NETWORK INTELLIGENCE

THE EVOLUTION OF RANSOMWARE

BY ADAM SIDDIQUI | BUSINESS DEVELOPMENT MANAGER

APRIL 2022

RAN·SOM·WARE

A type of malicious software designed to block access to a computer system until a sum of money is paid.

MALWARE / RANSOMWARE

Malware is defined as software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Yisrael Radai, the late Israeli professor, **coined the phrase malware** in 1990 as a combination of 'malicious' and 'software'.

Ransomware is a specific type of malware that is designed to extract a 'ransom'.

TABLE OF CONTENTS

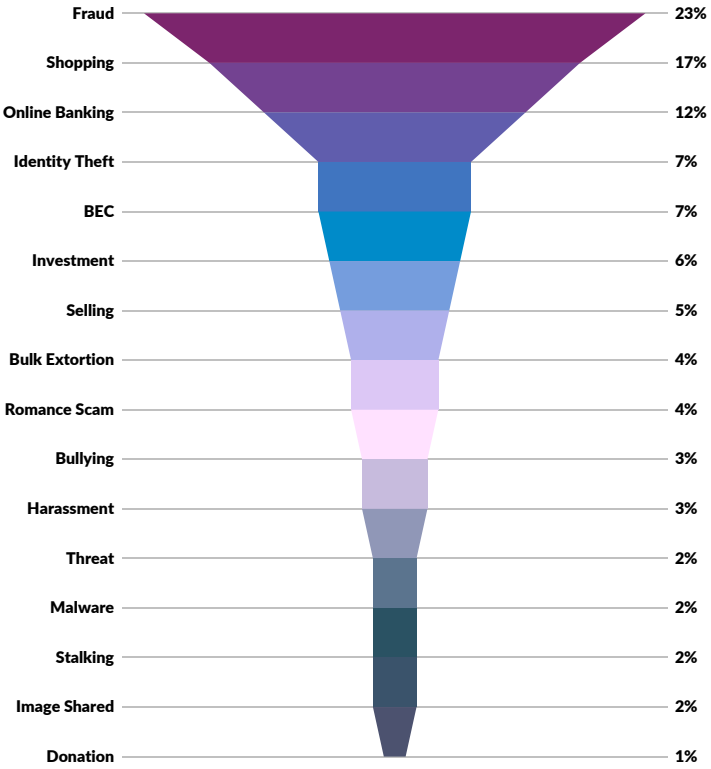
Young and Yung proposed the concept of Cryptovirology in 1996, demonstrating that cryptography may be used for hostile reasons like extortion. Since then, this concept has evolved into ransomware, which has grown to become a major cyber security issue, with an increasing number of infections and variants being created daily.

THE EVOLUTION

When it comes to ransomware, it's all about the money. **Self-reported financial losses due to cybercrime in Australia-based cybercrime reports totaled more than $33 billion (AUD)**, according to the Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report; and these statistics are only the cases that have been reported to the ACSC.

As per the **ACSC report** an attack occurs once every 8 minutes in Australia.

Although ransomware-related cybercrime reports are a relatively small percentage of all reported cybercrimes, ransomware remains the most serious threat because of its high financial impact and disruption to victims and wider society.



CYBERCRIME REPORTS BY TYPE FOR FINANCIAL YEAR 2020-21 (CYBER GOV AU ACSC REPORT)

1989
Dr Popps AIDS Trojan

2006
Archiveus and GPCode Ransomware

2009
Sccareware used to distribute Ransomware

2011
Sudden exponential increase in Ransomware

2014-15
Chimera and CryptoWall V1-4

2016
Ransomware as a Service becomes more maintream

2017
Wannacry

JAN 2020
Sodinokibi infects Travelex

MAY 2020
Maze Ransomware picks up activity

JUNE 2020
Snake Ransomware suspected to have infected Honda

There are two popular varieties of ransomware:

CRYPTO RANSOMWARE

To extort money, crypto ransomware encrypts files on computers systems. Crypto ransomware's goal is to encrypt your vital data, such as documents, photos, and videos, but not to disrupt your computer's core functioning. Because people can see their files but not access them, this causes panic. Crypto developers frequently include a countdown to their ransom demand. After crossing the countdown, the ransom amount would double. Crypto ransomware is the most widely present ransomware where it usually encrypts user's files or the entire disk. **Revil** and **Petya** would be examples of Crypto ransomware

Crypto ransomware can have a devastating impact due to the large number of users who are unaware of the need for backups in the cloud or on external physical storage devices. As a result, many victims pay the ransom so that they can regain access to their information.

The increase in attacks can be attributed in part to malware makers adopting an easy-to-use, modular form of ransomware. The availability of **ransomware-as-a-service (RaaS) has also been growing**, allowing the attacker to distribute the malware via phishing and exploitation kits, in addition to providing an economic model that is reliable.

LOCKER RANSOMWARE

MALWARE OF THIS TYPE DISABLES BASIC COMPUTER FUNCTIONALITY.

You may, for example, be denied access to the desktop while your mouse and keyboard are partially disabled. This permits you to continue interacting with the ransom demand window to pay the ransom. Aside from that, the machine is completely unusable. However, there is some good news: Locker malware rarely targets essential files, preferring instead to shut you out. As a result, complete data destruction is unlikely.

Who are these Threat Actors?

ORGANIZED CRIMINAL GROUPS

To find victims, organized criminals largely employ a wide range of ransomware techniques. Mal-Spam kits are usually employed in their campaigns to quickly and indiscriminately transmit virus-infected software, often to hundreds of thousands of victims in a single attack.

These attackers often develop highly automated infrastructure to handle infections, payments, decryption, and laundering. In the past, they typically demanded small ransom payments; it was a high volume, low dollar value attack. Although this has changed in recent attacks.

STATE ACTORS

State-led ransomware typically comes from heavily sanctioned countries like North Korea, Iran, and Russia. They operate for a variety of reasons, not just to steal funds but also to sow chaos for their adversaries.

For instance, NotPetya was a widespread ransomware **attack led by the GRU**, the intelligence arm of the Russian military. NotPetya never developed a workable payment mechanism; the attackers may not have ever intended to decrypt any files. Given the large number of Ukrainian victims, it seems that NotPetya's primary objective was sabotage and geopolitical disruption.

The WannaCry ransomware attack, linked to North Korean cybercriminal group **Lazarus,** similarly had no known cases of decryption. This was another attack with no real infrastructure for handling ransom payments. It only had three payment addresses and there was no clear way to communicate with victims. It is unlikely that financial gain was the main objective, but it's difficult to discern a core motive.

How do they do it?

PHISHING

Phishing occurs when an attacker contacts a victim, usually via email, acting as a reputable company and attempting to obtain personal information or login credentials. These types of emails are designed to elicit a sensation of anxiety or (paradoxically), a lack of security.

A phishing attempt may take the shape of a message purporting to be from a reputable company such as LinkedIn, Microsoft, or a location where you save personal information, such as Google Drive. Phishers may warn you that your account has been compromised, and they will require you to log in through their website to verify your identity or change your password. In essence, this website is a ruse designed to steal the targets' login credentials for various services, such as their bank account or Google account.

While email is still the most common form of phishing attack, it isn't the only one around anymore. Alternatively, these messages can be delivered through instant messaging, social media, etc.

COMMONLY ABUSED PORTS IN RANSOMWARE ATTACKS:

- **PORT 139** – NETBIOS IS A LEGACY STANDARD FOR EXCHANGING FILES AND PRINTERS.
- **PORT 445** – SMB. PROVIDES SHARING CAPABILITIES OF FILES AND PRINTERS. USED IN THE 2017 WANNACRY ATTACK.
- **PORT 3389** – REMOTE DESKTOP. ATTACKERS USE PUBLIC FACING RDP PORTS AS AN ENTRY POINT INTO THE CORPORATE NETWORK

OPEN PORTS

Attackers can use ports that have been opened for the Internet as an initial attack vector. An open port may not necessarily indicate a security problem. It can, however, present a way for hackers to gain access to the application that uses that port. As a result, attackers can take advantage of issues such as weak credentials, the lack of two-factor authentication, or application flaws.
Limiting or completely closing ports by implementing well defined firewall rules is the recommended approach. If necessary, remote workers can use a secure VPN to access applications hosted internally in the corporate environment

Scanners are used by both attackers and security professionals to detect open ports automatically. Port scanning can be detected by a variety of network-based IDS/IPS and even workstation-based endpoint security solutions. Once an attacker gains access to a network, they may want to find additional systems which they can move to. To accomplish this, they would run internal port scans to determine services which can be exploited.

WHAT IS THE WEAKEST LINK?

Is there one? If we look at the statistics it seems to be more of a case of “what isn’t our weakness?”. Businesses have always been quick to adapt to new technology. After all, it provides several benefits to help us work easier, faster and adapt to an ever-evolving global marketplace. To remain competitive, organisations across the globe have felt compelled to stay abreast of the latest technology, and often, security has been overlooked.

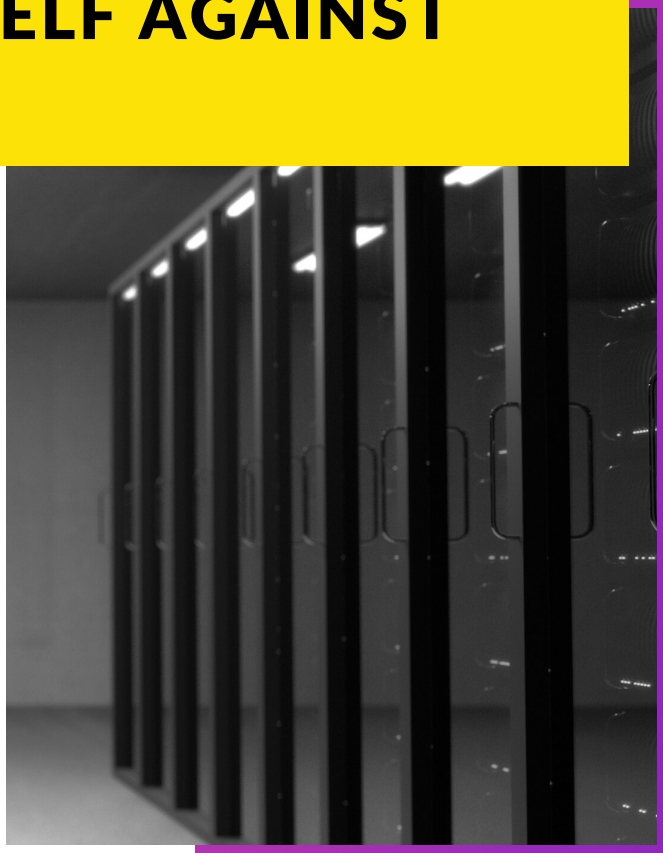
With Covid-19, this was exemplified to an even greater extent. Even though it was rapid and under intense pressure, most businesses judged the shift to remote work to be a success. Many firms even continued or accelerated digital transformation journeys that they had started earlier, thanks to the resilience of their leaders and employees. Contrary to popular belief, production did not fall in general, and in some cases, it even grew. However, many security challenges remained, and the move to distributed work introduced new risks.

INSUFFICIENT CONTROLS AROUND THE DIGITAL INFRASTRUCTURE:

Employees' home networks are usually less secure than the company networks, which is understandable. Valuable data resides in digital infrastructure, which requires a dynamic approach to defending critical information. For example, corporate servers are managed by employees with higher access privileges. As a result of this pandemic, employees moved from corporate offices to their homes, and in some cases the data also transferred to areas that are less secure.

The ransomware risks involve a lot more than just insufficient controls. There is a plethora of challenges businesses face that must be addressed, safe cyber practices, password management, BYOD (bring your own device), improved backup processes, etc.

PROTECTING YOURSELF AGAINST RANSOMWARE



MAINTAIN BACKUPS

The most effective method of recovering from a ransomware infection is to have a Disaster Recovery Plan in place which would contain the process and infrastructure for backing up data and then restoring data from these backups.
A backup should be properly protected and stored offline or 'out-of-band', so that it cannot be targeted by attackers. You may benefit from using cloud services in the event of a ransomware infection since many cloud providers retain previous versions of files. This will enable you to restore an unencrypted version if necessary. Ensure that backups are routinely tested for efficacy. If an attack occurs, you should verify that your backups are not infected before rolling them back.

Ensure your organization has an effective business continuity strategy or partner with a **Cybersecurity Expert** who can help you implement one.

DEVELOP PLANS AND POLICIES

Establish an incident response plan so your IT security team is prepared for any ransomware attack. Included in the plan should be roles and communication channels to be utilized during an attack. It is also recommended that you provide a list of contacts, such as any partners or vendors that would need to be notified.

How do you handle suspicious emails? Do you have a policy in place? It is important to train employees on what to do if they receive emails that they do not understand.

It may be as simple as forwarding the email to the IT security team. After the Incident Response plan has been setup, it is crucial that you test it by conducting Cyber Drills for various scenarios to ensure all the relevant teams are in sync.

REVIEW PORT CONFIGURATIONS AND RULES

As discussed earlier, several ransomware variants utilize the Remote Desktop Protocol (RDP) port 3389 and the Server Message Block (SMB) port 445. You should consider whether your organization needs to leave this port open, and whether it is appropriate to only allow connections from trusted hosts. Consider reviewing these settings for both on-premises and cloud environments, coordinating with your cloud service provider to disable unused RDP ports.

Also, conduct a rule set review of all firewalls on a quarterly basis to ensure the rules are proper and there is no gap through which an attacker could enter the environment. Use automated tools, such as **FireSec**, to conduct a firewall rule set review.

KEEP SYSTEMS UP TO DATE

Update all operating systems, applications, and software in your organization on a regular basis. By updating your software, you will close any security holes that attackers may try to exploit.

Make sure that auto-updates are enabled and there is a patch management system in place.

HARDEN YOUR ENDPOINTS

Configure your systems in a manner that ensures security.

Secure endpoint configuration via proper Active Directory Group Policy Object (GPO) settings can help reduce your organization's threat surface and close security gaps that may be left over from default settings. Ensure that your systems are following a Security Baseline.

Besides a commercial-grade anti-virus, you can implement an EDR to enhance the Anti-Malware defenses of your endpoints.

IMPLEMENT AN MDR SOLUTION

As part of Network Intelligence's Managed Detection and Response (MDR) service, customers are provided with active threat hunting services.

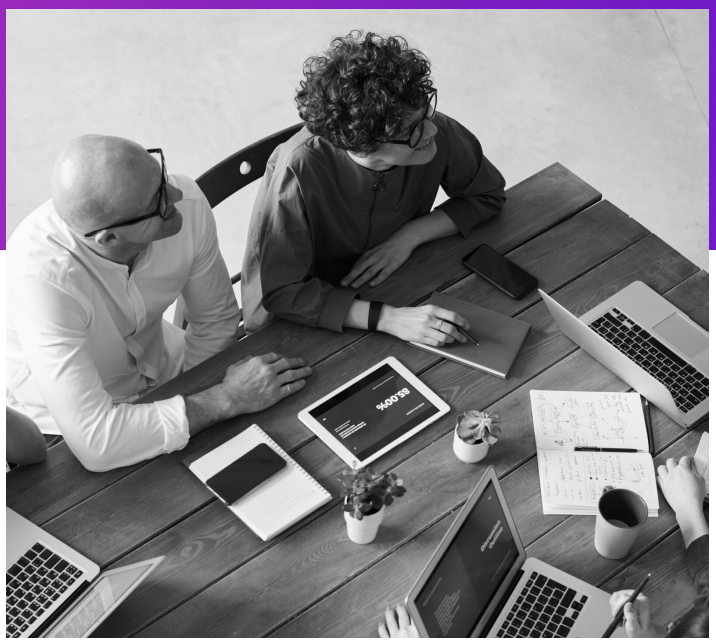
We analyze ingested data from your endpoints. We can use a combination of unique AI&ML based tools along with human analysis from our trained experienced experts.

Network Intelligence combine our proprietary software, along with IBM Q Radar, Cylance as well as 30+ Intel feeds including AI & ML to provide this service to our clients 24/7 365 days a year.

TRAIN THE TEAM

Ransomware can be stopped in its tracks by implementing security awareness training.

If employees can recognize and avoid malicious emails, they play a key role in protecting the organization. Team members can benefit from security awareness training by learning what to look for in an email before they click on links or download attachments.



ABOUT NETWORK INTELLIGENCE

INFO@NIICONSULTING.COM

WWW.NIICONSULTING.COM

We are a global cybersecurity provider founded in 2001 with more than 500 team members working out of our New York, Amsterdam, Sydney, Riyadh, Dubai, Mumbai, and Singapore offices.

We offer services across 6 broad spectrums - Assessment, BCMS, GRC, Professional Services, MSSP & Trainings. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, Healthcare, and more.

Based on our experience of helping companies prepare for and fight against ransomware, we have launched our – **Ransomware Readiness Assessment Service (RRAS)**. RRAS aligns organizations' Ransomware prevention and mitigation requirements, objectives, risk appetite, and resources with the elements of the Cybersecurity Standards. This service is built on the proven NIST Cybersecurity Framework approach. **For more information, visit our RRAS page today!**

We believe that cybersecurity is not a destination, it is a journey and we partner with our clients to address the dynamic cybersecurity threat landscape.

STAY CONNECTED!