Ransomware

Information Security Policies and Procedures

Ransomware:

How to manage the risk

OVERVIEW OF RANSOMWARE

Ransomware is a type of malicious software (malware) that can encrypt files and render a victim's computer unusable. Cybercriminals try to infect a computer or network with this malware, and then demand a ransom to unlock or decrypt the victim's files. Payment is usually demanded in digital currency such as Bitcoin.

Businesses and organisations that fall victim to ransomware often fail to report this to police or agencies like the ACSC. This may be due to fear of damaging their reputation, losing customers, the impact on their revenue, or compliance action from the government. There is also no guarantee that the payment will lead to data being recovered, prevent information from being on-sold to other criminals, or that victims won't be attacked again. Each ransomware payment incentivises cybercriminals, perpetuates the crime, and puts other Australian organisations at risk.

To improve their chances of success and profitability, criminals have adopted the following strategies:

- Targeting large organisations (known as ‘big game hunting’) to demand larger ransom payments.
- Forming partnerships with other cybercriminals, to share resources and expertise.
- Double extortion, by not only encrypting data and demanding a ransom, but also threatening to publish the data. This threat is often followed through, and sensitive data is uploaded to dedicated leak sites, allowing other cybercriminals to steal personal information.
- Requesting payment in digital currencies that are harder to trace (known as privacy coins) to obscure ransomware payments.
- Operating via Ransomware as a Service (RaaS) business models, using malware provided by other cybercriminals for a fee.

HOW A COMPUTER MIGHT BE INFECTED WITH RANSOMWARE

Ransomware can be deployed in a number of ways, including:

- Remote Desktop Protocol (RDP) that is not protected from the internet.
- Infected USB sticks that pass on and install malware on between machines.
- Taking advantage of vulnerabilities in unpatched software (known as exploits).
- Victims unknowingly visiting infected websites and becoming infected with malware.
- Pirated software that has malware added, which is then installed on a computer by a user.
- Phishing emails that entice victims to open attachments or click links which launch the malware.
- 'Malvertising' where a cybercriminal rents ad space on a website, luring a victim to click on an advertisement. The ad is linked to a hacking toolkit known as an 'exploit kit', which scans the victim's machine for a vulnerability, installing ransomware if possible.

Remote Desktop Protocol (RDP) - A network communications protocol developed by Microsoft which provides a user with remote access to their physical work desktop computers.

RANSOMWARE TYPES

The most common types of ransomware:

Crypto ransomware - encrypts files within a system but doesn't disable basic computer functions.

Lockers - locks basic computer functions, rendering it inoperable. Complete destruction of data is unlikely.

Scareware - a fake software claiming to have detected a virus and demanding a payment to fix the issue.

AN ORGANISED CRIME: THE RANSOMWARE ECOSYSTEM

Ransomware exists in a symbiotic ecosystem. Even people with very little experience in coding or cybercrime can access all the services and tools required to carry out a ransomware attack on the darknet. These include:

- **Ransomware as a Service (RaaS**) - a business model increasingly used by cybercriminals, where ransomware administrators or creators charge a fee to affiliates for the use of their malware and may take a percentage of earnings from successful attacks. RaaS administrators will also support affiliates seeking further assistance during the process.
- **Infrastructure as a Service** - a third party will provide the cybercriminal with the infrastructure required to carry out a ransomware attack, such as email services or domain registration services that provide the cybercriminal with anonymity on the network.
- **Access as a Service** - offers cybercriminals network access to an already compromised machine or network.
- **Exploit kits** - assist in scanning networks for vulnerabilities, providing an entry point into the machine.
- **Post-attack services** - employees of ransomware administrators will assist victims through the payment process.

THE RANSOMWARE PAYMENT CYCLE

FLOW OF FUNDS

Following the money trail of ransomware is difficult. Cybercriminals use many methods to try and conceal the origin and destination of ransomware payments before the digital currency arrives at the final wallet under their control.

A wallet, or virtual wallet, is a collection of private keys and corresponding addresses (which enable the transfer of digital currency) under the control of an entity. Some of the ways criminals try and conceal their payments include:

- Use of privacy coins. Privacy coins are digital currencies that provide enhanced anonymity by obscuring the amount, destination and origin of transactions.
- Chain-hopping. This is where one digital currency is exchanged for another. The digital currency is moved from one blockchain to another, hence the term 'chain-hopping'.
- Directing a ransomware payment via multiple intermediary digital currency addresses, exchanges and mixers. Mixers increase anonymity by mixing the customer's digital currency with the transactions of others before being redirected back to the customer.
- Use of mule accounts. A mule account is created using a stolen or fake identity or, a legitimate account held by another party who is complicit in its use.

OBSCURING THE FLOW OF FUNDS FROM A VICTIM TO THE CYBERCRIMINAL

Cybercriminals will use sophisticated methods to try and obscure the true ownership and flow of funds. In the example below, wallet addresses 'B', 'C' and 'D' are part of a peel chain. A 'peel chain' is a transaction pattern created when a large amount of cryptocurrency is sent through a series of transactions. In each of these transactions, a small amount of the funds 'peels off' this chain of transactions to another address, typically held with a digital currency exchange. The goal is to make it difficult to tell where the funds originated.

This is a common method of trying to distance someone from the final wallet address.

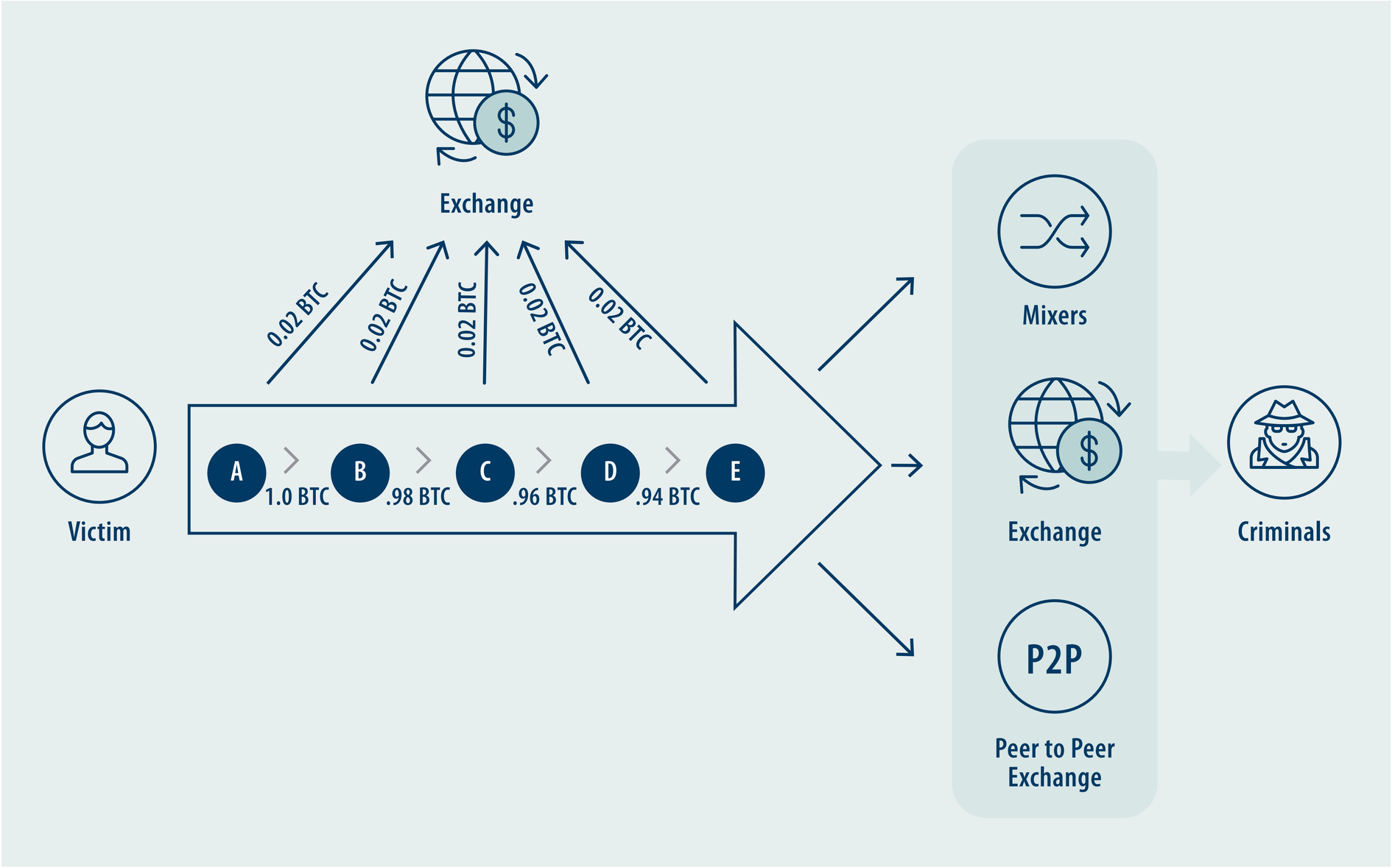
1. The victim is instructed to pay the ransom in a digital currency such as Bitcoin (BTC), to wallet address **A**. This wallet may have been created by the cybercriminal in another person's name.

2. The BTC from wallet **A** is sent to wallets **B**, **C** and **D**, and finally wallet **E**. Each of these wallets is controlled by the cybercriminal or their associates.

3. The cybercriminal sends the BTC to one or more other exchanges (often exchanges perceived to have weak or no know your customer (KYC) controls), mixers and peer-to-peer (P2P) exchanges to further obscure the money trail.

4. Finally, the cybercriminal will receive the BTC. They often receive this into a private wallet, or cash out the BTC using multiple exchanges and services.

Simple money trail example when viewed through blockchain analysis software:



At each stage of the process, criminals will often try to select a digital currency exchange they perceive to have weak KYC and AML controls. They may also use private wallet addresses that do not have KYC or identity verification safeguards. They will cash out their digital currency using services which are less likely to report suspicious activity, such as exchanges they perceive as weak, P2P exchanges or gambling services.

Cybercriminals may use part of the ransom they receive to pay for services that helped them carry out the ransomware attack, such as RaaS administrators and Post-Attack services.

Peer-to-peer (P2P) exchange - A platform that allows users to trade directly with each other and negotiate a price for the digital asset they are selling or buying.

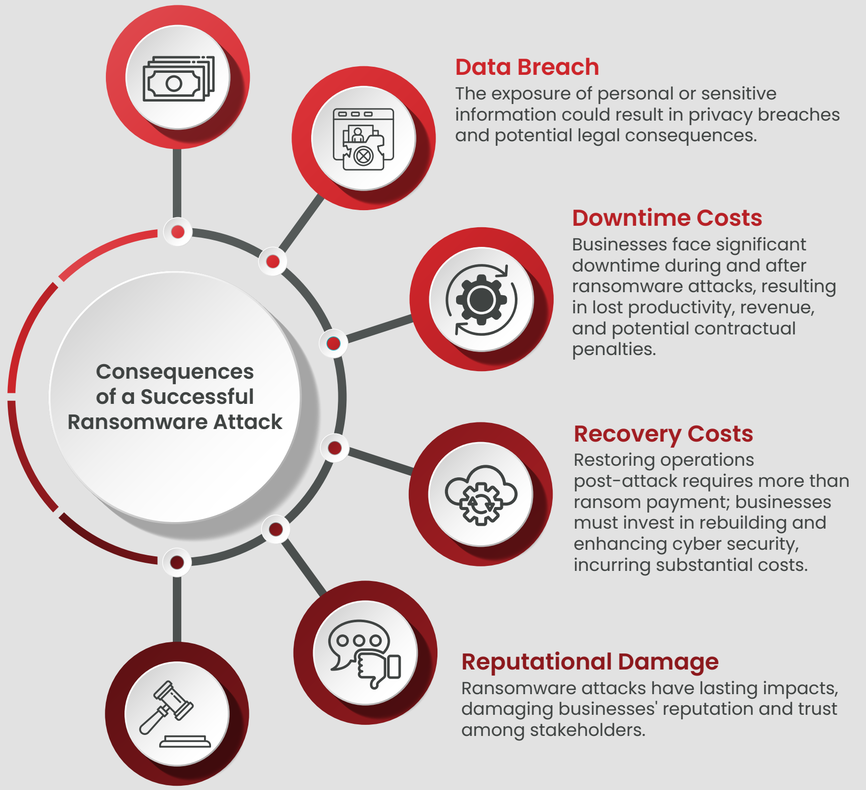
Consequences of A Successful Ransomware Attack

Ransomware attacks have far-reaching consequences that extend beyond the immediate loss of data or system. The ramifications of these attacks are profound and wide-ranging, impacting individuals, businesses, and even entire communities.

Here are some common consequences of ransomware attacks:

Ransom Payments

Ransom demands can be exorbitant, with no guarantee of receiving the decryption key even if paid.



Data Breach

The exposure of personal or sensitive information could result in privacy breaches and potential legal consequences.

Downtime Costs

Businesses face significant downtime during and after ransomware attacks, resulting in lost productivity, revenue, and potential contractual penalties.

Recovery Costs

Restoring operations post-attack requires more than ransom payment; businesses must invest in rebuilding and enhancing cyber security, incurring substantial costs.

Reputational Damage

Ransomware attacks have lasting impacts, damaging businesses' reputation and trust among stakeholders.

Legal Consequences

Data breaches from ransomware attacks can lead to legal action and fines under data protection laws for businesses that fail to safeguard sensitive information.

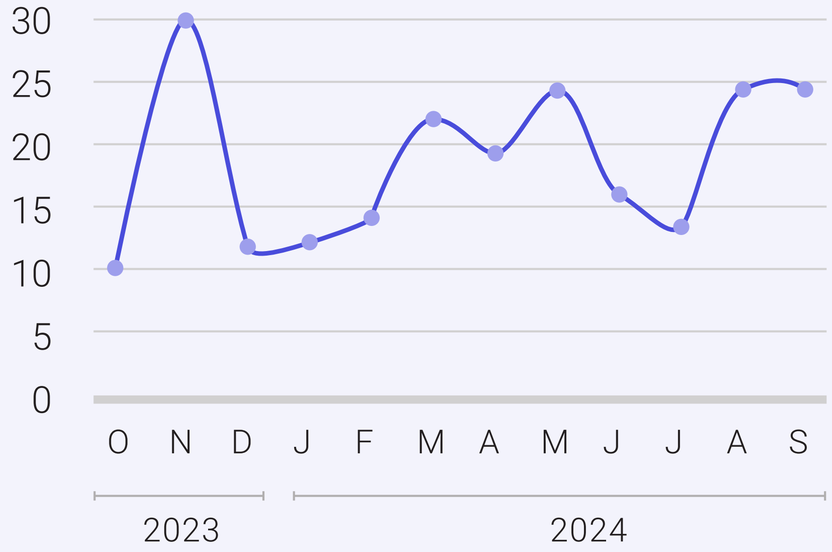
Ransomware: It's a Matter of "When," Not "If"

Data is a key competitive differentiator in the digital economy and has quickly become the crown jewel for modern enterprises. As such, data is increasingly targeted by cybercriminals in ransomware attacks. Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion U.S. dollars annually by 2025 and that a business will fall victim to a ransomware attack every 2 seconds by 2031. Thus, it's practically a matter of "when," not "if" your organization will be targeted.

Ransomware is on the Rise

⬆ 70%	Increase in observed events[1]
⬆ 64%	Ransomware attacks on the financial services sector[2]
⬆ 4,374	New victims over the last 12 months[3]

Events | Last 12 Months



Ransomware events in the financial sector over the last 12 months. Source: eCrime Threat and Risk Intelligence Services[4]

Statistics

5,070 ransomware attacks were recorded in 2023, marking a 55% increase from 2022[1]...

20% of ransomware costs are attributed to reputation damage[2]...

$1 Billion in ransomware payments were surpassed in 2023[3].

Examples of Ransomware Attacks

LockBit Attack on Royal Mail, January 2023[4]

In January 2023, the LockBit group targeted Royal Mail, causing chaos in international mail delivery. The attack crippled crucial services like the parcel tracking website and online payment system. Printers at the Royal Mail distribution centre in Northern Ireland churned out copies of LockBit's orange ransom note.

Despite threats to post stolen data online, Royal Mail refused to pay the ransom, leading to the publication of the data.

Clop Group Attack Through Vulnerability in MOVEit Transfer, June 2023[5]

In June, the notorious Clop group, known for its February attacks on Fortra GoAnywhere MFT, exploited a vulnerability in Progress Software's MOVEit Transfer. Despite Progress fixing the vulnerability (CVE-2023-34362) by May's end, not all clients applied the patches promptly.

This attack, one of the year's largest incidents, targeted various organisations, including oil giant Shell and the BBC.

In February 2023, VMware ESXi hypervisors were targeted by attacks designed to deploy ransomware by taking advantage of an OpenSLP (Service Location Protocol) heap-overflow vulnerability that potentially allows remote code execution. Ransomware attacks leveraging this vulnerability were detected globally, particularly in Europe, beginning in December 2022.

CASE STUDY 1: RANSOMWARE EVIL

REvil (short for Ransomware Evil), also known as Sodinokibi, is a type of RaaS, 'leased' to affiliates wishing to carry out an attack. Once criminal affiliates have infiltrated a network, stolen as much data as possible and gained administrative access, REvil is deployed and a ransom demand is made. REvil affiliates typically use double extortion, threatening to post the data on a dedicated website called *Happy Blog*.

In May 2021, affiliates using REvil attacked JBS, the world's largest meat processing company. The ransomware affected servers supporting North American and Australian IT systems, bringing JBS's operations to a halt. The shut-down saw temporary lay-offs at some plants in Australia and farmers reported that shipments of livestock were cancelled. JBS's back-up servers were not affected and, with the assistance of a cybersecurity firm, operations resumed within a few days. Despite this, JBS elected to pay a $14.2 million ransom in Bitcoin to avoid unforeseen implications and data extortion.

In July 2021, REvil's website and *Happy Blog* shut down, vanishing from the internet and leaving many victims unable to recover their data.

CASE STUDY 2: WANNACRY

In May 2017, the ransomware WannaCry infected more than 230,000 computers in 150 different countries. The malware used took advantage of weaknesses in the Microsoft Windows operating system using a hack known as EternalBlue.

The perpetrators demanded $300 worth in Bitcoin, later increasing this to $600, and threatened to delete all files on the victim's system, if payment wasn't received. Some victims chose to pay the ransom. It is unknown exactly how many victims were able to recover their data.

The WannaCry ransomware campaign was estimated to have collectively cost victims $4 billion and dangerously impacted the health system, particularly in the UK where ambulances were rerouted, leaving people in need of urgent care.

Using financial intelligence from financial services businesses, AUSTRAC used specialised tools to provide the Australian Government with intelligence regarding the financial impact of WannaCry.

Top 3 Ransomware Families[6]

LockBit3
LockBit3 operates under a Ransomware-as-a-Service (RaaS) model and appeared around September 2019. This ransomware primarily targets large enterprises and government entities across multiple countries. Interestingly, it avoids targeting individuals in Russia and nearby countries.

8Base
The 8Base group has been around since at least March 2022 but became more famous in mid-2023 for being extra active. They use different kinds of ransomware, with one called Phobos being quite popular. What's notable about them is how they use advanced techniques and double extortion tactics.

Akira
Akira Ransomware showed up at the start of 2023 and doesn't pick sides between Windows and Linux computers. It spreads through things like infected emails or flaws in virtual private networks (VPNs). When it infects a computer, it scrambles up files and adds a ".akira" tag to their names. Then it asks for money to unscramble them.

[6] Checkpoint 'January 2024 Most Wanted Malware'

Phase 1

Phase 2

Access systems

Attack vectors include:

- Social engineering
- Compromised credentials
- Zero-day exploits
- Open network shares
- Remote access services
- Public-facing application and supply chain vulnerabilities
- Untargeted “drive-by downloads”

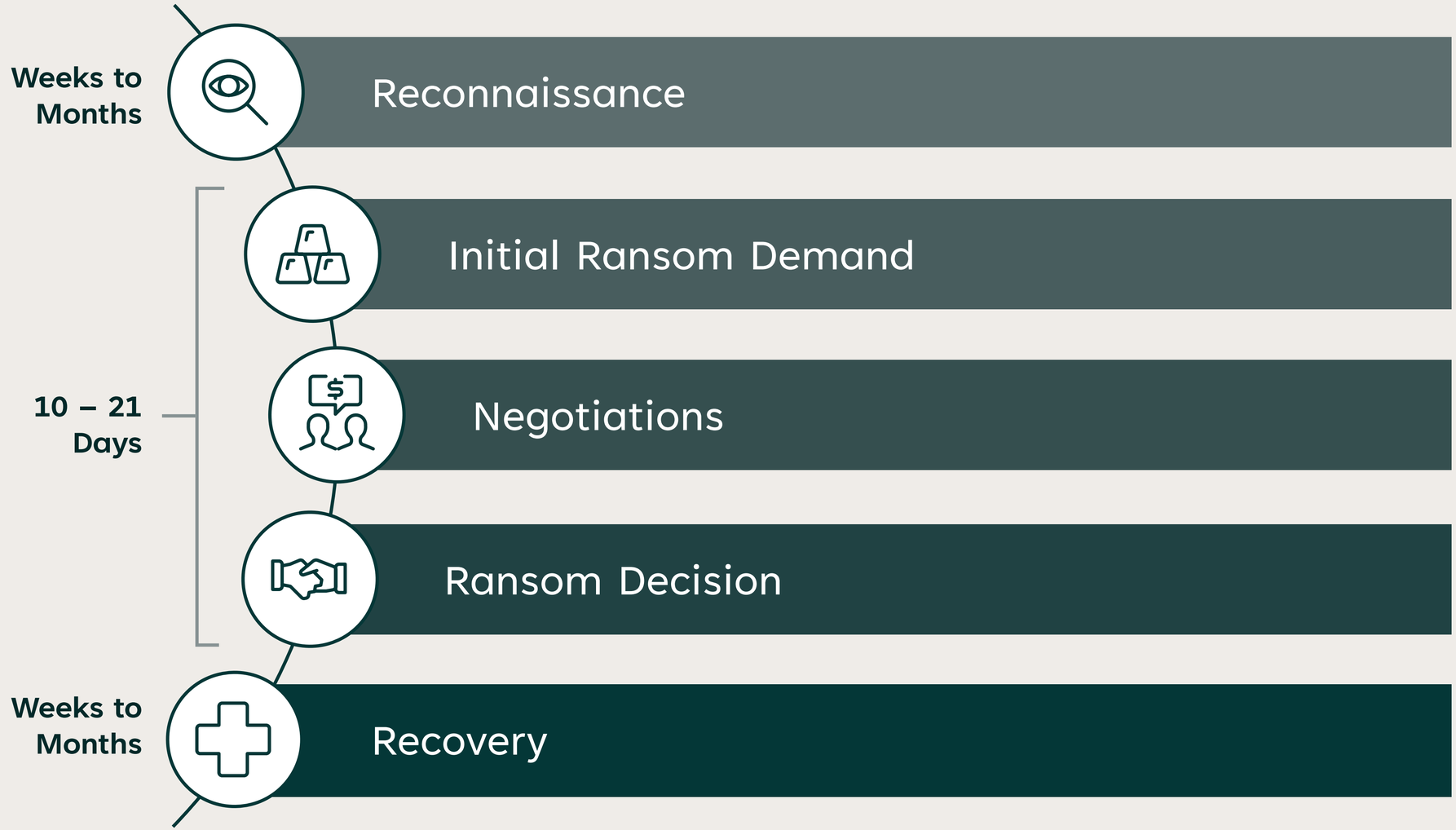
Deploy malware

- Infect computers
- Encrypt files
- Spread malware through systems, drives, and devices
- Disable security and backup systems
- Exfiltrate data

Steal data and issue demands

- Hold data hostage until payment is made
- Public data release to increase pressure
- Customer notification of attack

Figure 1 – Ransomware Attack Phases



Ransomware Attack Phases

Figure 2 – Cyber Incident Response Teams

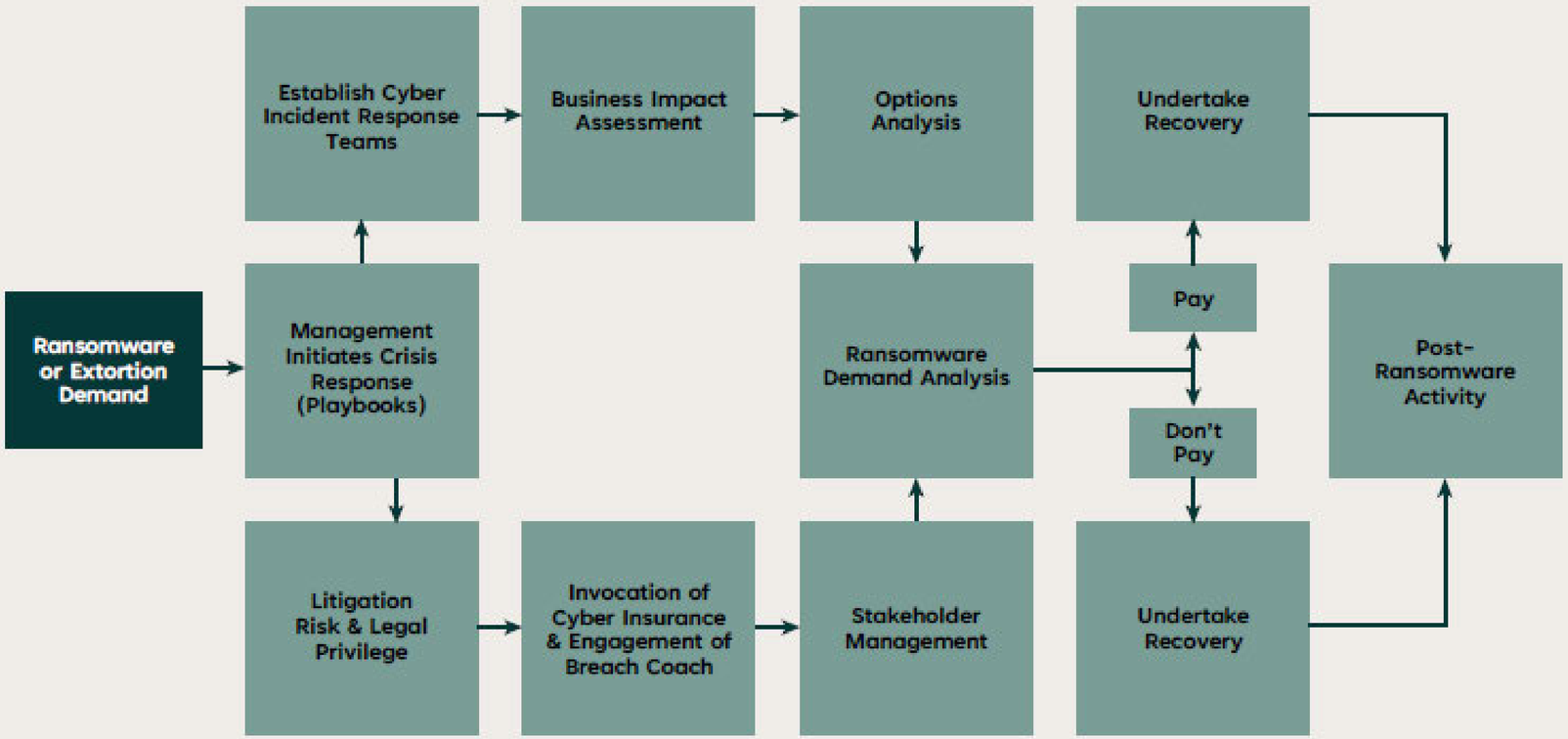


Figure 3 – Cyber Incident Response Teams

Executive Team

- Develop immediate situational awareness regarding the nature of the incident
- Provide direction and guidance to the Business Continuity Team, Incident Response Team, and staff to respond to the incident
- Manage stakeholder relations
- Remain informed to make key decisions and delegate response activities

Business Continuity Team

- Gather accurate facts regarding the nature of the incident
- Respond to the incident, managed by the Business Continuity Team, and supported by the Incident Response Team
- Assess the likely enterprise-wide impacts
- Provide recommendations to the Executive Team on how the organization should respond

Incident Response Team

- Receive and manage incident notification
- Conduct immediate incident triage
- Inform Business Continuity Team and Executive Team of the nature of the outages and how the incident impacts critical services

Figure 4 – Key Stakeholders

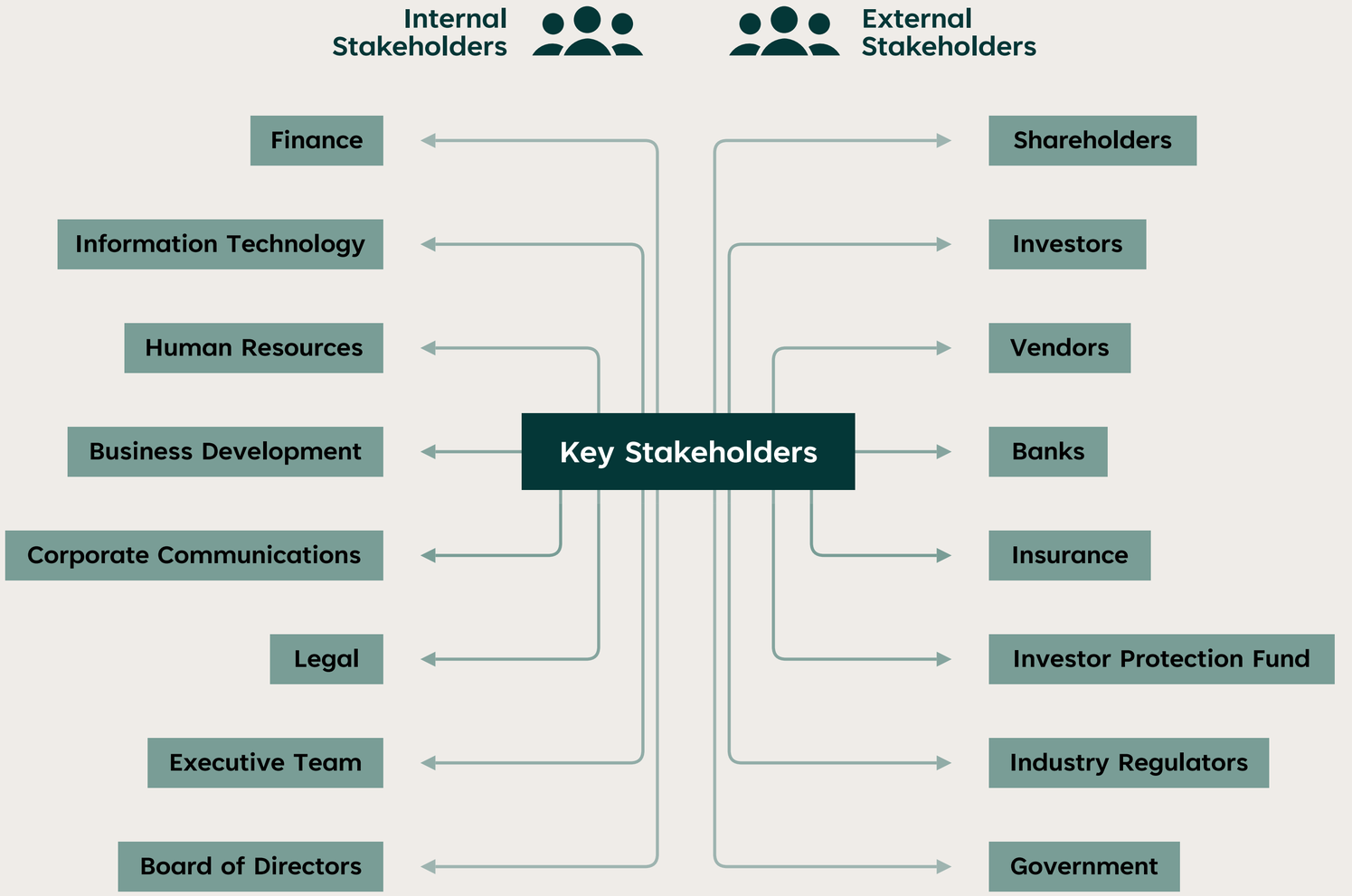
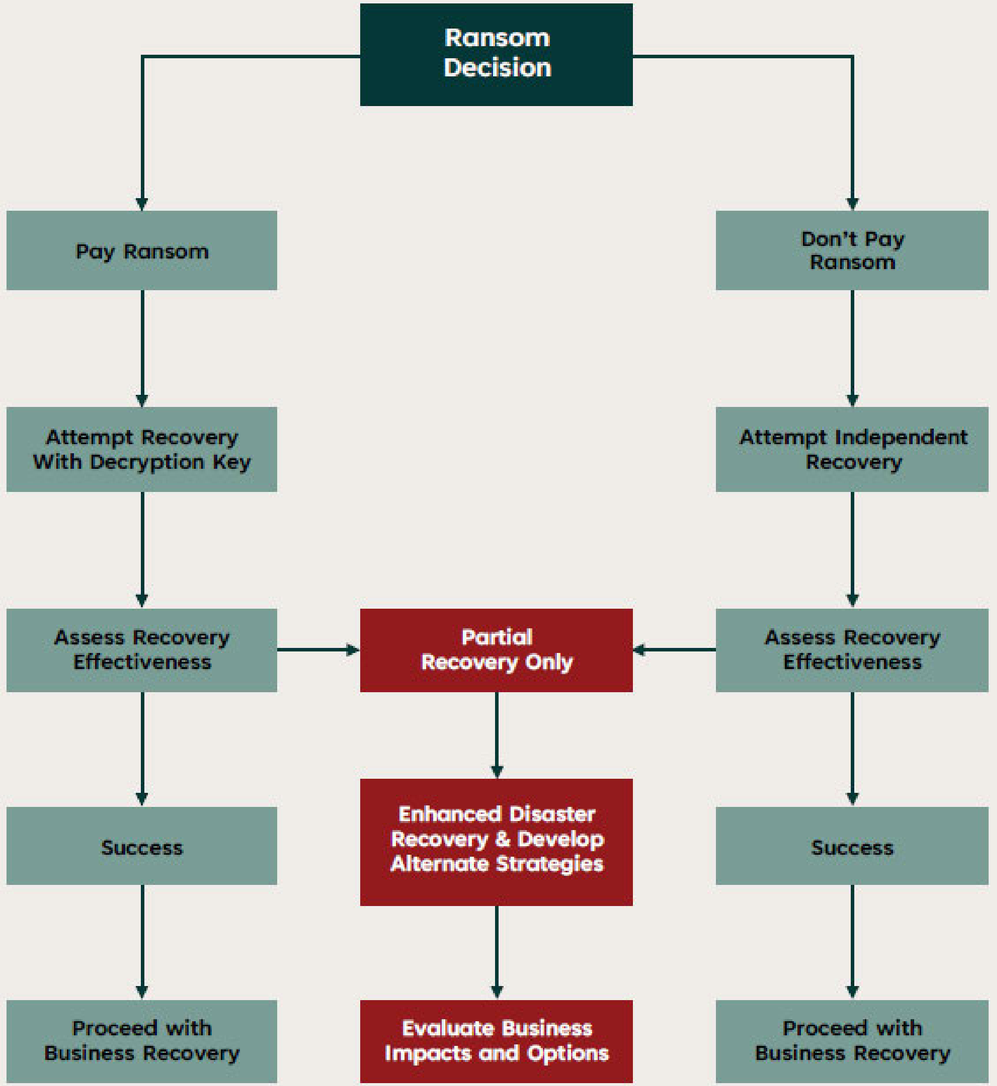


Figure 5 – Options Analysis Model



Cyber Fundamentals Checklist:

1. Isolate, test, and exercise backups

2. Update software, automate patching

3. Require MFAs and strong passwords

4. Train employees

5. Write and exercise incident response plan

6. Use EDRs, DLPs, and firewalls

1 Use non-erasable and non-modifiable backup systems to duplicate data and system configurations

> Regularly back up critical data and system configurations to isolated environments. If segmentation is in place and backups are preserved, the impact of an attack may be manageable.

> Test backups at least annually in real-world technical exercises to ensure backups can be restored quickly and completely in the event of an attack. Cloud computing makes testing and restoration easier, but some firms may only be able to test restoration of certain critical functions. A robust restoration plan, likely on a separate new infrastructure, will take a great deal of effort, especially in large firms.

2 Regularly update and patch software

> Updates and patches reduce initial infection potential from both technical and social engineering attacks.

> Where the risk is acceptable, automate patch management to ensure consistent application of updates across all systems, reducing human error and delays.

> If patching is delayed, develop standard processes to implement mitigation strategies like virtual patching utilizing a web application firewall (WAF).

3 Use a zero-trust and least privilege policy with multi-factor authentication, and require strong passwords for every employee, device, and account

> Implement a zero-trust approach where all users and devices, inside or outside the network, are authenticated, authorized, and continuously validated before gaining access to applications and data.

> Leverage resources like NIST 800-207 Zero Trust Architecture to develop your strategy.

4 Train employees on their role in cybersecurity

> Conduct regular training sessions to educate employees on the latest cybersecurity threats, including phishing, social engineering, and the dangers of clicking on unknown links or downloading unverified attachments. People who understand the potential impact of clicking on external links or reusing passwords will generally take more care about their activities.

5 Develop an incident response plan specific to ransomware attacks

> Detail the steps to be taken immediately upon detection, including isolation, communication, and recovery procedures.

> Conduct regular tabletop exercises and full-scale drills to ensure that all team members are familiar with the response plan and can act quickly and effectively under pressure. Exercises allow you to review and update plans to adapt to evolving threats and changes in your organization.

6 Implement EDR, DLP, and firewall solutions

> Implement Endpoint Detection and Response (EDR) solutions. EDR solutions monitor endpoints (computers, servers, mobile devices) for suspicious activity, and respond to threats in real-time to disrupt ransomware before it can spread.

> Implement Data Loss Prevention (DLP) solutions. DLP solutions monitor and control the movement of sensitive data, helping to prevent exfiltration attempts by cybercriminals.

> Use firewalls, configured closed by default, with active blocking. When deploying firewalls, look at internal segmentation as well. One example is agent-based microsegmentation augmentation of traditional firewalls, which minimizes the potential impact of encryption malware. Another key control for exfiltration monitoring is a SWG/DNS firewall that can detect data being stolen and prevent users from going to malicious websites.

How to Develop and Implement a Crisis Management Plan

Crisis Management Plan Checklist:

> Policy on paying ransoms
> Crisis management framework
> Roles and responsibilities

Ransomware presents a unique challenge in that the time between detection and impact – the flash to bang – is essentially zero. Unlike cyber incidents that unfold over weeks, ransomware requires immediate execution of crisis management plans in real-time, without some of the normal phases of mitigation.

While the technical controls mentioned above are critical to defending against and responding to a ransomware attack, process-based capabilities are equally important. A crisis management plan must involve the entire leadership team and include a clear policy on whether to pay the ransom. If your legal team approves paying, you'll need to have a contract with a payment negotiator and be prepared to purchase cryptocurrency – most criminals require ransom payment in crypto.

Next, consider how to respond effectively if an attack is successful. You will need both a strategic crisis management plan and a tactical response plan. The ISO 2700 is a great framework, as is the NIST 2.0 crisis management framework (and it's the baseline for all FFIEC guidance). That framework helps you plan the essential factors of strategic and tactical responses.

As you build out the plan, identify the Incident Response (IR) team. It should include functions from across the organization. All their actions should be driven by the Responsible, Accountable, Consulted, Informed (RACI) model.

Crisis Management Team

Senior Leadership	> Chief Executive Officer > Chief Financial Officer > Board of Directors
General Counsel and Legal/ Risk Management Consultants	> General Counsel > External cyber SME advisor > Ransomware consultants/payment experts > Law enforcement agency (LEA) liaison > Cyber insurance liaison
Communications/ Public Relations	> External cyber incident SME
Operations	> IT leadership > Call centers, customer service, and related functions > Business continuity planning team
InfoSec	> IR/SOC > Threat intel > Forensics teams > External forensics experts
Vendor Management (lead team if ransomware impacts vendors)	> Third-party risk management
Human Resources	> Employee communications > Staff support and counseling

Managing the risk of ransomware infection

The US National Institute of Standards and Technology's Cybersecurity Framework includes five high level functions for preventing and managing a ransomware attack: Identify, Protect, Detect, Respond and Recover.

We have used this framework to develop a systematic process to help our clients prevent and manage ransomware attacks, including the AIG CyberEdge pre-loss services.

Preventing infection:

IDENTIFY

Preventing infections from happening starts with identifying:

- The organisation's physical and software assets and the business environment that the organisation supports, such as its role in the supply chain and place in the critical infrastructure sector.
- Asset vulnerabilities, threats to organisational resources, and risk response activities.

These need to be considered for the entire asset inventory including unmanaged devices in relation to the reliability, availability and serviceability of the IT and OT.

Preventing infection:

PROTECT

Effective protection means implementing a set of protective processes and procedures to maintain and manage the security of information systems and assets. Different aspects should be considered, including:

- The patching of IT and OT.
- The creation and testing of online and offline data and system information backups, stored in different locations.
- Network segmentation and system hardening.
- Staff empowerment through awareness and training, including role-based and privileged user training.

Preventing infection:

DETECT

Detecting anomalies and events is the third step to successfully preventing malware infections. This includes:

- Implementing security continuous monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures, including network and physical activities.
- Maintaining detection processes to provide awareness of anomalous events.

Ensuring rapid detection starts with establishing a Security Information and Event Management (SIEM) or even a Security Operation Center (SOC) functions with strong threat intelligence. Having clear network and endpoint visibility helps your organisation to make the detection easier.

RESPOND

before and after an infection

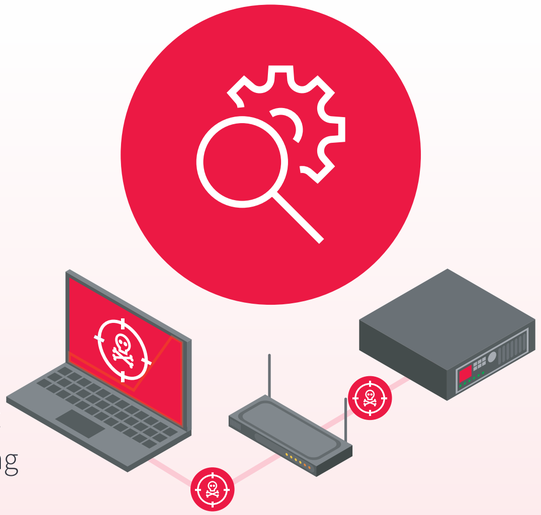
Before an infection, a well-developed response mechanism within the organisation helps to mitigate the potential damage during a ransomware infection. This can include:

- Performing mitigation activities to prevent expansion of an event and to resolve the incident.
- Implementing improvements by incorporating lessons learned from current and previous detection or response activities.

All this requires a Cyber Security Incident Response Team (CSIRT) that has developed and established a tested Incident Response Plan.

After an infection reactive measures must be initiated, including:

- Ensuring response planning processes are executed during and after an incident.
- Managing communications during and after an event with stakeholders, law enforcement agencies, and external stakeholders as appropriate.
- Conducting analysis to ensure effective response and support recovery activities, including forensic analysis, and determining the impact of incidents.



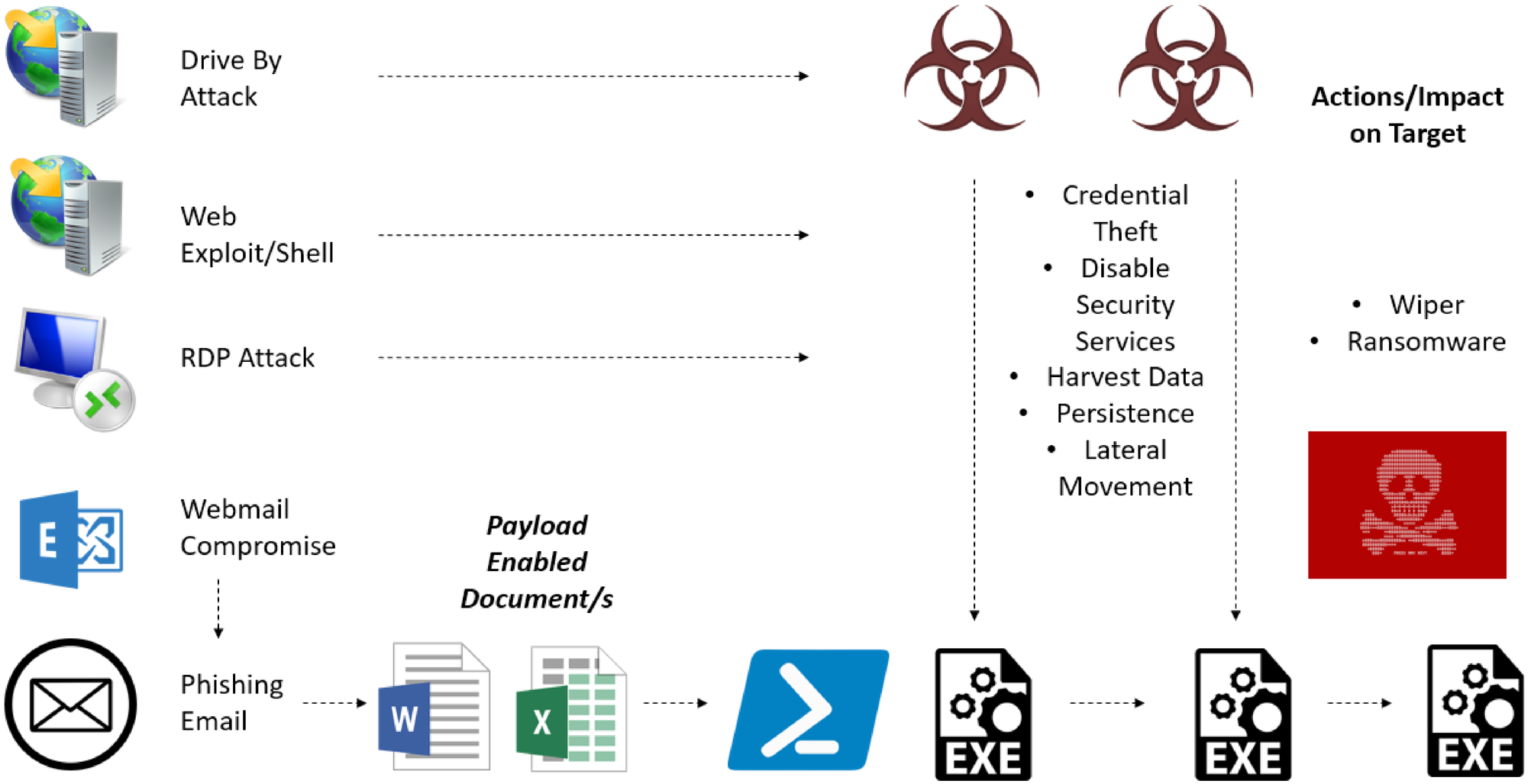
RECOVER

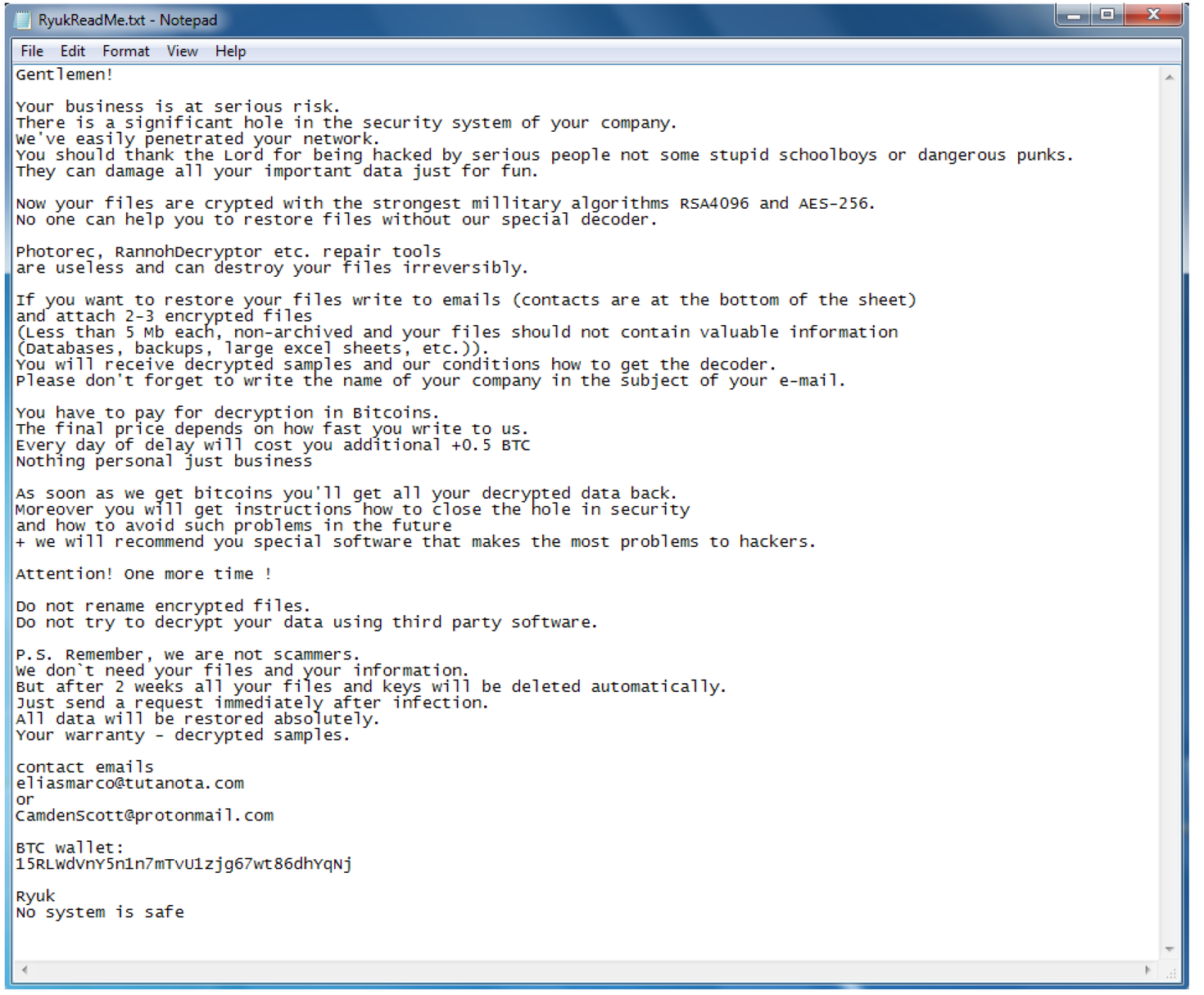
after a ransomware attack

For optimum business recovery after a cybersecurity attack, it is essential to execute plans for resilience and restore any capabilities or services that were impaired due to the incident. Timely recovery to normal operations will reduce the impact of a ransomware infection.

Organisations need to implement recovery planning processes and procedures to restore systems and/or assets affected by Cybersecurity incidents and recover data from (offsite) backups.

Common Ransomware Attack

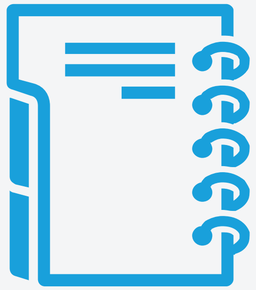



RyukReadMe.txt - Notepad
File Edit Format View Help
Gentlemen!
Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.
Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.
Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.
You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business
As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.
Attention! One more time !
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.
contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com
BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj
Ryuk
No system is safe

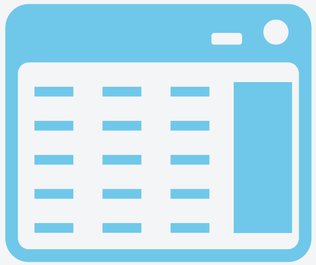
User receives spammed message with archived attachment

Attachment is downloader malware that connects to URLs hosting the crypto-ransomware

The crypto-ransomware is downloaded onto the computer

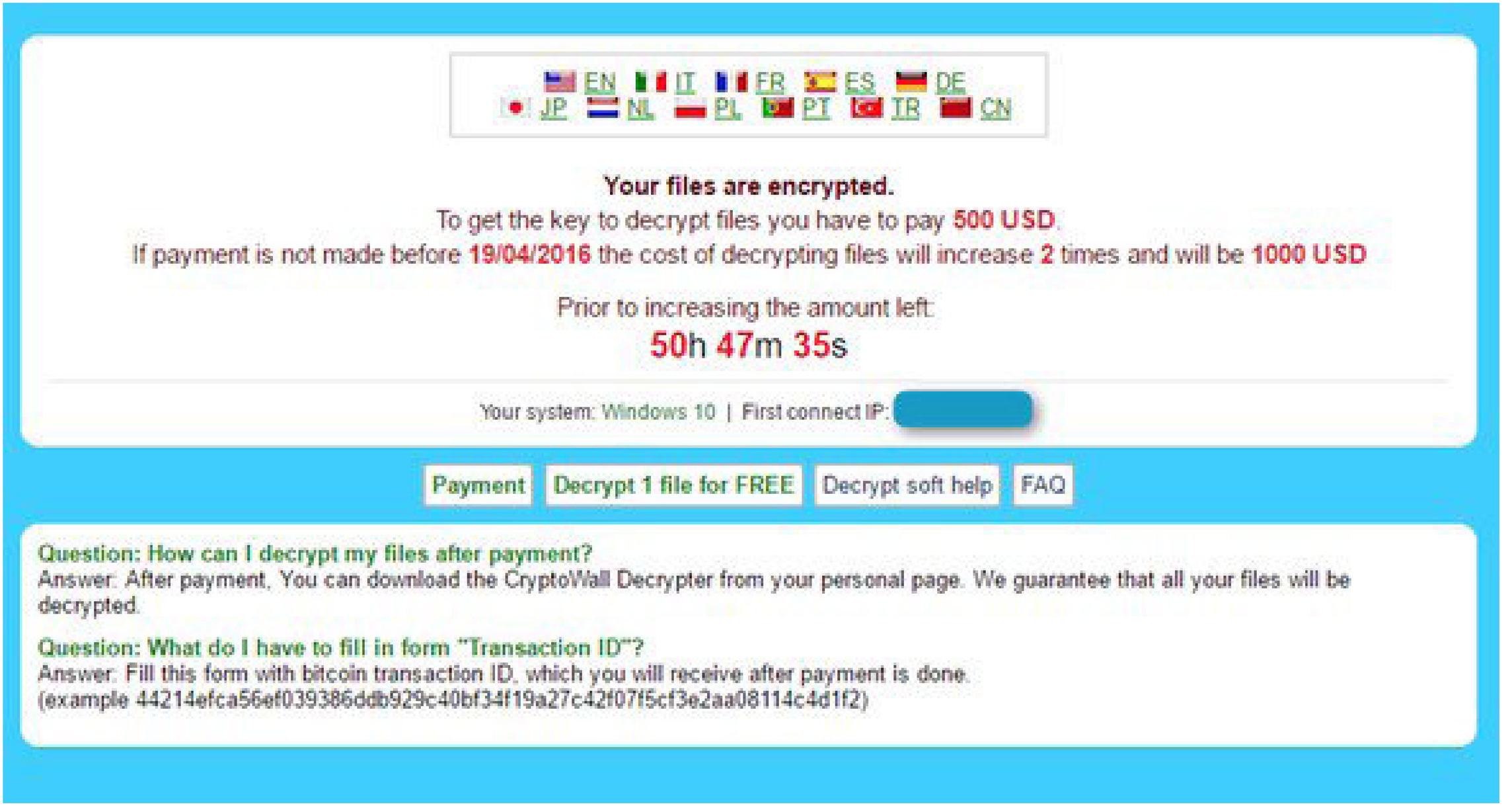


Files in the affected computer are encrypted



A ransom message is displayed, stating the deadline and amount

Victims must use Tor browser to pay using Bitcoins


EN IT FR ES DE
JP NL PL PT TR CN
Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD.
If payment is not made before 19/04/2016 the cost of decrypting files will increase 2 times and will be 1000 USD
Prior to increasing the amount left:
50h 47m 35s
Your system: Windows 10 | First connect IP:
Payment
Decrypt 1 file for FREE
Decrypt soft help
FAQ
Question: How can I decrypt my files after payment?
Answer: After payment, You can download the CryptoWall Decrypter from your personal page. We guarantee that all your files will be decrypted.
Question: What do I have to fill in form "Transaction ID"?
Answer: Fill this form with bitcoin transaction ID, which you will receive after payment is done.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

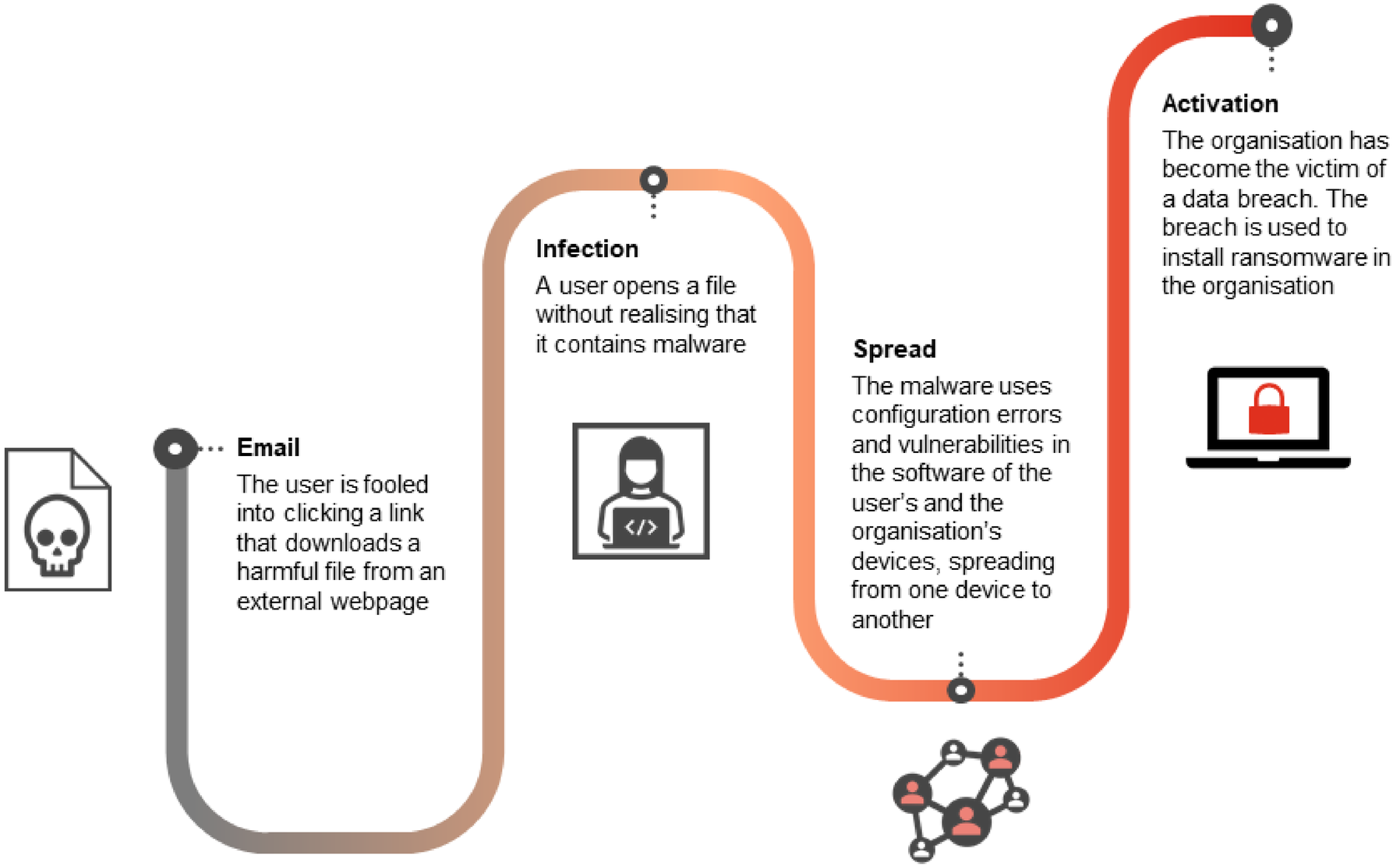


Figure 2: Example of a ransomware attack

Best Practices for Preventing Ransomware Attacks

Thankfully, numerous strategies exist to prevent against ransomware attacks. As technology evolves, adhering to fundamental cyber security practices and maintaining vigilance is key to safeguarding yourself and your business.

Backups

Follow the 3-2-1 backup rule: keep three copies of data in two locations, with one copy stored off-site for disaster recovery.

Employee Training

Educate employees on spotting phishing emails, suspicious links, and avoiding unknown attachments.

Software Updates

Regularly update software to install the latest patches, preventing exploitation of system vulnerabilities by cyber attackers.

Access Control

Employ robust access management to limit unauthorised access, thereby reducing potential entry points for ransomware.

Email Security

Use email security measures to block malicious executables, spam, phishing, and other common email-based ransomware attacks.

Anti-Virus

Deploy comprehensive anti-virus and anti-malware software to scan for, detect, and respond to cyber threats effectively.

Firewalls

Utilise firewalls as the first line of defence against external attacks, protecting against both software and hardware-based threats.

Network Segmentation

Divide your network into logical segments to enable isolation in the event of a ransomware attack.

Dark Web Monitoring

Stay ahead of potential threats by monitoring the dark web for any signs of compromised credentials belonging to your organisation.

Security Testing

Regularly conduct cyber security vulnerability assessments to adapt to evolving ransomware tactics and enhance security measures.

Post-Incident Activity

Post Crisis Analysis

Following the incident, organizations should seize the opportunity to investigate the cause of the crisis, looking for and acting on evidence of wider cultural problems that may have caused it, and identifying opportunities for change to gain competitive advantage and greater resilience.

Strengthened Defenses - Following the conclusion of the event, the organization should immediately begin steps to minimize the likelihood of a reoccurrence. Many of those companies that reported a cyber attack between 2021-2022 also reported that they experienced more than one attack. Given the publicity that accompanies a cyber attack, the organization can be assumed to have some form of vulnerability that allowed the initial attack. Failure to address that original vulnerability can lead to a follow-on attack.

Regulatory Reporting - Regulatory reporting including breach reporting may be required. In certain jurisdictions, in the case where a ransomware attacker exfiltrated data and claimed to have destroyed it as part of the ransom negotiations, a company may still need to make a breach report if there is no concrete evidence that the data was destroyed.

After Action Report - Document how the organization responded to the crisis and how best to improve the responses for future events. This process should also be directed by the General Counsel under legal privilege.

Client Management - Engage with key clients and third parties to manage relations to prevent client flight and long-term reputational damage.

Crisis Plans - Review crisis plans, processes and competencies to determine:

- Did processes work and did information flow well?
- Was communication with stakeholders adequate and timely?
- Were plans adequately prepared pre-crisis to assist in its management?
- Were regulatory requirements addressed accurately and in a timely fashion?

Lessons Learned - The Executive Team should ensure that the Business Continuity Team and Incident Response Team undertake a post-crisis lessons learned investigation led by an appropriately experienced senior executive. Key areas of focus for this process should include an evaluation of the nature of the threat the organization faces, the effectiveness of the organization’s incident response measures, and an assessment of the Board’s role in crisis response.