The Crypto-Ransomware prevention toolkit

intel Security

The Crypto-Ransomware prevention toolkit

Making it as hard as possible forCrypto-Ransomware to impact your trust and patients

Aim of this paper – why we wrote it?

Ransomware and specifically Crypto-Ransomware is impacting healthcare organisations around the world. This threat is not operating in the same way as previous malware threats. As is perhaps well known, the real damage done by Crypto-Ransomware is to encrypt your operational or patients' data, which can only be released through payment of a ransom or perhaps recovered through lengthy and risky restoration from backup.

Crypto-Ransomware is unfortunately really good at 'spreading' itself across the whole organisation, encrypting any shared storage it can find, and then can quickly removing access to critical data. And unless it is a known variant, there is little chance of detection and prevention through normal means. This means it is possible for services to the patient or practitioner to be seriously impeded or curtailed within minutes or hours of first infection.

This paper aims to provide a high level tool kit on what the NHS Board member should be looking for in terms of actions and mitigations their organisation should have in place to protect against Crypto-Ransomware.

Current Crypto-Ransomware trends and cost to the UK

Intel Security estimates that the annual cost of Cybercrime to the global economy is more than £470Bn. This is clearly more than the national income of some small countries and governments and most companies generally underestimate how much risk they face from cybercrime and how quickly this risk will grow. The Cyber Threat Alliance (cyberthreatalliance.org) recently stated the impact of the CryptoWall version 3 threat, which impacted hundreds of thousands of victims, resulted in over $325 million in damages worldwide.

Compounding this problem, complexity in the IT estate and infrastructure, and lack of resources available to address this issue cause a 'perfect storm' which is impacting the Health Service daily.

How to use this paper

The risk from Crypto-Ransomware can be reduced to a minimum by adopting a number of practical approaches. The checklist below is provided to allow senior Board Members to assess whether their organisation is taking the right mitigating actions to protect against this threat. It could perhaps also form an agenda to discuss with your CIO / CDIO / SIRO or general security teams. It is not a definitive list and other actions may need to be taken, but it is provided as a helpful guide.

Top ten potential mitigation actions to prevent Crypto-Ransomware infection

1. **Adherence to least privilege and deploy Identity and Access Management (IDAM) Systems.** If your organisation allows staff or users to have widespread permissions to access shared storage then your data is at risk. People should only have access privilege and access to the areas they need to do their jobs – Crypto-Ransomware will exploit this if not. Also, ensure passwords are not being reused across administration accounts, and make it harder for Crypto-Ransomware to exploit this by enhancing your access management through the implementation of IDAM systems (biometrics for example).
2. **Backup.** Your teams should be backing up systems daily to an off-site location and or offline media. This should be done using non-SMB based (a technical term for non-Windows File sharing) backups to prevent the potential spread of Crypto-Ransomware to your backup. Also, have your security team recently tested their ability to restore your systems (remote, mobile and static) if you are hit by Crypto-Ransomware? To restore fully from an infection can take days or weeks, so your teams should be investing in technology that can correct an infection automatically without the need to always restore from backup.
3. **Train your staff.** Your people should be using extreme caution when opening attachments or clicking on links. They should never open unsolicited business emails or attachments that they are not expecting, even from people they know. Well protected operations run exercises on this and evaluate the reaction and liability of staff.
4. **Deploy the best possible security technology and check it is up to date.** Is your IT infrastructure protected with the latest End Point, Network Monitoring and Code Analysis Technology? End Point protection such as Anti-Virus and Anti-SPAM is very important, but your teams should also be focused on other technologies that can detect and correct threats automatically (see later).
5. **Keep your systems up to date.** Run currently supported Operating Systems and keep them up to date. Other third party applications need to be updated as quickly as possible and Windows Updates should be applied as quickly as practical.
6. **Manage Cyber Risk at Board Level.** Implement an Information Risk Management policy and routinely assess Cyber Security risks as part of the Board Review. The potential for an infection from Crypto-Ransomware leading to a crippling of your services should be a risk managed at Board Level, and the protective measures and response plans reviewed monthly to ensure they are sensible and appropriate.
7. **Check your service provider.** Are your Cloud, mobile, data or other service providers taking adequate measures to protect you from threats? Do your security teams validate any claims made to protect you and are you ensuring compliance to the correct security standards?
8. **Incident Response.** Do your teams have an incident response plan and are you resourced to react quickly and effectively? Has the response plan been tested independently and do you have access to technical support and specialist expertise if needed?
9. **Establish a Security Operations Centre (SOC).** The impact from threats and the time taken to detect it and correct it can be reduced by deploying technologies such as SIEM. By using the latest versions the response can be automated and the time taken to react reduced to minutes. If your teams are still operating manually or do not have a SOC capability then you are vulnerable. You may be able to share operation of this facility with another Trust or agency.
10. **Keep up to date with threats.** Most threats are categorised quickly by security vendors and updates are applied automatically. Your teams should be ensuring their end point devices are fully updated, but also that devices such as web gateways and the SIEM are updated in real time. Your teams should also ensure resources such as CISP (cert.gov.uk/cisp) and threat reports from security vendors in the Cyber Threat Alliance (cyberthreatalliance.org) are consumed and analysed routinely. It may also be the case that through Law Enforcement Action the decryption keys may be available free of charge.

The crypto ransomware prevention toolkit

How we can help

For existing endpoint customers or new customers we can offer the following immediate help and solutions:

1. **Solutions:** Intel Security have prepared solutions that are immediately available to help protect you from Crypto-Ransomware and other cyber threats. This is an integrated and automated solution which will reduce the time taken to react and recover from an infection to minutes, rather than potentially days or even weeks, and reduce the manpower and skills overhead to the Health Service. The Intel Security portfolio for neutralising emerging threats is extremely comprehensive and advanced. More detail is provided on specific solutions to the Crypto-Ransomware threat below:

- **Threat Intelligence Exchange (TIE):** Along with our Data Exchange Layer (DXL) once Crypto-Ransomware is detected this will immediately inoculate endpoints (users) that may be targets. See: mcafee.com/uk/products/threat-intelligence-exchange.aspx
- **Advance Threat Defense (ATD):** This solution increases the potential for detecting new variants of Crypto-Ransomware even if they have not been seen before: mcafee.com/uk/products/advanced-threat-defense.aspx
- **Network Security Platform (NSP):** This solution has signatures in its default policies to detect Crypto-Ransomware. See: mcafee.com/us/products/network-security-platform.aspx
- **Web Gateway:** This is used to stop the spam and phishing that Crypto-Ransomware exploits. The on-board Gateway Anti-malware (GAM) inspection, aims to stop ransomware before it gets to the endpoints (users). See: mcafee.com/uk/products/web-gateway.aspx

Neutralizing Emerging Threats

Intel Security Solution Portfolio At-A-Glance

Security Ops	Data Analytics and Historical Forensics	Enterprise Security Manager, Log Manager, Advanced Correlation Engine	Visibility over the entire attack chain, historical forensic log services; event correlation and exploratory analytics
	Endpoint Forensics	Active Response	Endpoint Threat Detection and Response
	Malware Analytics	Advanced Threat Defense	Standalone or Integrated malware sandbox
	Technical Intelligence	Threat Intelligence Exchange, Global Threat Intelligence	Real time intelligence management and feeds for event correlation
	Orchestration	Data Exchange Layer (DXL)	Standardized messaging platform that unites Intel Security platforms, services and partners
Countermeasures	Endpoint Advanced Malware	Threat Intelligence Exchange module, Host IPS and Active Response	Endpoint and Server Malware and Exploit Threat Prevention, Detection and Response
	Application Sandbox and Control	Application Control and Advanced Threat Defense	Application Whitelisting, Change Control and Application Sandboxing
	Web Security	Web Gateway and Web SaaS	Network Malware and Exploit Threat Prevention, Detection and Response
	Partner Countermeasures	Avecto, TrapX, CloudHash, Autonomic	Partner technologies for patching, to control privileges and monitor malware from unmanaged systems

2. **Engage with our Professional Services team:** For existing customers: our Incident Response team can come in and diagnose, contain the breach and our education team can train staff on skills to tighten up security. Our Solution Services team can determine why existing products did not detect, assess current environment, design a new solution and or offer recommendations on future solutions. Our Managed Services team can also augment existing staff, if needed.
See: foundstone.com
3. **Proof of concepts and demonstrations:** Our technical solutions can be demonstrated either in our Corporate Briefing Centre or remotely via video conference. We are also happy to consider building Proof Of Concept specifically for your situation and running agreed 'use cases' to illustrate how we can reduce the time to respond and protect to minutes and free up resources for your Organisation.

Recommended Reference Sites:

1. **Solution Brief** - Defeat Ransomware: Ensure Your Data Is Not Taken Hostage: mcafee.com/uk/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf
2. **Blog** - Advice for Unfastening CryptoLocker Ransomware – Detailed article on what a customer should do after a ransomware attack: blogs.mcafee.com/business/advice-unfastening-cryptolocker-ransomware/
3. **McAfee Labs threat Reports** www.mcafee.com/us/mcafee-labs.aspx
4. **Understanding Ransomware and Strategies to Defeat it** www.mcafee.com/us/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf
5. **How to Protect Against Ransomware** www.mcafee.com/us/resources/solution-briefs/sb-how-to-protect-against-ransomware.pdf

For more information please contact: gordon.morrison@intel.com

Legal Disclaimer

This document and the information contained herein is provided only for educational purposes and for the convenience of Intel customers. The information contained herein is subject to change without notice, and is provided “AS IS” without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com