THREE WAYS TO PROTECT AGAINST RANSOMWARE

UNISYS | Securing Your Tomorrow®

A security perspectives paper by:
Ashwin Pal, Director of Security Services,
Unisys Asia Pacific.

There have been a number of ransomware attacks on Australian businesses lately such as Toll Holdings and Service NSW. Awareness of this threat is increasing, but many organisations are still in the dark about what it is and how to protect themselves against it.

What Is Ransomware and How Does It Work?

Ransomware is a class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while others simply lock the system and display messages intended to coax the user into paying.

Ransomware typically propagates like a conventional computer worm, entering a system through, for example, a downloaded file (usually send via a link in an email) or a vulnerability in a network or operating system service.

Two styles of 'ransomware attacks' have emerged.

The first may be the more likely of the two to strike but it is also potentially less debilitating. This version simply locks the victim's screen. The second style of ransomware is a more targeted attack, and actually encrypts files on the target computer.

In the first type, criminals typically use an official looking logo to intimidate the victim (such as a local law enforcement agency or a government department) and simply lock their victim's screen so they cannot access their computer until a payment is made. It is a broad brush approach, distributed en masse with the hope that a portion of victims will pay the 'fine' or ransom demanded on the locked screen. This scenario does not typically encrypt any files on the victim's computer (although early examples may have) and is more often just a form of malware, for which most security vendors have tools to assist.

The second type of ransomware is a more targeted and challenging concern. In this scenario, cyber criminals target a particular victim, typically a business or an organisation. The targeted computers are actually hacked and files on the computer encrypted. Without payment, files are inaccessible.

To understand how to protect against ransomware attacks, you must first understand how they work and propagate. Attacks like these usually start with a phishing email to users. Once a user clicks on a malicious link in the email or opens a malicious attachment, malware is downloaded to their machines. An example of this is WannaCry, where the malware spread laterally in the network using a Windows vulnerability that was patched two months before WannaCry was released in the wild. After that, the process is simple – the malware infects a computer, locking users out of the system (usually by encrypting the data on the hard drive), and then holds the decryption or other release key ransom until the victim pays a fee, usually in bitcoin.

Steps to Protect Yourself and Your Organisation

Here are some simple steps that can be taken to minimise the damage.

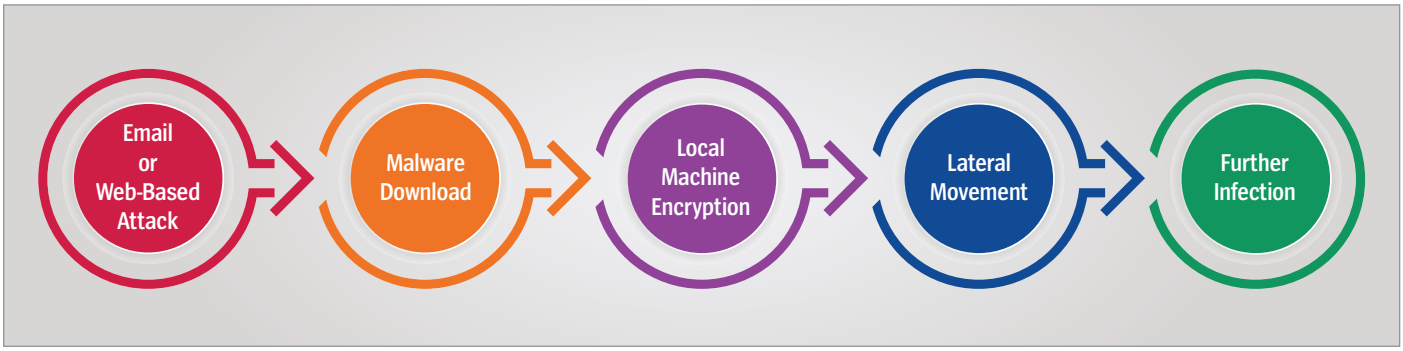
Focus on The Basics

1. **User education** – almost all ransomware attacks start by targeting users and enticing them to click on a malicious link or open a malicious attachment. Your people can be your weakest link in your security strategy or your greatest ally if they have the right education. Ensure that all your users know IT security basics and undergo regular education programs. Run mock phishing campaigns to test their knowledge and reinforce the learnings.
2. **Malware entry points** – Protect potential entry points for ransomware related malware into your organisation. This includes email, web and removable devices on endpoints. Use well regarded web and email filtering solutions. It is particularly important to protect the Web as not only can malware be downloaded from websites, web-based emails also come into your network via this channel. Employ web and email protection measures that do not just rely on signatures, but use better detection techniques such as behaviour analysis, heuristics, and artificial intelligence to detect and stop sophisticated threats. Use next generation endpoint protection technologies that protect against advanced threats using user and network behaviour analysis, heuristics and other advanced techniques.
3. **Vulnerability management and patching (applying software updates)** – this is one of the simplest and practical ways to prevent attacks in your organisation. Attackers search for, and exploit, unpatched vulnerabilities in your systems to spread and infect your IT assets. Run regular (at least monthly) vulnerability scans and patch your systems before attackers can exploit these vulnerabilities. Environments that cannot be patched should use **virtual patching** – software that cloaks vulnerable machines in order to stop attacks based on these unpatched vulnerabilities.

4. **Segmentation** – Malware spreads so fast through networks because almost everyone's network is flat and designed like chocolate M&Ms – hard on the outside and soft on the inside! Many organisations are constrained by certain critical applications that need to run on older operating systems. To protect against such scenarios, organisations should segment their networks based on the criticality of information they house and the level of risk to them. Machines that cannot be patched, for whatever reason, should be further segmented to protect them. **Microsegmentation** makes this easy and very practical without requiring major changes to the network or application infrastructure itself.
5. **Minimal user privileges** – malware usually executes on a machine using the privileges of the logged-on user. Therefore ensure that users only have the required privileges to perform their tasks. Allowing blanket local admin access to all users is not ideal.
6. **Incident response plan** – recognise that despite all our best efforts, bad things will happen. Have a robust and well-tested incident response plan that can be activated in the case of a security breach so that you recover easily and in a methodical fashion.
7. **Back-ups** – run regular backups. The back-up schedule should be based on the criticality of the systems i.e. the more critical the system, the more frequent the backups required. Ensure that you have a robust Disaster Recovery Plan and have documented your Recovery Point Objectives (how much data can you afford to lose) and Recovery Time Objectives (how soon do you want the system back up and running to limit the hindrance to your business operations). Under no circumstances should you have your back-up systems connected to your production networks. Recent ransomware attacks look for backup systems to encrypt your back-ups. It is critical to ensure that your back-up systems are **air-gapped** from your production systems.
8. **Protect against advanced threats** – know that the threat landscape will only get worse. The 'success' of recent ransomware encourages attackers to come up with even better ways to attack you. Invest in technologies that detect and protect you against advanced threats. Ensure that the protection is applied at all the right layers – including endpoints, servers, network, web traffic and email traffic.
9. **Limit remote access to your systems directly from the Internet** – allowing direct remote access using mechanisms such as Microsoft's Remote Desktop Protocol from the internet exposes your systems to intruders on the outside. It provides a simple way for intruders to gain access to your systems, so you should avoid its use.
10. **Ensure secure remote access** – where remote access is necessary, use secure methods such as point-to-point cryptographic cloaked connections that require two-factor authentication (two methods, not just password), and restrict access to only those individuals, systems and services that really require remote access. The latter is best achieved through an identity based **microsegmentation** solution that allows strict enforcement of role based access controls.
11. **Strong authentication** – at a minimum, enforce strong passphrase/password policies on your systems to reduce the risk from brute force attempts at cracking passwords. Ideally, use multi-factor authentication particularly for remote access. Consider biometric based authentication to remove passwords easing the logon process and enhancing security. Implement account lockout policies (account locks if too many false attempts are made) on your systems to reduce the risk from brute forcing attempts.
12. **Privileged account management** – ransomware attacks can exploit easily accessed privileged accounts. Ensure that you have appropriate controls to make unauthorised access to privileged accounts difficult. Examples of controls include ensuring multi-factor authentications ideally based on biometrics. Use privileged management software to manage and monitor privileged access. **Microsegment** privileged access to ensure controlled use.
13. **Application whitelisting** – this is one of the most effective controls where particular application will not execute if it is not whitelisted, including malware. Having said that, this can be difficult on user endpoints as users may want to run their own applications which does necessitate the other controls mentioned above.

Take an Attack-Based Approach

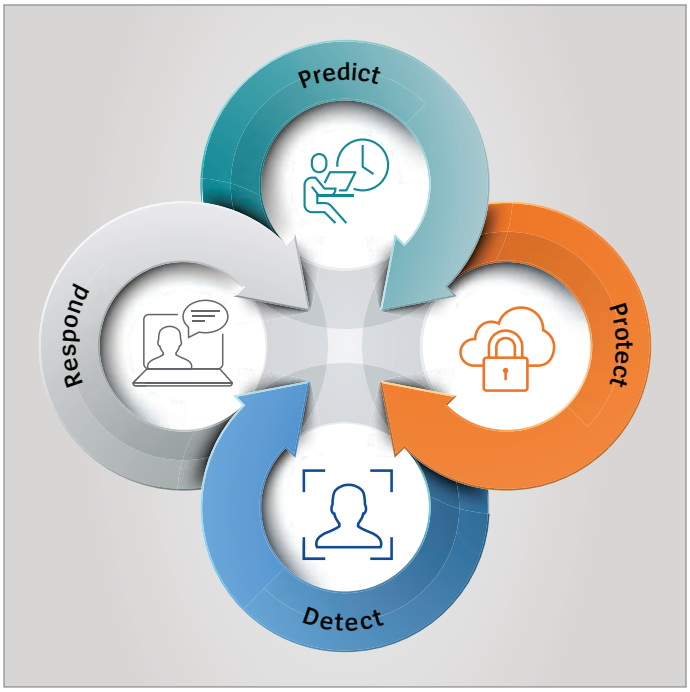
To truly protect yourself from ransomware attacks it is important to understand the stages of the attack and how can you apply controls at each stage to protect yourself. Here is the typical attack methodology:



- **Email or web based attack** – initially the attacker will send an email with a link or an attachment that will either contain or direct a user to malware.
- **Malware download** – once the user opens the attachment or clicks on the link, the malware downloads to the user's device. This usually exploits a missing patch on the device.
- **Local machine encryption** – once the malware has been downloaded to the device, the machine gets encrypted.
- **Lateral movement** – the malware then move laterally within the network, usually by exploiting existing vulnerabilities.
- **Further infection** – as the malware spreads to other machines, it continues to spread and encrypt.

Let's look at how we can implement controls that help stop this type of attack.

Controls within a cybersecurity context generally falls into four categories:



- **Predict** – systems, tools, policies and procedures that help detect vulnerabilities in systems and predict potential avenues of attack.
- **Prevent** – systems, tools, policies and procedures that prevent threats affecting your systems. Examples include the corporate firewall and **microsegmentation technology**.
- **Detect** – systems, tools, policies and procedures that give you the ability to detect threats that may affect your system. An example is an Intrusion Detection System.
- **Respond** – systems, tools, policies and procedures that allow you to respond to threats and contain/eradicate them. A policy example is the corporate Incident Response Plan and associated tools such as a Security Information and Event Management (SIEM) system and automated response and isolation technology such as **Dynamic Isolation**.

Now comes the important part – we need to look at all the steps in the attack methodology and apply controls for each category of control for each step to help stop the attack. The simplest way of doing this is in a table whereby you map existing controls against each category of controls that protect against the relevant attack phase. Any gaps should be addressed urgently. As you do this gap analysis, do not forget controls for people and processes, physical security, disaster recovery and third parties. Mapping your controls to an adversary's attack methodology, is the best way to stop the attack.

Get Strategic

The advice so far has been purely tactical. Threats will evolve and get worse. The only way to truly protect yourself is to conduct a robust risk analysis of your environment using standards such as ISO 27001, NIST, ISM, etc. and address the issues that are found. Start with a simple health check. Understand your vulnerabilities and address them methodically. Moreover, once you are done, rinse and repeat! The threat landscape and your environment will constantly change and evolve. In order to stay on top of new and emerging threats, you have to stay ever vigilant and reassess your risks regularly.

In addition, engage in intelligence-led security. This is having relevant intelligence about threats and vulnerabilities related to your environment and protecting yourself against them. Many organisations provide very useful threat information from sources including the open, deep and dark web. Importing this information along with your vulnerability information into your Security Information and Event Management (SIEM) tool will allow you to detect threats faster and much more accurately. This process will greatly enhance your capability to pick up Indicators of Compromise, the investigation of which can prevent or minimise damage. Use of tools that allow **quick isolation of endpoints** upon detection of a security incident will greatly reduce the chances of east west spread of ransomware as well as ease the burden on your security operations centre.

The traditional risk analysis approach looks at strategies from the inside out as you are primarily focused on control gaps inside your organisation. The intelligence-led approach looks at strategies from the outside in (from the attacker's perspective). The combination of these two approaches can truly give you a well-rounded perspective to risks and threats affecting your organisation. It is critical to ensure that whatever methodology or tool is used, it must take into account **threats and vulnerabilities** to give you a true picture of likelihood. Further, this information needs to be made available in near real-time so that Boards and Executives are fully informed of the organisation's risk posture and can make informed decisions. Providing a clear idea on the value of risk mitigated based on previous breach costs within your industry will allow Boards and Executives to better understand the value of requested cybersecurity investments and will make obtaining funding easier.

As the threat landscape evolves, it is important to take some simple and practical steps to protect yourself. The steps outlined above can restrict the impact of ransomware.

About the Author

Ashwin Pal

Ashwin Pal is the Unisys Director of Security Services responsible for the delivery of Unisys' security business in the Asia Pacific region.

Contact Ashwin at Ashwin.Pal@au.unisys.com or connect with him at LinkedIn.

Sign up for a complimentary two hour workshop to learn how to use microsegmentation to secure your organisation: secureoutreach.unisys.com/stealth™workshop.

Find out how Unisys builds better outcomes securely at unisys.com/security.

For more information visit www.unisys.com