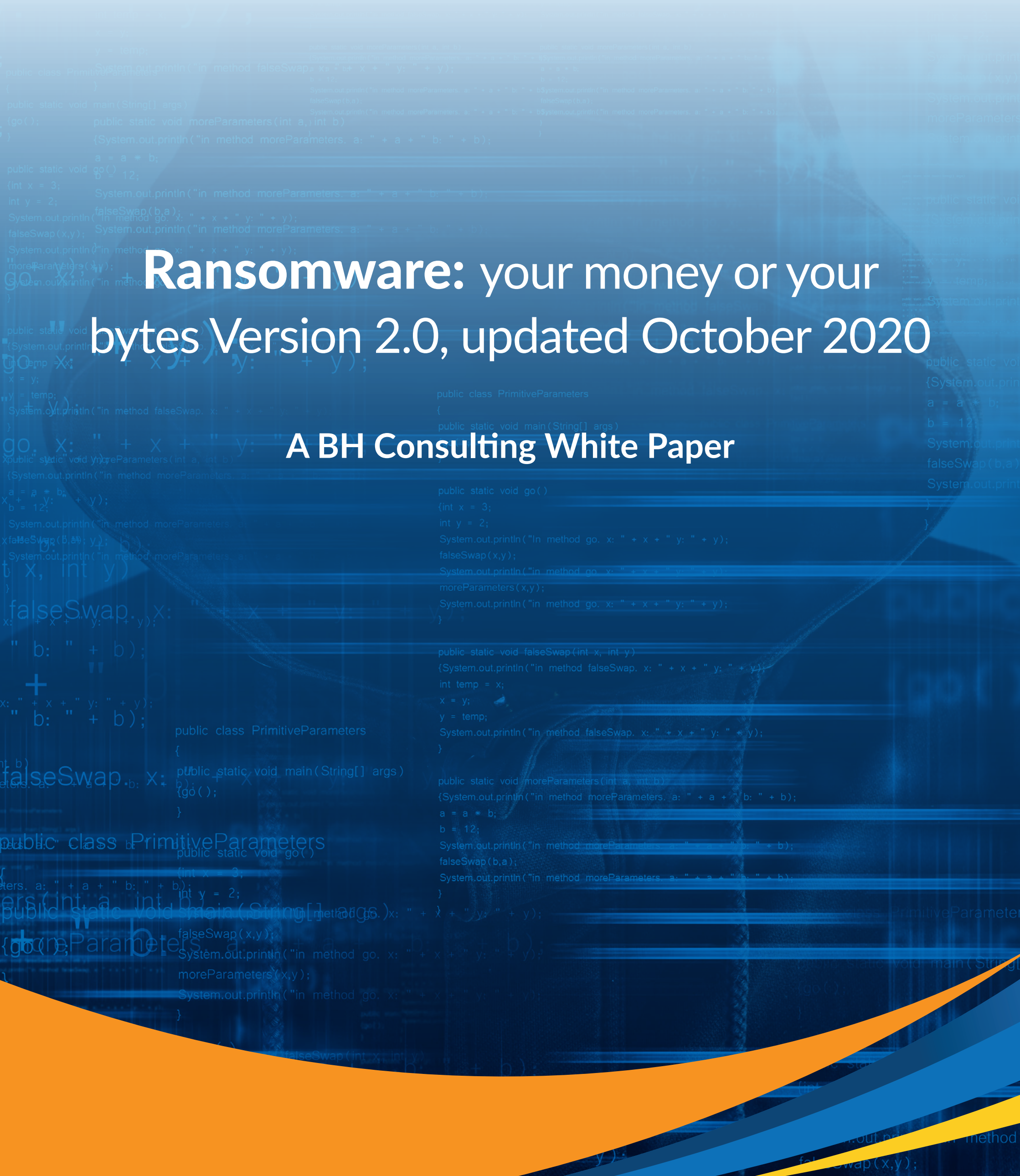
BHConsulting

Your Trusted Cybersecurity Partner



Ransomware: your money or your bytes Version 2.0, updated October 2020

A BH Consulting White Paper

About this guide

Over the past five years, few cybersecurity threats have matched the reach and damage of ransomware. Worldwide, it has cost businesses collectively billions of euro[1][2][3]. According to the widely respected 2020 Data Breach Investigations Report[4], ransomware was responsible for 27 per cent of all malicious software infections in 2019, and that figure has risen since the year before. In the first nine months of 2019, over 600 US government entities suffered a ransomware incident.

This type of malware can effectively punish its victim many times over:

- It costs money and time to fix
- It disrupts normal operations, potentially for a number of weeks depending on their business continuity plan
- If the compromised files include sensitive personal information, a ransomware infection may also be considered a data breach under the EU GDPR
- Some ransomware gangs also threaten to release the compromised data on the internet if they are not paid.

We created this white paper to help companies and public agencies of all sizes to recognise signs of a possible ransomware infection, and take measures to take to prevent it from spreading and causing damage.

This document details several recommendations to help you in reducing the likelihood of future infection by ransomware, or indeed any other computer viruses or malware.

By following the steps in this paper, we hope companies will avoid having to face the possibility of paying to get their data back. BH Consulting strongly advises never to pay the ransom.

We first published this document in 2017 and we have updated it now to reflect changes in the techniques that criminals use, and the additional risk posed by working from home, as many people have had to do during the COVID-19 pandemic.

[1] https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/
[2] https://www.infosecurity-magazine.com/news/ransomware-costs-may-have-hit-170/
[3] https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/
[4] https://enterprise.verizon.com/resources/reports/dbir/

The first section is a high-level explanatory guide that outlines the nature of the risk for managers; the second is aimed at a technical audience and includes some of the measures to take that mitigate the risk of an infection.

In addition to this white paper, we recommend you also review the advice in the following guides:

- NIST SPECIAL PUBLICATION 1800-11 - Data Integrity Recovering from Ransomware and Other Destructive Events[5]
- Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center joint Ransomware Guide[6]
- Microsoft - Human-operated ransomware attacks: A preventable disaster[7]
- The UK National Cyber Security Centre: Mitigating Malware and Ransomware Attacks[8].

What is ransomware?

At its heart, ransomware is simply another form of a computer virus, albeit a very potent one. It is an aggressive form of malicious software that criminals use to infect computers and encrypt the data on them. This blocks the victim from accessing their own data unless they pay the criminals to unlock it.

Ransomware is sometimes known as crypto-ransomware. It is not a new threat but has become more widely used among criminals simply because attacks are easy to execute and can be highly profitable. Cryptocurrencies have helped to enable this type of crime because they allow criminals to receive money from victims in a way that's practically untraceable.

Ransom demands vary, but they can be as high as multiple thousands of euro. In return for payment, attackers promise to give a decryption key that unlocks the victims' data. (We will make the point here and elsewhere: paying the ransom is not a guarantee of getting this data back.)

- To increase the pressure on victims, some criminals threaten to deny access to the data permanently unless they receive the ransom within a set period of time
- Sometimes, the cost to decrypt the data increases as the deadline gets closer
- In other cases, attackers threaten to release the stolen data on the internet in the event of non-payment, with the risk of disclosing confidential or sensitive information.

[5] https://csrc.nist.gov/publications/detail/sp/1800-11/final
[6] https://www.cisa.gov/publication/ransomware-guide
[7] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
[8] https://www.ncsc.gov.uk/blog-post/rebooting-malware-and-ransomware-guidance

How does ransomware infect its victims?

Many of the methods that criminals use to infect a computer with ransomware are the same as for other types of malware or viruses. One of the most common ways is via phishing emails which contain attachments that launch the infection when the recipient opens them.

Other times, the emails have a link to a website that infects the victim's machine when they visit the site. These phishing-style emails tend to be sent indiscriminately in large numbers, so criminals only need a small fraction of victims to open the email to be successful.

In other cases, criminals attack weak points in the remote desktop protocol (RDP), in Citrix gateways, and in some virtual private network (VPN) tools. They have used brute-force methods, a technique using trial-and-error to obtain user credentials, known software vulnerabilities in these systems, or credentials purchased on darknet marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware including ransomware to infect their victims.

The COVID-19 crisis has made this type of attack more prevalent, because many organisations enabled remote working for their staff during restrictions on gathering in offices. In many cases, they didn't properly configure and secure their remote access technology, or the organisations' IT teams weren't able to ensure the latest software patches were installed on all systems.

Cybercriminals can also take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware, as happened when they exploited vulnerabilities in two remote management tools used by managed service providers (MSPs) to deploy ransomware on the networks of customers of at least three MSPs.

What damage can it do?

Part of what makes ransomware so devastating is how it can bring normal business operations to an almost-complete halt. When various UK healthcare facilities were struck by the WannaCry ransomware in 2017[9], they were forced to suspend operations and go back to using pen and paper.

Garmin, the wearable technology and fitness tracking company, suffered an infection from the WastedLocker ransomware in summer 2020[10]. This caused an outage that lasted for days, affecting the company's email systems, and all of its consumer-facing online services. In effect, its entire business model of logging customers' workouts was unavailable.

[9] https://www.tripwire.com/state-of-security/latest-security-news/wannacry-affected-34-of-nhs-trusts-in-england-investigation-finds/

Sometimes the victims are not limited to the ones infected by ransomware. An attack on the cloud-based education and financial management provider Blackbaud, discovered in May 2020, resulted in data stolen from at least two universities in Ireland – NUI Galway and NUI Maynooth[11] – as well as 10 in the UK, US and Canada, along with some charities.

As well as the immediate effects of ransomware, the longer-term impact can be devastating: the currency exchange company Travelex entered into administration, the UK form of bankruptcy, having suffered a ransomware attack in late December 2019 which left it unable to resume business for almost three weeks[12].

Norsk Hydro is one of the world's largest aluminium companies; it became a case study for how to respond to a ransomware incident after suffering a crippling infection in 2019. Even as it recovered many of its key systems within a week – and maintained an impressive level of open communication with the public – nevertheless it emerged that the attack cost the company an estimated €40 million in the first week alone[13].

This money goes on everything from staff overtime to engaging with external consultants and experts to investigate the incident and bring key systems back up.

For other victims such as AP Moller-Maersk, the shipping company, the costs of remediating the infection were even higher, running into hundreds of millions[14]. That's before we get to the cost of getting data back if the victim chooses to pay ... To pay or not to pay; is that even a question?

When it comes to ransomware, law enforcement agencies and security consultants have consistently advised victims not to pay up. There are many good reasons for this:

- Paying extortion effectively amounts to giving the extortionists money not to commit crime, and enables them to become better funded, more sophisticated, and more motivated
- Victims who pay are more likely to be infected again (for example, Pitney Bowes and Toll Group both suffered second ransomware infections within months of a first incident[15])
- When an organisation pays, the cost of dealing with the incident can double[16]
- Paying up is not a guarantee of getting data back. Figures vary, but a percentage of organisations weren't able to access their data even after they gave in and sent money
- If a company fails to address the underlying issue that facilitated the first breach, they may still be vulnerable to attack
- Criminals could leave malware on the victim's network that enables them to attack again.

[10] https://threatpost.com/garmin-suffers-ransomware-attack/157698/
[11] https://www.thejournal.ie/maynooth-university-cyber-attack-blackboard-random-paid-5194864-Sep2020/
[12] https://www.infosecurity-magazine.com/news/travelex-forced-administration/
[13] https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/
[14] https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

Some companies may look to their insurance policies, but a word of warning: this might not come close to covering the cost. Norsk Hydro, one of the most high-profile ransomware victims of recent times, subsequently disclosed that its insurance amounted to just 6 per cent of the cost of ransomware[17].

There may be times when victims feel they have no choice but to hand over their money, because the cost of the resulting downtime is too high to bear, or they have no other way of recovering their data – a point the FBI acknowledged[18].

However, it is worth stating again: we strongly advise not to pay the ransom.

How can I prevent it?

Fortunately, there are some basic preventative steps you can take to protect yourself from a ransomware infection. The key thing to remember is that ransomware is a risk to your data rather than your devices. So, a good place to start is to understand what is the most important, critical, or sensitive data your organisation has and where that data is stored. This way, it's easier to prioritise what information gets the highest level of protection.

At a high level, these six steps can help to guide your ransomware planning.

1. Always keep a backup copy of your most important files. Ideally, this backup should be stored securely offline and offsite.

2. Formulate a business continuity plan that tests for disruption to normal operations such as from a ransomware attack.

3. Use reliable and up-to-date anti-malware software on all devices and keep software patched and updated.

4. Provide effective and regular security awareness training to all staff on how to identify suspicious emails and how to report same to your security team.

5. Ensure all remote access systems are properly secured and patched against the latest vulnerabilities.

6. Segment your network to prevent and control the spread of ransomware, or other malware, throughout your environment.

[15] https://www.bankinfosecurity.com/blogs/toll-group-data-leaked-following-second-ransomware-incident-p-2902
[16] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
[17] https://threatpost.com/insurance-pays-norsk-hydro-cyberattack-damages/149707/
[18] https://www.ic3.gov/media/2019/191002.aspx

In the following section, we present detailed recommendations to prevent a ransomware infection. You should assess each of these recommendations for their applicability to your specific environment. You should also conduct a thorough risk assessment to determine if the recommendations outlined here are suitable for your environment and are proportionate to the identified threat and risk.

For ease of use, we have divided the recommendations into three categories and colour-coded them accordingly. These categories are:

RED: Will have a **HIGH** impact in preventing ransomware

AMBER: Will have a **MEDIUM** impact in preventing ransomware

YELLOW: Will have **LOW** impact in preventing ransomware

High-impact actions

Implement geo-blocking for suspicious domains and regions

Criminals often host their infrastructure on domains in regions or countries that staff in your organisation would not regularly need to access. If there is no business need for staff in your organisation to access systems in these areas, you should consider configuring your firewalls to block all incoming and outgoing traffic to these domains and geographical areas.

Block outgoing I2P traffic

Ransomware often employs the Invisible Internet Project (I2P)[19] which is an overlay network and darknet that allows applications to send messages to each other pseudonymously and securely. You should consider blocking all outgoing I2P and other unnecessary peer-to-peer network traffic at the firewalls on the perimeter of your network. This will prevent infected computers communicating with their masters and receiving further instructions.

Review backup process

One of the most effective ways to recover from a ransomware infection is to have a comprehensive and up-to-date backup in place. You should regularly review your backup processes to:

- Ensure all relevant data is backed up as often as possible
- Ensure the backups are completed successfully
- Ensure the backup media is protected from being overwritten by ransomware
- Implement the **3-2-1** backup rule: have at least **three** copies of the most valuable data, keep **two** of them on different external media, and store **one** copy offsite.

[19] https://geti2p.net/

Secure Remote Access Gateways

One of the most common avenues for criminals to compromise a network with ransomware is to exploit weaknesses in the target company's remote access gateways. Criminals exploit unpatched vulnerabilities, weak passwords, or insecure configurations of these gateways to gain access to the network.

You should regularly review the security of your remote access gateways by:

- Ensuring remote access gateways are updated with the latest software releases and patches
- Implement Multi-Factor Authentication for all remote users, in particular those who have administrator access.
- Regularly review the configurations of the remote access gateways to ensure they are in line with the manufacturer's' security guidelines
- Run vulnerability scans against the remote access gateways
- Limit remote access by administrators to predefined known IP addresses
- Block remote access from geographical regions that none of your users will need to access from.
- Implement controls to allow remote access from only predefined and authorised devices.

Conduct regular testing of restore process from backups

While backing up data is critical, equally as important is the ability to restore the data successfully when needed. You should conduct regular tests to restore data from backups to:

- Ensure the restore process works as expected
- Ensure that data has been properly backed up
- Ensure the data has not been modified or altered by ransomware
- Ensure the timely recovery of critical data.

Enhance email security with DMARC, SPF and DKIM

By analysing publicly available information relating to an organisation's email configuration, it is possible to see if Domain-based Message Authentication, Reporting & Conformance (DMARC)[20] is implemented. We recommend you implement DMARC for your email systems, as it can help to reduce the amount of fraudulent email which may contain ransomware. Implementing it also protects from other security risks such as phishing, spoofing and CEO fraud.

We also recommend you regularly review the email configuration of your email servers to ensure that it has properly configured Sender Policy Framework (SPF)[21] , and DomainKeys Identified Mail (DKIM)[22].

[20] https://dmarc.org/
[21] http://www.openspf.org/
[22] http://www.dkim.org/

Review your incident response process

You should develop a comprehensive incident response process to include how to deal with ransomware infections. This process should include how incidents are prioritised, recorded, managed, remediated, recovered, and escalated where necessary. This process should also include:

- Understanding what conditions call for the issue to be reported to your local law enforcement agency
- Referring to the Europol website[23] to determine how you can report issues in your jurisdiction
- Understanding whether you will need to report an issue to relevant regulators.
- Developing a range of standard operating procedures to manage security incidents. (See incident response resources available from the European Union Agency for Network and Information Security (ENISA)[24] among others
- The NoMoreRansom.org website[25] may have decryption keys available. It is a joint initiative by law enforcement and the cybersecurity industry, with useful software tools and free decryption keys for more than 140 strains of ransomware, so anyone who has been infected can see if it's possible to recover their files without having to pay the ransom. However, with new strains of ransomware emerging all the time, this resource might not have the keys you need when you need them.
- Determine and agree your organisation's policy on whether or not you pay the ransom. While we do not condone this course of action we understand that many businesses may consider it. It is important to have this discussion and the relevant supports in place regarding this option

Implement a robust cybersecurity awareness training programme

Technical controls may not detect and contain all ransomware, or indeed all malware, especially given the rapidly evolving nature of these threats. In this event, the last line of defence is the end user who receives the email or browses the web. Therefore, it is essential that all users are properly empowered to identify security threats and deal with them accordingly.

Review your current security awareness training programme to ensure that it is appropriately resourced and that it targets all users. Although technical controls can minimise the risk of various threats, you must constantly manage the human factor. If people are not aware of the threats posed to their systems or data, or the reasons why certain policies and controls are in place, or how to react to a suspect security breach, then the risk of a security breach occurring increases significantly.

Tailor your security awareness programme for the audience. For example, developers should have a different programme and focus on topic relevant to their role compared to the programme aimed at the sales and marketing function.

[23] https://www.europol.europa.eu/report-a-crime/report-cybercrime-online
[24] https://www.enisa.europa.eu/
[25] https://www.nomoreransom.org/

Ensure appropriate security training for technical staff

Develop a technical training programme to ensure that technical staff have the relevant training to enable them to confidently manage the various security platforms installed in your environment.

Ensure anti-malware software is updated and all features enabled

Ensure that all PCs, laptops – and mobile devices if necessary – have up to date anti-malware software installed and that they are regularly updated with the latest software updates, virus signatures, and security features. You should also ensure that the security software on all devices have all the anti-malware features implemented, so you can quickly identify any unusual behaviour that may indicate an infection.

Apply all operating system and software patches

Ensure that all computing devices have the latest operating system and software updates deployed and applied in a timely manner. You should investigate and implement a means to keep all PCs and laptops patched with the latest updates for all software applications installed on those devices.

Disable ActiveX in Office files

You should disable ActiveX content in the Microsoft Office suite of applications. Many malicious software variants use macros to take advantage of ActiveX and download malware onto the affected device. This step is particularly recommended to any organisation running devices with any Microsoft operating system earlier than Windows 10.

Block executable files from the %APPData% and %TEMP% paths

You should look at methods to block executable files from the %APPDATA% and %TEMP% paths on computers running the Microsoft Windows operating system. Malicious software often uses these folders to download and execute the files associated with ransomware and other malicious software.

Your PC should be configured to not allow executable files to be run from the following folders

Appdata; LocalAppData; Temp; ProgramData; Desktop.

We strongly recommend you test all policies before deploying them into a live environment.

[26] https://support.microsoft.com/en-gb/office/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?redirectSourcePath=%252fen-ie%252farticle%252fEnable-or-disable-macros-in-Office-documents-7b4fdd2e-174f-47e2-9611-9efe4f860b12&ui=en-US&rs=en-GB&ad=GB

Deploy Windows AppLocker

On devices with older versions of Microsoft Windows (including Windows 7 and Windows Server 2008 R2), consider deploying AppLocker to manage which applications can be run. AppLocker is a more advanced way than software restriction policies for managing the applications users can access. It has several features that allow it to be centrally managed, for it to be tested more rigorously before deployment, and create exceptions to the rules.

Disable macros in Microsoft Office files

You should disable macros in the Microsoft Office suite of applications, as many types of malware use macros to download malware onto the affected device. This page[26] has details of how to do this.

Upgrade to latest version of Windows

You should upgrade computers running Microsoft Windows to the latest version of the operating system. At the time of writing, Windows 10 Professional is now considered to be one of the most secure desktop operating systems.

Implement network segmentation

Consider segmenting your network to reduce the ability of computer worms, whether ransomware or otherwise, to spread rapidly from one system to another. This will give you the ability to cut off infected sections of the network and prevent the infection spreading further.

Run regular phishing tests

You should run regular phishing simulations against staff to determine how many would potentially fall victim to such an attack. A phishing simulation is a tool to send fake emails to staff with an attachment or link to determine how many staff would click on the attachment or link. Since most ransomware attacks are the result of phishing emails, this type of testing, combined with an effective cybersecurity awareness programme, can be quite effective in conditioning staff not to trust all emails and to be cautious when dealing with emails.

Aim to have the click-through rate of staff responding to the phishing simulations to be consistently below 15 per cent, which is considered the industry norm.

Staff who consistently fail the phishing simulations should receive additional security awareness training and/or have additional technical controls and restrictions placed on their systems.

Medium-impact actions

Improve visibility of security events

You should consider deploying a Security Information and Event Management (SIEM) solution to provide visibility into ongoing threats within your network. This SIEM solution could either be deployed internally, or if you do not have the resources available in-house, you can outsource this to a managed security service provider that specialises in this area.

Establish baseline network behaviour

You should ensure that you have full visibility of how your network traffic behaves under normal business conditions. You can then use this knowledge as a baseline to identify any unusual activity which should then be investigated to determine whether it is the result of a potential breach or an issue with the network.

Implement an IDS/IPS

A properly configured intrusion detection system/intrusion prevention system (IDS/IPS) can be very effective at detecting and managing threats on a network. You should initiate a project to ensure the IDS/IPS is fully and properly deployed and that it is regularly reviewed. Intrusion detection/prevention models can be:

Signature-based:
This is where patterns, or signatures, of known attacks are downloaded by the system. It compares network traffic against these patterns to identify potential attacks. A disadvantage for signature-based detection is that it cannot detect new attacks because it only compares attacks against signatures that already exist.

Anomaly-based:
Intrusion software first needs to learn the “normal” behaviour of your network and the types of traffic and network packets it usually handles. Then, it can be put into action when it detects traffic that is out of the normal state.

Rule-based:
Rule-based systems employ a set of rules or protocols defined as acceptable behaviour. The IDS analyses the behaviour of network traffic or application traffic and if it is deemed as normal, it is allowed. If the traffic is outside the norm, then it is blocked.

Enable user access control (UAC) on Windows

User access control is a security feature built into Windows Vista, 7, 8 and 10 which helps prevent unauthorised changes to a computer. Having UAC enabled makes sure changes are made only with approval from the person using the computer or by an administrator – not by applications or viruses.

Enable the operating system to show file extensions

Attackers can trick users into running a file infected with a computer virus by appending a hidden extension to a filename. For example, a user receives a file called “Not Ransomware.jpg” but the file has a hidden extension of .EXE, thus making the actual filename “Not Ransomeware.jpg.exe”. The user, thinking the file is a picture, opens the file, but because the file is an executable (.exe) file the ransomware hidden in the file is launched. You should change the operating system to show Hidden File Extensions.

Disable AutoPlay

Windows’ AutoPlay feature begins reading from media as soon as it is inserted into a device. You should disable it when plugging in external media to reduce the chances of an attack infecting your device from that source. You can also disable AutoPlay via Group Policy.

Implement user behavioural analytic (UBA) systems

In line with the network baselining recommendation, you should implement a user behavioural analytic (UBA) system to identify any unusual or suspicious user activity on the network. It’s possible to identify many ransomware infections quickly by the high rate of file system access to network shares as the ransomware encrypts the targeted files. UAB technologies could detect such activity and enable you to proactively react to a ransomware infection.

Implement ad blocking software at the network perimeter

Compromised adverts on websites may infect a computer with ransomware simply by visiting a site that is displaying the malicious advert. To reduce the attack surface from this vector, consider implementing blocking software on your network's firewall to prevent infections via this route.

Implement threat intelligence

Subscribe to reliable threat intelligence services which provide indicators of compromise (IoCs) and other data which you can use to identify malware threats within your network. These will regularly update you with details of malicious and suspicious URLs, domains, and IP addresses on the internet, to which you can then block access from your network.

Although several of these threat intelligence services are commercial and require a subscription, there are open source options available such as the Malware Information Sharing Project (MISP)[27]. This is a free threat sharing platform which enables organisations to share information on security incidents to help other organisations better protect themselves.

[27] https://www.misp-project.org/

Low-impact actions

Deploy honeypots

A honeypot system is a decoy set up to look like a live system; any activity on it could be a strong indicator that the network is compromised. By deploying honeypots on your network, you can proactively detect an intrusion on your network, including intrusions relating to ransomware.

Honeypots can be an effective tool if used correctly; however, we advise caution when working with them to ensure they do not adversely impact your environment or that attackers do not compromise them to attack other systems within your network, or indeed systems external to your organisation.

ENISA has a good paper[28] on how best to deploy honeypots.

Implement appropriate rights/permissions for users

You should create and maintain users' rights and permission sets within their network operating system. Users should only have the rights/permissions they need for their job role. If they change role within the organisation, then their rights/permissions should change accordingly.

Monitor DNS logs for unusual activity

The Domain Name System (DNS) servers have logs which contain records of all the domains and networks that devices on your network have accessed. Regular monitoring of the DNS server logs could identify traffic being relayed to or from unusual hosts which may not be associated with normal business activity. This unusual traffic could indicate a malware infection.

Review mobile device security

Ransomware is migrating towards mobile devices such as smartphones and tablets, and it would be prudent to review the security of mobile devices to include:

- Ensuring anti-malware software is installed, running, and regularly updated on mobile devices
- Software and operating system patches are applied in a timely manner
- Sensitive data is backed up from mobile devices.

[28] https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection

Copyright Notice

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie