# RANSOMWARE
## WHITE PAPER

OCTOBER 2020
VERSION: 1.0

TABLE OF CONTENTS



**Document History**

| Version | Status | Date | Author |
|---|---|---|---|
| **0.1** | Issued | 17/09/2020 | Justin Greenwood-Delgado |
| **1.0** | QA Review | 18/09/2020 | Sean McCarthy |

# 1.0 What is Ransomware

Malware categorised as ransomware is a type of malware that aims to extort the organisation by preventing the end users from accessing their system, files or data unless they make some form of payment (conventionally via cryptocurrency or credit card) to regain access.

## 1.1 How do I get Ransomware?

There are several different ways that ransomware can infect your computer. One of the most common methods today is through malicious spam, or malspam, which is unsolicited email that is used to deliver malware. The email might include trojanised attachments, such as PDFs or Word documents. It might also contain links to malicious websites (drive-by downloads). There are many examples of organisations that have been impacted by collateral malware, even though they were not the intended target. Purely because of the interconnection of modern communications and a third party having your email or some kind of access to your enterprise.

**Malspam** uses social engineering to trick people into opening attachments or clicking on links (this can be via Email, phone call, SMS or any communications method) by appearing as legitimate, whether that's by seeming to be from a trusted institution or a friend. Cybercriminals use social engineering in other types of ransomware attacks, such as posing as official or government entities in order to scare users into paying them a sum of money to unlock their files.

Another popular infection method, which reached its peak in 2016, is malvertising. **Malvertising**, or malicious advertising, is the use of online advertising to distribute malware with little to no user interaction required. While browsing the web, even legitimate sites, users can be directed to criminal servers without ever clicking on an ad (known as drive-by attacks). These servers catalogue details about victim computers and their locations, and then select the malware best suited to deliver. Often, that malware is ransomware.

## 1.2 Types of ransomware

There are three main types of ransomware, ranging in severity from mildly off-putting to organisation cripplingly dangerous. They are as follows:

### Scareware

Scareware, as it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you will likely continue to be bombarded with pop-ups, but your files are essentially safe.

A legitimate cybersecurity software program would not solicit customers in this way. If you do not already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you would not need to pay to have the infection removed—you have already paid for the software to do that very job.

## Screen Lockers

Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you are frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking government department warning saying illegal activity has been detected on your computer and you must pay a fine. However, these departments would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

## Encrypting Ransomware

This is the most worrying kind of ransomware. These are the criminals who hold files hostage by encrypting them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get a hold of your files, no security software or system restore can return them to you (unless you have a backup copy). Unless you pay the ransom—for the most part, they are gone. And even if you do pay up, there is no guarantee the cybercriminals will give you those files back.

Ransomware will encrypt a victim's files and replace them with encrypted data using one of the three methods below:

1. Writing the encrypted data from memory to the original file.
2. Writing the encrypted data from memory to a new file and then deleting the old one.
3. Writing the encrypted data from memory to a new file and then using the Rename call to replace the original file.

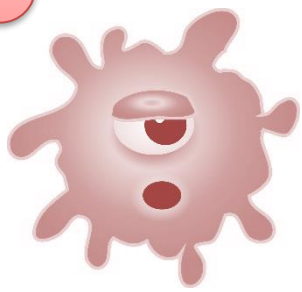
Methods 1 and 2 are the most common observed by most ransom malware and there are several controls with modern operation systems and anti-malware software to protect against this. However as of late 2019 newer versions have started to emerge that subvert the method known as *RIPlace technique* which these controls use to protect a system.

# 2.0 Trends & Risks

In 2020 the trend has been for threat actors to use one of the following popular strains or variations of ransom malware:

**Maze** is a relatively new ransomware group known for releasing stolen data to the public if the victim does not pay to decrypt it.

**RobbinHood** is an EternalBlue variant that brought the city of Baltimore, Maryland, to its knees in 2019.



**Thanos** is the newest ransomware on this list, discovered in January 2020. It is sold as ransomware as a service, it is the first to use the *RIPlace* technique, which can bypass most anti-ransomware methods.

**GandCrab** might be the most lucrative ransomware ever. Its developers, which sold the program to cybercriminals, claim more than $2 billion in victim payouts as of July 2019.

**Sodinokibi** targets Microsoft Windows systems and encrypts all files except configuration files. It is related to GandCrab

In 2019, education organisations were the top target for Trojan malware (based on the data from the top three anti-malware solutions on the market). They were the number one most-detected (and therefore most pervasive) threat category for all businesses in 2019 and early 2020. Adware and ransomware were also particularly drawn to the education sector last year, finding it the third and fourth most desired target among industries, after public sector service organisations and health providers.

22% of organisations had to cease business operations immediately because of ransomware

50% of organisations infected with ransomware received demands of **£1,000** or more

Reason why attackers go after health and education bodies are:

- These organisations rely heavily on the availability of data on their highly distributed networks and due to the remote accessibility to core infrastructure from multiple sites and locations. These organisations rely heavily on the availability of data across their highly distributed networks which could allow for multiple entry points into core infrastructure and services including remote sites and users

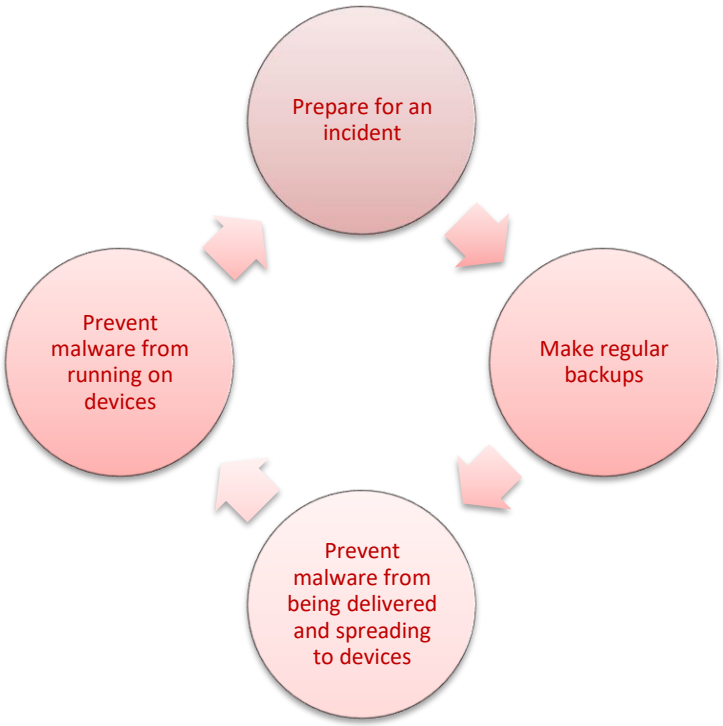
- The vast number of end users (patients, students, and staff) connect from personal devices (that may have local administrative rights and permissions) both on-premises and at home. Additionally, a rotating influx of new users to manage daily, leaves a larger and more open attack surface for criminals to infiltrate.


- The nature of ransom attacks is to extort money from the data an organisation stores and has access to and these organisations have vast quantities. This information is highly sought-after by threat actors (due to the fact that much of it can be highly sensitive in nature and of a personal nature to individuals), who can use it to hold the organisation for ransom or to sell for high profit margins on a black market.

- The final reason is the technological infrastructure of these organisations is typically outdated in areas and easily penetrated by cybercriminals due to legacy hardware and operating systems that are no longer supported with current security patches and/or security hardening.

# 3.0 Protective Measures

Since there is no way to completely protect your organisation against malware infection, a **defence-in-depth** approach should be adopted. This means using layers of defence with several mitigations at each layer to provide a holistic level of assurance. Providing more opportunities to detect malware, and then stop it before it causes real harm to the organisation. It should be assumed that some malware will infiltrate your organisation. It is therefore critical that steps are taken to limit the impact this would cause and identify ways to speed up your response and recovery to such incidents.




The following are several steps an organisation should be taking to prevent and prepare in case their organisation is affected by a ransomware attack:

•Managers should identity their critical assets and what the impact would be if they were disrupted by a malware attack (specifically focused on business operational data stores, shares, and ledgers). Then develop and test an incident response plan that accounts for what should happen if there is an attack.

•Organisations should be making regular backups, of key data sets and critical operational data repositories, so in the event of an incident these can be restored ensuring minimal impact and no loss of data to the business.The validity of data back-up should also be tested using a managed process.

- Permissions assigned and allocated to data and network shares should enforce using controls such as authenticated internal proxies, user multi-factor authentication, user session expiry. Rights allocated to end-users should be done using a least privilege security model; based on their requirements and need. This access should be reviewed quarterly so that permissions are not grandfathered, and access pruned in-line with a personnel's roles requirements.

- Data stores should be highly segregated base on the end users' roles, internal departments and business units. Making use of gateway security controls such as:

    - Mail filtering
    - Internet gateway content inspection (file type whitelisting) and safe browsing lists
    - Making use of internal traffic proxies for both ingress and egress traffic

- Several steps should be taken to prevent malware from running on end-user assets. The measures required will vary for each device type, operating system, and version, but in general device-level security features should be used where possible, such as:

    - AppLocker
    - Enterprise grade antimalware and endpoint protection software
    - Disable or constrain scripting environments and macros execution
    - Remove applications and software not required for job role
    - Disable autorun for mounted media
    - Configure host-based and network firewalls
    - Sandboxing access and content so end users only have a presented or read only view where appropriate.

The URL below is a more detailed look at NCSC guidance and recommendations on malware prevention https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

# 4.0 Additional Services

The protective measures highlighted in the previous section are not exhaustive just a high-level overview of the security controls that can be adopted and layered by an organisation. AMR CyberSecurity can expand and highlight additional controls based on the bespoke requirements of an organisation, as well as testing, benchmarking, and auditing existing controls.

AMR Cybersecurity as a 360-security organisation can offer the following services to aid against the ransomware threat:

- **Organisation External Assessment:** This involves scanning OSINT resources and data sources to identify the external and publicly accessible digital footprint of your organisation. Then performed a vulnerability assessment against these domains, ingress points and portals, IP address and networks simulating a real-world attacker.
- **IT Device Security Configuration review and gap analysis:** This service benchmarks the configuration of your IT hardware assets against known industry best practise, guidelines, and security standards to identify deviations and area that can be security hardened.
- **Red Teaming and Phishing exercise:** This service is a goal/object oriented penetration assessment aiming to leverage access from the outside to the inside of your organisation, subverting security controls and highlighting the real world impact of Intellectual Property acquisition and key asset compromise.
- **Domain and user security review:** This service involved parsing your organisation domains, defined user groups and roles and auditing them for security weaknesses (in password management and controls) as well as group permissions and access throughout the estate.
- **Incident Response Planning Assessments:** These are tabletop exercises with your department heads and key stakeholders to simulate specific threats to your organisations working through your Incident Response process and disaster recovery plans to identify gaps and areas for improvement. Additionally, this product works as a valuable training internally preparing personnel in the key steps and process (clarifying the roles and responsibilities of both staff and third parties) to steer the organisation though an event to system recovery.

For more information on any of **AMR Cyber Security** Services please contact **Rachel Bi** on enquiries@amrcybersecurity.com