to how legitimate files are shared across devices on a network), compromising the devices but not the network. This can be prevented through

- **Gateway Security** – Gateway security appliances, like K7's Next Generation Firewall solutions, include a hardware firewall with Intrusion Detection System/Intrusion Prevention System (IDS/IPS) that guards against attempts to penetrate the network and gain access to endpoints
- **Segmentation** – Network segmentation effectively creates multiple internal networks. This hinders the lateral movement of ransomware through the organisation and reduces the possibility that a single compromised endpoint allocated to a minor task, or a guest being granted network access, can be used to launch an attack against the entire organisation. Networks can be segmented using K7's Next Generation Firewall solutions

Do Data Backups Form Effective Protection?

Data backups are a necessary measure to protect against ransomware attacks, because operational capacity can be regained by restoring a backup. However, data backups cannot be considered the primary defence against ransomware because

- **The backup may also be infected** – Ransomware can encrypt your backed up data as well, rendering the backup useless

- **Data restoration requires resources** – Restoring data from a backup for a large organisation requires time and effort, and has a financial cost associated with it as well

- **Attackers threaten to release data** – As mentioned in the discussion on attackers' incentives, threat actors exfiltrate data in addition to encrypting it and threaten to release the data if the ransom isn't paid

The last is particularly alarming as there is no guarantee that the attacker will not release the stolen data in future if the ransom is paid, and can repeatedly extort money from the victim who will wish to avoid the penalties and brand erosion that will result if the data is released. Preventing a ransomware attack, rather than relying on a data backup, is the prudent and advisable course of action.

Training and Awareness

Threat actors are aware that organisations utilise technology solutions to stop attacks against devices and networks, and have responded with social engineering attacks such as phishing that target the user instead. It is estimated that 91% of all attacks begin with phishing. While technology can act as a secondary defence against some social engineering attacks, a well informed user remains the primary defence.

Cyber security training requirements will vary within your organisation as roles, responsibilities, and access to sensitive resources expose users to different levels of risk. However, all staff should be trained on the fundamentals of cyber hygiene, including

- Creating strong passwords that are not reused, recycled, or shared
- Ensuring physical security of IT assets
- Identifying phishing attacks
- Verifying the bona fides of a message or sender
- Exercising caution before opening an attachment or clicking a link
- Precautions to be followed on mobile devices
- Essentials of network security for those who might need to work from home
- Whom to contact if a cyber attack is noticed

Creating a culture of cyber security in your organisation is necessary to prevent continuously evolving ransomware attacks and therefore training should not be a one-time event. Cyber security tips and reminders should be frequently distributed to all stakeholders through notice boards, newsletters, and other internal communication channels. Cyber security refresher courses should also be conducted periodically to ensure that all users are aware of your organisation's cyber security policy, their responsibilities, and defensive measures against the latest ransomware attacks.

How K7 Security Protects Against Ransomware

K7 Security's cyber security products offer multiple layers of protection against ransomware. We can classify these as protection before ransomware enters a device, and protection after ransomware enters a device.

Protection Before Ransomware Enters a Device

Protection before ransomware enters a device involves preventing ransomware from gaining access to your IT assets. This protection includes both network and endpoint protection. We have already examined K7's network security against ransomware under the discussion on Gateway Security. We will now examine K7's endpoint protection.

Endpoint Protection

K7 Security's Endpoint Security (K7 EPS) offers multiple features to prevent ransomware intrusion through common malware vectors.

- **USB Storage Devices** – Blocking access to USB storage devices prevents ransomware from entering the organisation through infected USB drives

- **Malicious Websites** – Access to phishing websites and websites that distribute malware can be blocked to prevent ransomware download

- **Wi-Fi Access** – Preventing Wi-Fi access, or allowing Wi-Fi access only within the office, prevents ransomware from infecting the endpoint through an unsecured Wi-Fi network

- **Pirated/Unauthorised Applications** – Only allowing authorised applications to run, and blocking applications based on file path/MD5 value/checksum/version prevents ransomware from entering through compromised, insecure, or outdated applications

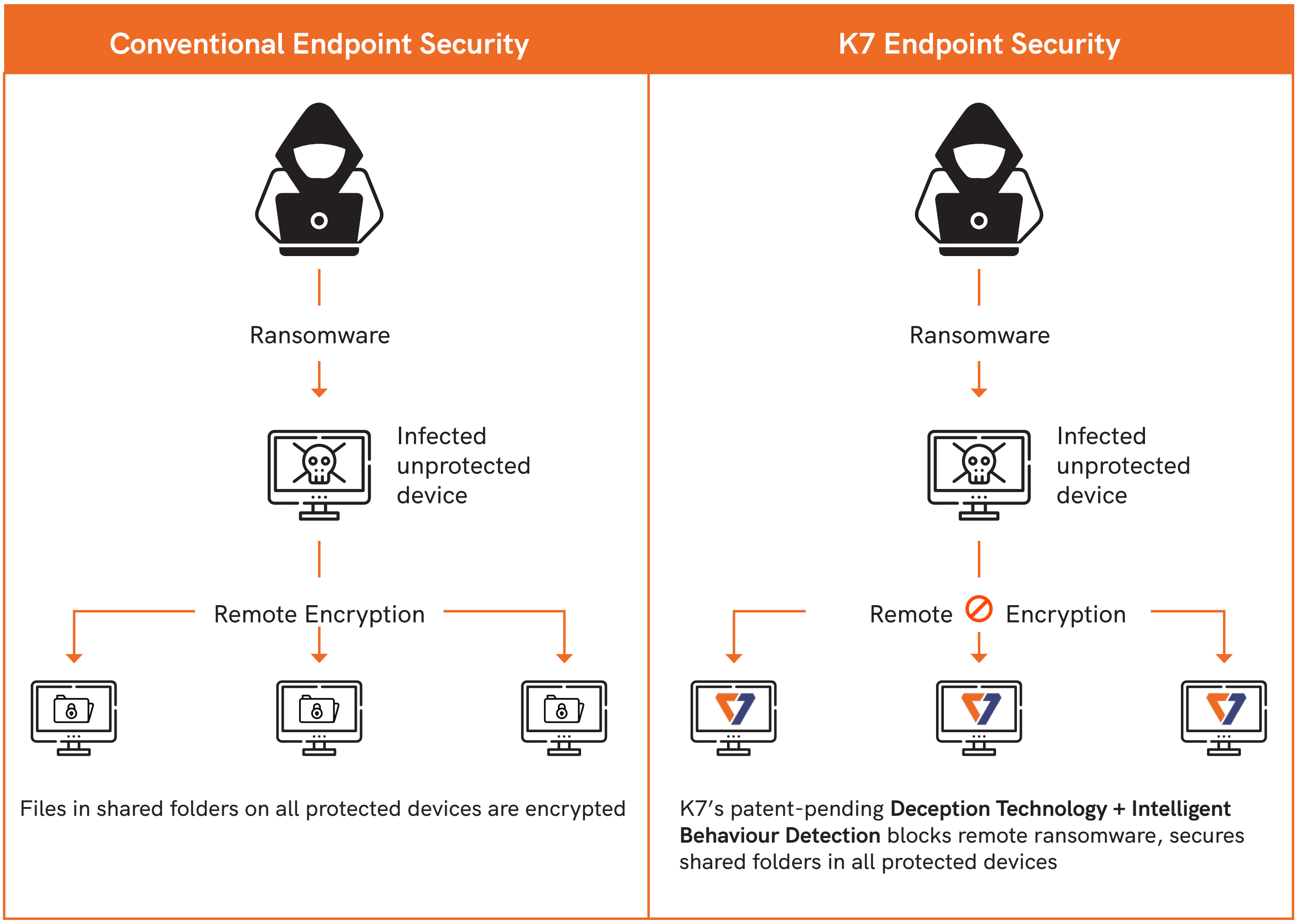
Remote Ransomware Protection

Conventional ransomware is deployed on a device, and encrypts files on the same device. Conventional endpoint security systems check for, and block, ransomware processes running on the device on which the endpoint security system is deployed. Threat actors have developed remote ransomware, where the ransomware is deployed on an unprotected device in the network from where it encrypts files on shared folders in machines that are protected.

Conventional endpoint security solutions are unable to detect remote ransomware as the ransomware process does not run on the protected machine. Just one unprotected device in a business network can result in ransomware spreading throughout the organisation.

K7's Patent-pending Technology

K7 has developed patent-pending Deception Technology which is combined with K7's Intelligent Behaviour Detection to identify and block remote ransomware* in real time on protected devices. The unprotected device from which the ransomware originates can also be automatically blocked for a specified period to contain the threat and allow time for the IT team to eliminate the ransomware on the unprotected device.


Conventional Endpoint Security
K7 Endpoint Security
Ransomware
Infected unprotected device
Remote Encryption
Ransomware
Infected unprotected device
Remote ⊘ Encryption

Files in shared folders on all protected devices are encrypted

K7's patent-pending **Deception Technology + Intelligent Behaviour Detection** blocks remote ransomware, secures shared folders in all protected devices

** Remote ransomware protection is available for Windows 7 and above*

K7 Endpoint Security for the enterprise blends these methods to stop known, novel, and remote ransomware. Our detection and prediction methods are constantly optimised to match the evolution of the ransomware threat landscape.

Protection After Ransomware Enters a Device

A threat actor may be able to drop a ransomware payload under certain circumstances, such as when USB device access is granted but the storage device is infected, or when an email attachment from a trusted contact is opened but the contact's device has been compromised to spread malware. The ransomware may also be already present on the device before Endpoint Security is installed. To protect against such cases, K7 Endpoint Security utilises two ransomware detection techniques to prevent attacks.

Signature Based Analysis/Detection

K7 Labs analyses hundreds of thousands of malware samples a day. Ransomware threats are identified and their signatures are determined. These signatures are included in our definition updates that are distributed several times a day. Files on the endpoint are analysed and flagged if they match the ransomware signature. Detection names for prevalent ransomware are:

Ransomware	K7 Detection Name
Maze	Trojan (005633091)
MBR_unknown	Trojan (0055e4ee1)
Dharma	Trojan (0040eff71)
Ryuk	Trojan (005571bd1)
WannaCry	Trojan (0050db011)
LockerGoga	Trojan (005470f61)
Bad Rabbit	Trojan (0051a3031)
NotPetya	Trojan (00510cfe1)
GandCrab	Trojan (005382c11)

Threat actors may try to evade signature based detection by disguising their malware to avoid matching their identified signatures. Behaviour based detection techniques have been developed to protect against such obfuscation attempts.

Behaviour Based Analysis/Detection

K7 Security's ransomware protection monitors the behaviour of potentially suspicious processes, especially those that try to modify specific file types and the frequency of such attempts. K7 Security also examines sudden increases in file entropy (randomness of content) of unrecognised file types such as free-flowing text files, as unencrypted files usually have more uniformity than encrypted files, to stop malicious encryption.

Behaviour based detection and analysis protects against different ransomware approaches:

1. **Standalone** – Ransomware that directly encrypts files is detected and deleted when it attempts to begin encryption

2. **Injection** – Malware that attempts to encrypt device files by injecting itself into a system process is detected and the injected system process is killed

3. **MBR Compromise** – Heuristic detection is used to detect and block ransomware that attempts to encrypt the Master Boot Record

Types of Ransomware Scanning

- Real-time scanning examines files when they are accessed or activated. For example, an email attachment is scanned before it is opened when a user clicks on it; if ransomware is identified, it will not be allowed to deploy

- Scheduled/On-demand scanning examines all the files on the device for signs of ransomware. This is used to spot and stop dormant ransomware before it activates. As its name suggests, this scan can be scheduled to run at periodic intervals and can also be run on-demand. Remote triggering of scans from the K7 EPS console is also supported

The Importance of Malware Definition Updates

Signature based detection is critical to defeating ransomware. Therefore, endpoints must receive all the definition updates that are issued daily. The large volume of new malware that is identified every day makes any cyber security solution only as good as its last update. K7 EPS is designed with an innovative update mechanism that minimises the size of updates to ensure that all connected endpoints receive all updates even if they are located in connectivity constrained environments, delivering reliable and up-to-date cyber security for organisations with widely distributed operations.

Allowing Legitimate Encryption

All organisations have legitimate need to encrypt at least some of their data to guard against exploitation of stolen data or accidental data breaches. They may also be contractually or legally required to encrypt data. K7 Endpoint Security is designed to differentiate between malicious and legitimate encryption and permit that latter.

K7 Security’s Enterprise Cyber Security Solutions

K7 Security combines over 30 years’ expertise in cyber security with a state-of-the-art threat research lab to deliver rapidly updated enterprise cyber security solutions that protect critical data and devices in SMEs and large enterprises across the world.

- Endpoint Security – Our Endpoint Security utilises multi-layered protection, heuristic malware detection, ransomware protection, and a dedicated firewall to help defend the growing number of connected devices within organisations against cyber attacks

- Network Security – Our Next Generation Firewall, VPN Concentrator, and SD-WAN devices provide enhanced network security and secure connectivity between branch offices, headquarters, and the cloud

Our solutions are recognised across the world for 24×7 enterprise cyber protection. K7 Endpoint Security emerged as the winner against major international cyber security brands in the Performance Test conducted by AV-Comparatives (Austria).

K7 SECURITY

www.k7enterprisesecurity.com

MAR 2024