Cyber Incident Response Ransomware Playbook

“Cybersecurity incidents are a matter of “when,” not “if.” By 2026, organizations investing at least 20% of their security funds in resilience and flexible design programs will cut total recovery time in half when a large blast attack occurs.” -Gartner

“In 2023, 51% of organizations worldwide did not have a ransomware incident response plan.”- 2023 Thales Data Threat Report

Ransomware payments surpassed US$ 1 billion in 2023 — an all-time record high.Cost of data breach, IBM 2023

24% of cybersecurity incidents involved ransomware.- Cost of data breach, IBM 2023

Groot279

Standards
1. NIST Special Publication 800-61
2. NIST Cybersecurity Framework (CSF)

Compliance:
1. ISO 27001 – A.16
2. PCI DSS 4.0 12.10

Regulation:
1.EU GDPR – Article 32 33, 34
2. CA CCPA - Standard of Reasonable Cybersecurity - Incident Response Plan

Document Control - - -> ISO 9001 7.5

Title	Ransomware Playbook
Version	3.1
Date Issued	30/12/2023
Status	Final
Document Owner	Thor
Creator Name	Iron Man
Creator Organization Name	Avengers
Subject Category	Infinity Stone
Access Constraints	I am Groot

Document Revision History

Version	Date	Author	Summary of Changes
3.1	30/12/2023	Groot279	Implement approval steps for sensitive actions, like backup restoration, to avoid missteps.

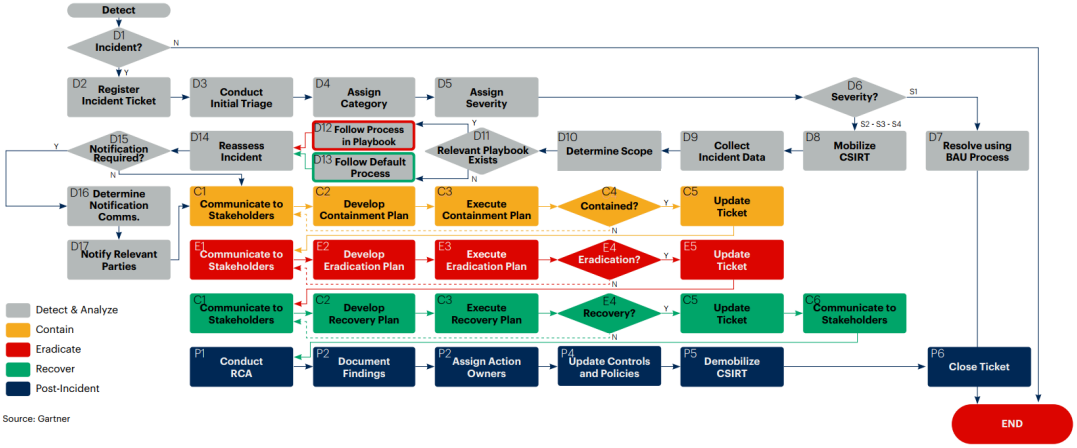
Groot279

Contents

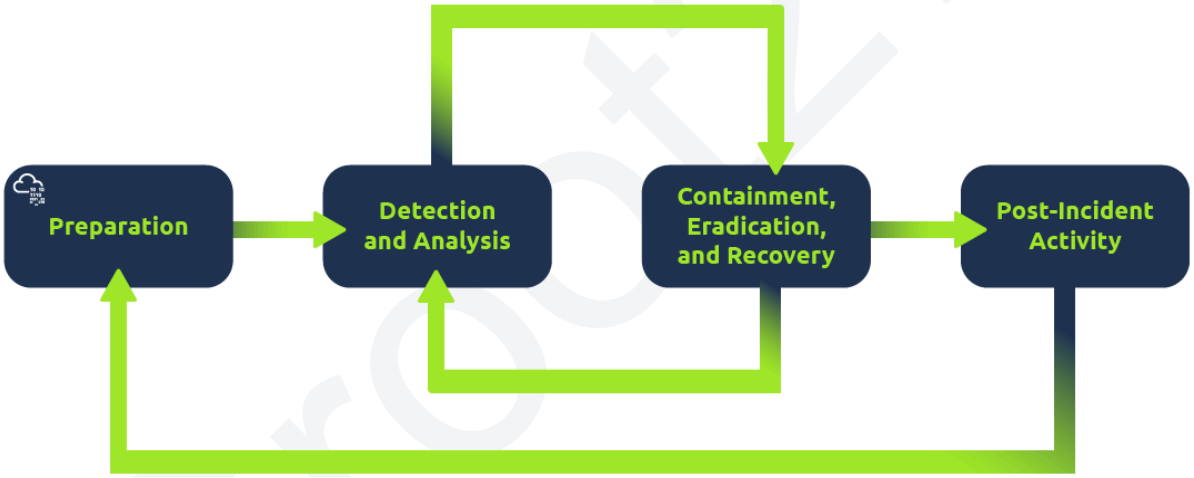
Groot279

Develop a Response Process Map

The incident response plan should dictate detailed, sequential procedures to follow in the event of an incident. The incident coordinator (or similar role) should ensure that each step of the process is completed and that progress is tracked and communicated on a rolling basis.



Source: Gartner



1. Introduction

1.1 Overview

In the event of a cyber incident, it is important that the organisation is able to respond, mobilise and execute an appropriate level of response to limit the impact on the brand, value, service delivery and the public, client and customer confidence. Although all cyber incidents are different in their nature and technologies used, it is possible to group common cyber incident types and methodologies together. This is in order to provide an appropriate and timely response depending on the cyber incident type. Incident specific playbooks provide incident managers and stakeholders with a consistent approach to follow when remediating a cyber incident.

References are made to both a Core IT CIRT and a CIRT within this document. This is in recognition of the different size and capabilities of organisations. Some may initially manage an incident with a small response team within IT services but where there is a confirmed compromise this may be escalated to an extended level CIRT comprising of members of the organisation outside the IT services who will deal with agreed categories of compromise. The Playbook as with the Cyber Incident Response Plan (CIRP) will require to be adjusted to reflect the organisational make up.

Playbooks describe the activities of those directly involved in managing specific cyber incidents. However, it is important to acknowledge the speed at which cyber incidents can escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Early consideration should be given to engaging Business Continuity, Resilience Leads in order that the wider issues can be effectively managed. Business Continuity and Resilience leads within the organisation must therefore be familiar with the CIRP and Playbooks and how they link to wider Incident response and Exercising Playbooks and arrangements

1.2 Purpose

The purpose of the Cyber Incident Response: Ransomware Playbook is to define activities that should be considered when detecting, analysing and remediating a Ransomware incident. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3 Ransomware Definition

Ransomware is a type of malicious software in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack.

1.4 Scope

This document has been designed for the use of the first responders such as the Service Desk team when responding to a Cyber incident. It is not standalone and must be used alongside the CIRP.

1.5 Review Cycle

This document is to be reviewed for continued relevancy by the Cyber Incident Response Team (CIRT) lead at least once every 12 months; following any major cyber incidents, a change of vendor, or the acquisition of new security services.

Groot279

2. Preparation Phase

Preparation Phase		
Phase objectives	The preparation phase has the following objectives: ● Prepare to respond to cyber incident in a timely and effective manner; ● Inform employees of their role in remediating a Ransomware incident including reporting mechanisms.	
Activity	**Description**	**Stakeholders**
Prepare to respond	Activities may include, but are not limited to:	
	Review and rehearse cyber incident response procedures including:- ● technical and business roles and responsibilities ● escalation to major incident management, where necessary	● Head of Information Governance ● Head of IT ● Information Security Manager ● Team Leader ● Service Delivery Manager ● Service Desk Analysts/Technicians ● Legal Team ● Communications Team ● Resilience Lead ● Business Continuity Lead
	Review recent cyber incidents and the outputs.	● Information Security Manager
	Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities.	● Information Security Manager
	Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: ● CIRP;	● Information Security Manager
	Identify and obtain the services of a 3rd party Cyber Forensic provider.	● Information Security Manager

	Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.	• Information Security Manager
Activity	**Description**	**Stakeholders**
Inform employees	Activities may include, but are not limited to:	
	Conduct regular awareness campaigns to highlight information security risks faced by employees, including: • Phishing attacks and malicious emails; • Ransomware; • Reporting a suspected cyber incident.	• Head of IT • Information Security Manager • Resilience Lead • Business Continuity Lead
	Ensure regular security training is mandated for those employees managing personal, confidential or high risk data and systems.	• Head of IT • Information Security Manager • HR • L&D Department • Resilience Lead • Business Continuity Lead

Groo270

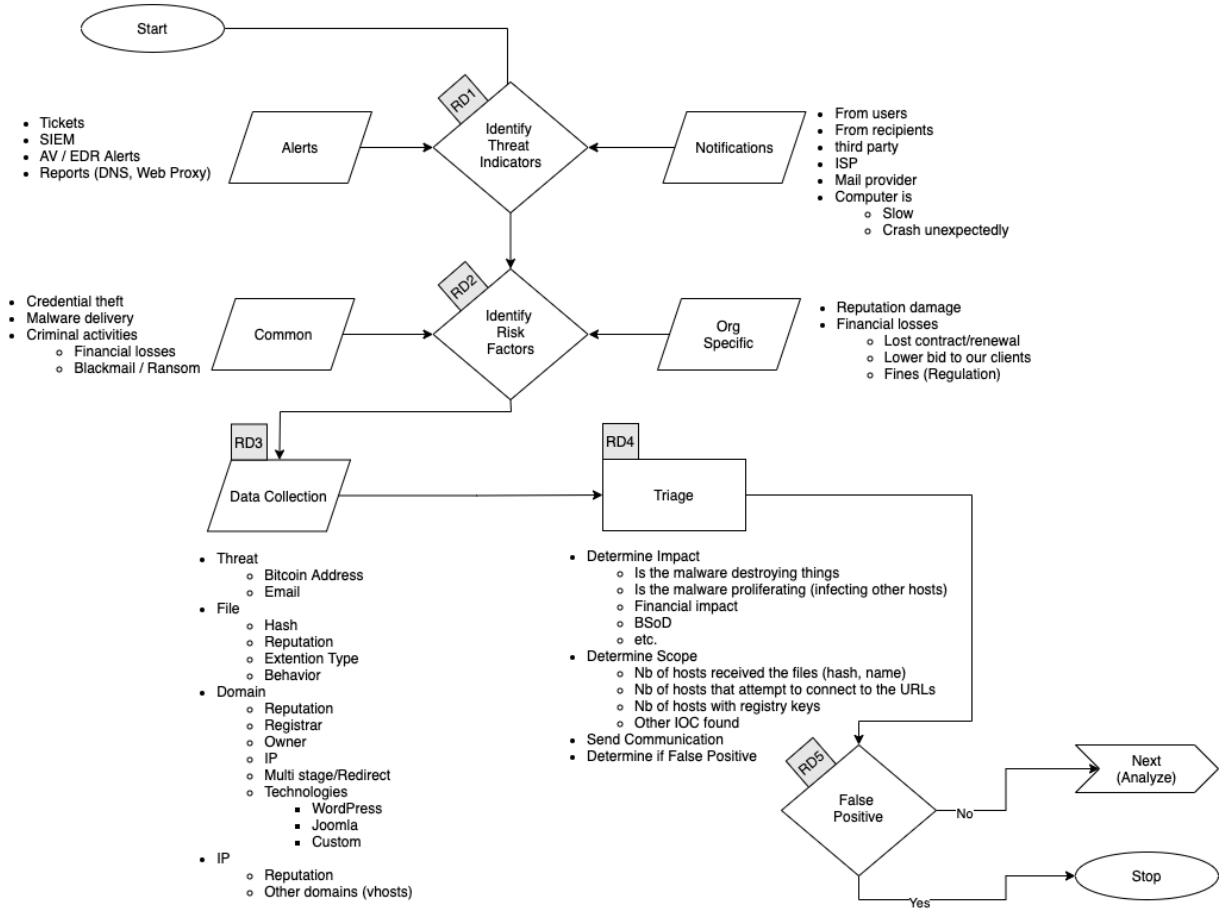
3. Detect

Detection Phase		
Phase objectives	The detection phase has the following objectives: ● Detect and report a breach or compromise of the confidentiality, integrity or availability of organisational data; ● Complete initial investigation of the Ransomware; ● Report the Ransomware attack or compromise data formally to the correct team as a cyber incident.	
Activity	**Description**	**Stakeholders**
Detect and report the incident	Activities may include, but are not limited to:	
	Monitor detection channels, both automatic and manual, customer and staff channels and social media for indications of a data breach or compromise, these can include but are not limited to: ● Automated AV alerts ● Detection from email filters ● Unusual activity on end-point devices, servers or phones ● Reports from end-users	● Information Security Manager ● Core IT CIRT
	Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information. To report an incident, follow the process defined in the CIRP.	● Information Security Manager ● Core IT CIRT
	Consider whether data loss or data breach has occurred and if so refer to data breach playbook.	● Information Security Manager ● Information Governance Team
	Classify the cyber incident, based upon available information related to the data loss and the incident types (see CIRP).	● Information Security Manager ● Core IT CIRT
	Report the cyber incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the CiSP	● Information Security Manager ● Core IT CIRT ● CIRT

	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Initial investigation of the incident	Activities may include, but are not limited to:	
	Mobilise the CIRT to begin initial investigation of the cyber incident (see staff contact details within CIRP).	• Information Security Manager • Core IT CIRT • The following may also be included in the incident response team where appropriate for the incident: • Service Desk Analysts • Server Desk Technicians • Server Team • Mobile Device Team
	Identify likelihood of widespread Ransomware infection.	• Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Collate initial incident data including as a minimum for following; • Type of cyber incident; • How was the cyber incident reported; • Where are Ransomware messages appearing; • Identify the attack email; • Location of detection(s), both physical and logical; • Number of affected assets across the organisation (initial), is this increasing; • Additional reporting relating to affected assets, including AV logs, system event logs, and network monitoring logs; • Preliminary business impact; and • Any current action being undertaken.	• Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Secure artefacts, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis.	• Information Security Manager • Core IT CIRT

	Research Threat Intelligence sources and consider Cyber Security Information Sharing Partnership (CiSP) submission to gain further intelligence and support mitigation by others.	• Information Security Manager • Core IT CIRT
	Review cyber incident categorisation to validate the cyber incident type as a Ransomware attack and assess the incident priority, based upon the initial investigation. (See CIRP for Incident Severity Matrix)	• Information Security Manager • Core IT CIRT
Activity	**Description**	**Stakeholders**
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incident in accordance with the organisation's CIRP. Specifically Consider the Intelligence value to other organisations and share on the CiSP	• Information Security Manager • CIRT
	Consider whether the Incident meets the Scottish Public Sector cyber Incident Central Notification and Co-ordination Policy as contained within the CIRP.	• Information Security Manager • CIRT • CIRT • Resilience Lead • Business Continuity Lead
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Establish the requirement for a full forensic investigation	Activities may include, but are not limited to:	
	Consider conducting a full forensic investigation, on the advice of legal counsel. All evidence handling should be done in line with the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence.	• Information Security Manager • Core IT CIRT • CIRT

Ransom - Detect



4. Analyse

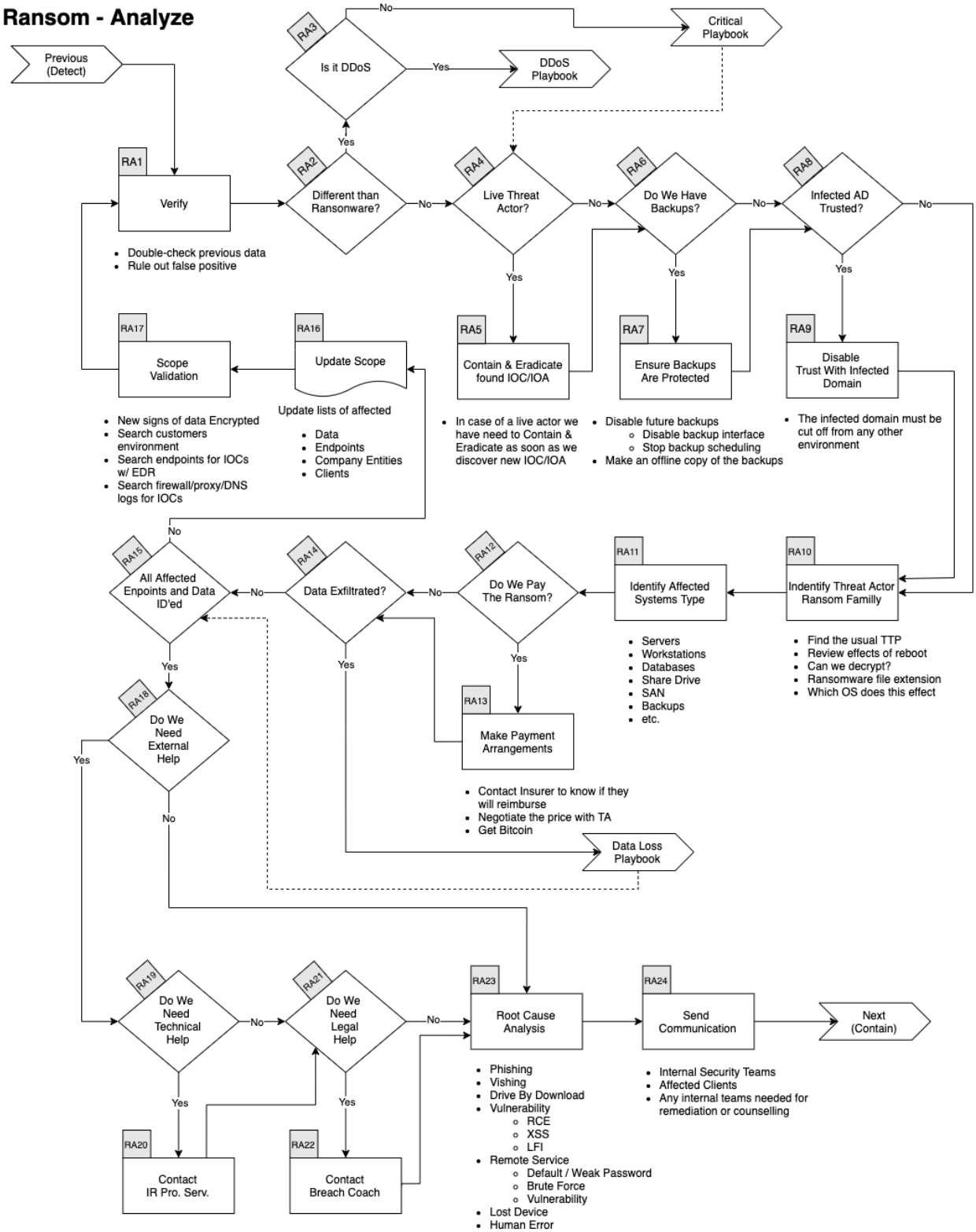
Analysis Phase		
Phase objectives	The analysis phase has the following key objectives: ● Analyse the cyber incident to uncover the scope of the attack; ● Identify and report potentially compromised data and the impact of such a compromise; ● Establish the requirement for a full forensic investigation; ● Develop a remediation plan based upon the scope and details of the cyber incident.	
Activity	**Description**	**Stakeholders**
Analyse the extent of the incident	Activities may include, but are not limited to:	
	Engage technical staff from resolver groups.	● Service Desk Technicians ● Core IT CIRT
	Classify the ransomware by submission to multiple AV vendors and determine the family it belongs to.	● Information Security Manager ● Core IT CIRT
	Scope the attack. ● Where are ransom messages appearing? ● Are there any infected network drives? Which? ● Identify the attack email or ingress point and the extent of travel.	● Information Security Manager ● Core IT CIRT
	Reverse-engineer the Ransomware in a secure environment to understand its mechanisms, and the functionality it implements.	● Information Security Manager ● Core IT CIRT ● External Security Partner ● NCSC ● Police Scotland
	Execute the Ransomware in a secure environment or sandbox, segregated from the business network, to determine its behaviour on a test system, including created files, launched services, modified registry keys and network communications.	● Information Security Manager ● Core IT CIRT ● External Security Partner ● NCSC ● Police Scotland
	Review affected infrastructure for indicators of compromise derived from the malware analysis to identify any additional compromised system(s).	● Information Security Manager ● Core IT CIRT

Groot25

	Preserve all evidence to support attribution or anticipated legal action.	• Information Security Manager • Core IT CIRT
	Examine threat intelligence feeds to determine if the ransomware attack is bespoke and targeted at specific accounts, infrastructure or systems.	• Information Security Manager • Core IT CIRT
	Verify all infected assets are in the process of being recalled and quarantined.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Identify and report potentially compromised data	Activities may include, but are not limited to:	
	Identify any data impacted by the ransomware attack, including data-in-transit.	• Information Security Manager • Core IT CIRT • CIRT
	Engage data owners and the business to understand the business impact of the compromised data.	• Information Security Manager • CIRT • Head of IT
	Report the Cyber incident to the organisation's senior stakeholders, as required.	• Information Security Manager • CIRT
	Establish the likelihood that identified data's confidentiality, integrity or availability was compromised.	• Information Security Manager • Core IT CIRT • CIRT
	Consider whether reporting suspected or confirmed unauthorised access to any personal data to the Information Commissioner's Office (ICO) is appropriate at this stage. Consider reporting to incident to Police Scotland Consider reporting requirements to relevant regulator or Competent Authority if applicable	• Information Security Manager • CIRT • Data Protection Officer • Legal Services
	Update the senior stakeholders of any suspected or confirmed data breach including the unauthorised access to personal or sensitive organisational data.	• Information Security Manager • CIRT • Data Protection Officer
	CIRT to immediately report any suspected or confirmed data breach including any personal/ data breach to the appropriate parties (refer to data loss/breach playbook).	• Information Security Manager • CIRT • Data Protection Officer

		• Legal Services`
	Consider Intelligence Sharing value on CiSP	• Information Security Manager • Resilience Lead
Activity	**Description**	**Stakeholders**
Develop a remediation plan	Activities may include, but are not limited to:	
	Incorporate technical and business analysis to develop a prioritised remediation plan.	• Information Security Manager • Core IT CIRT • CIRT
	Implement a communications strategy in line with the remediation plan.	• Head of IT • Information Security Manager • CIRT • Communications Team • Resilience Lead • Business Continuity Lead

Groot27


Ransom - Analyze
Previous (Detect)
RA3
Is it DDoS
No
Yes
Critical Playbook
DDoS Playbook
RA1
Verify
RA2
Different than Ransonware?
RA4
Live Threat Actor?
RA6
Do We Have Backups?
RA8
Infected AD Trusted?
Double-check previous data
Rule out false positive
RA17
Scope Validation
RA16
Update Scope
RA5
Contain & Eradicate found IOC/IOA
RA7
Ensure Backups Are Protected
RA9
Disable Trust With Infected Domain
New signs of data Encrypted
Search customers environment
Search endpoints for IOCs w/ EDR
Search firewall/proxy/DNS logs for IOCs
Update lists of affected
Data
Endpoints
Company Entities
Clients
In case of a live actor we have need to Contain & Eradicate as soon as we discover new IOC/IOA
Disable future backups
Disable backup interface
Stop backup scheduling
Make an offline copy of the backups
The infected domain must be cut off from any other environment
RA15
All Affected Enpoints and Data ID'ed
RA14
Data Exfiltrated?
RA12
Do We Pay The Ransom?
RA11
Identify Affected Systems Type
RA10
Indentify Threat Actor Ransom Familly
Servers
Workstations
Databases
Share Drive
SAN
Backups
etc.
Find the usual TTP
Review effects of reboot
Can we decrypt?
Ransomware file extension
Which OS does this effect
RA18
Do We Need External Help
RA13
Make Payment Arrangements
Contact Insurer to know if they will reimburse
Negotiate the price with TA
Get Bitcoin
Data Loss Playbook
RA19
Do We Need Technical Help
RA21
Do We Need Legal Help
RA23
Root Cause Analysis
RA24
Send Communication
Next (Contain)
RA20
Contact IR Pro. Serv.
RA22
Contact Breach Coach
Phishing
Vishing
Drive By Download
Vulnerability
RCE
XSS
LFI
Remote Service
Default / Weak Password
Brute Force
Vulnerability
Lost Device
Human Error
Internal Security Teams
Affected Clients
Any internal teams needed for remediation or counselling

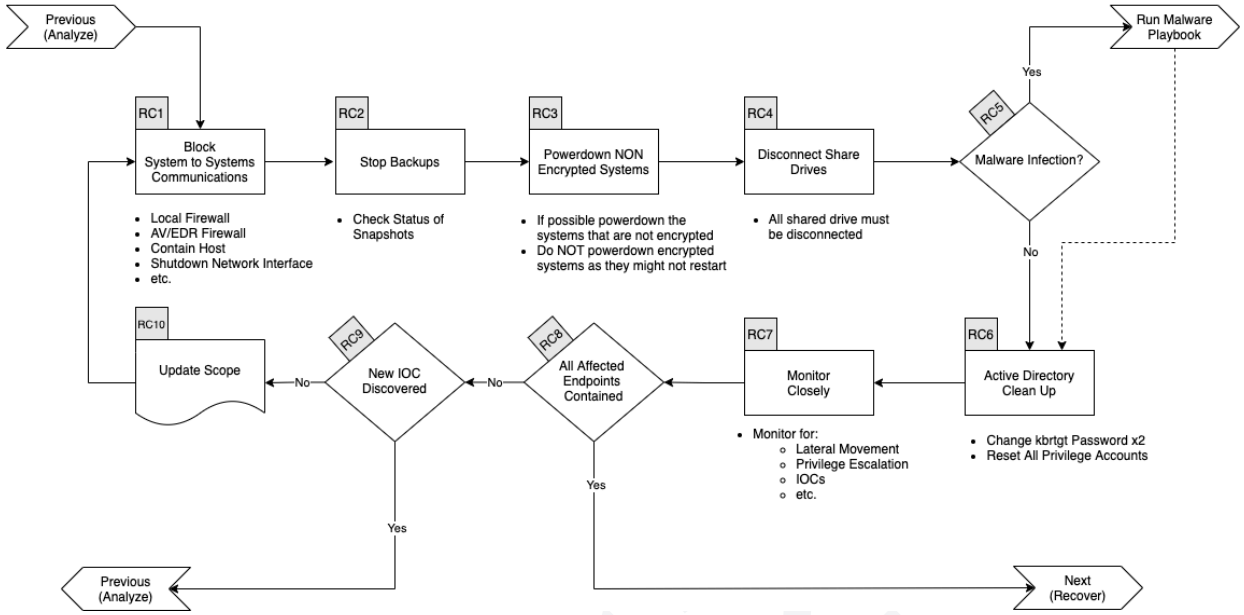
5. Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	The remediation phase has the following objectives: ● Contain the effects of the ransomware on the targeted systems; ● Eradicate the ransomware from the network through agreed mitigation measures; ● Recover affected systems and services back to a Business As Usual (BAU) state.	
Activity	**Description**	**Stakeholders**
Containment	Contain the technical mechanisms of the ransomware attack, including:	
	Reduce any further malicious activity by quarantining affected systems and removing them from the network, where possible, or applying access controls to isolate from production networks.	● Information Security Manager ● Core IT CIRT ● CIRT
	Develop protection measures derived from the results of malicious code analysis to protect infrastructure from the malicious code and other ransomware that may attempt to infect using the same mechanism.	● Information Security Manager ● CIRT
	Define scope by searching for: ● The SHA-1 process name; ● The executable file name; ● The URL or IP address of similar connections on the network.	● Information Security Manager ● Core IT CIRT
	In the case of an email attack: ● Block the sender and the message by marking it as spam; ● Block the IP address identified in the email header. In the case of a website compromise: ● Block the website at the network perimeter; ● Sinkhole the domain on internal DNS servers; ● Block the site IP address on the network firewall; ● Ensure all web browsers used within DANB have the latest patches; ● Encourage users to switch to newer browsers.	● Information Security Manager ● Core IT CIRT

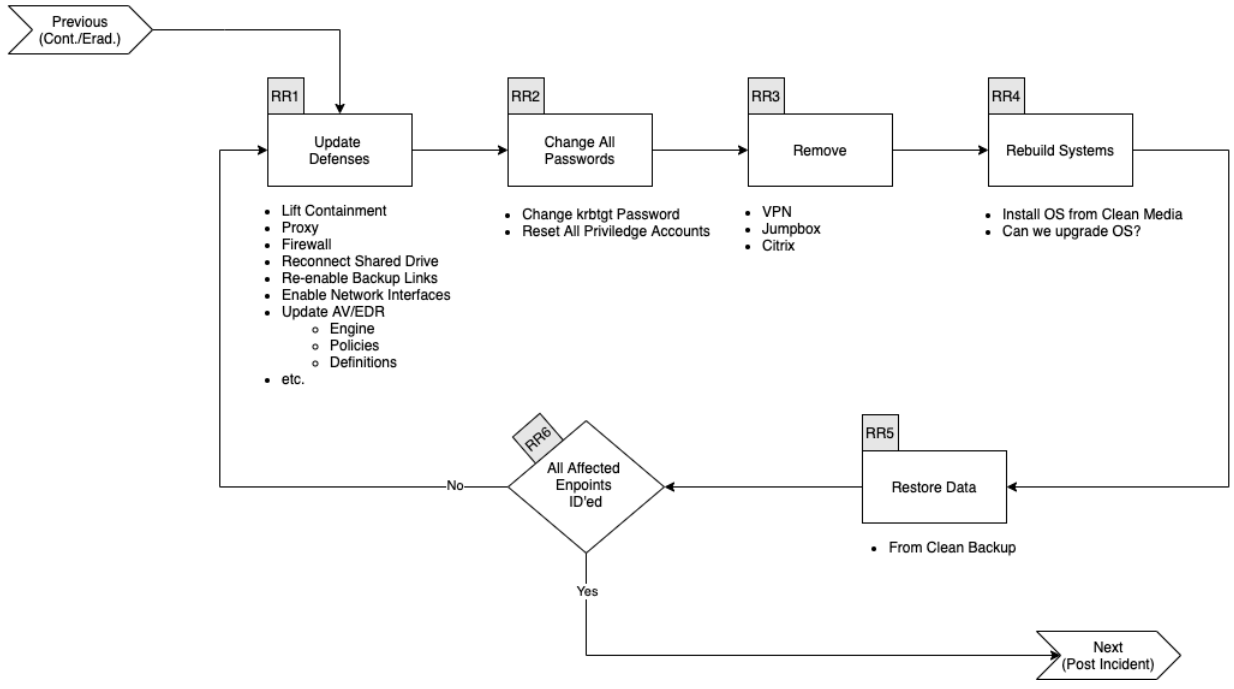
Remediation Phase		
	Block access to any identified Remote Access Tools (RATs) to prevent communication with command and control servers, websites and exploited applications.	• Information Security Manager • Core IT CIRT
	Suspend the login credentials of suspected compromised accounts.	• Information Security Manager • Core IT CIRT
	Secure copies of the malicious code, affected systems and any identified artefacts for further investigation (engaging with forensic support if forensic copies are required).	• Information Security Manager • Core IT CIRT
	Inform business data owner(s) and stakeholders of the progress of containment activities.	• Information Security Manager
	Remind users to move the attack email to the 'Junk' folder.	• Information Security Manager
Activity	**Description**	**Stakeholders**
Eradication	Activities may include, but are not limited to:	
	Identify removal methods from the results of the malicious code analysis and trusted sources (AV providers).	• Information Security Manager • Core IT CIRT
	Complete an automated or manual removal process to eradicate ransomware or compromised executables using appropriate tools.	• Information Security Manager • Core IT CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	• Information Security Manager • Core IT CIRT
	Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.	• Information Security Manager • Core IT CIRT
	Change any compromised account details.	• Information Security Manager • Core IT CIRT

Remediation Phase		
	Continue to monitor for signatures and other indicators of compromise to prevent the ransomware attack from re-emerging.	• Information Security Manager • Core IT CIRT
	Confirm policy compliance across the estate.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Recover to BAU	Activities may include, but are not limited to:	
	Recover systems based on business impact analysis and business criticality.	• Information Security Manager • Core IT CIRT • CIRT
	Complete Ransomware scanning of all systems, across the estate.	• Information Security Manager • Core IT CIRT
	Re-image systems.	• Information Security Manager • Core IT CIRT
	Re-set the credentials of all involved system(s) and users account details.	• Information Security Manager • Core IT CIRT
	Reintegrate previously compromised systems.	• Information Security Manager • Core IT CIRT
	Restore any corrupted or destroyed data.	• Information Security Manager • Core IT CIRT
	Restore any suspended services.	• Information Security Manager • Core IT CIRT
	Establish monitoring to detect further suspicious activity.	• Information Security Manager • Core IT CIRT
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	• Information Security Manager • Core IT CIRT

Ransom - Contain / Eradicate



Ransom - Recover



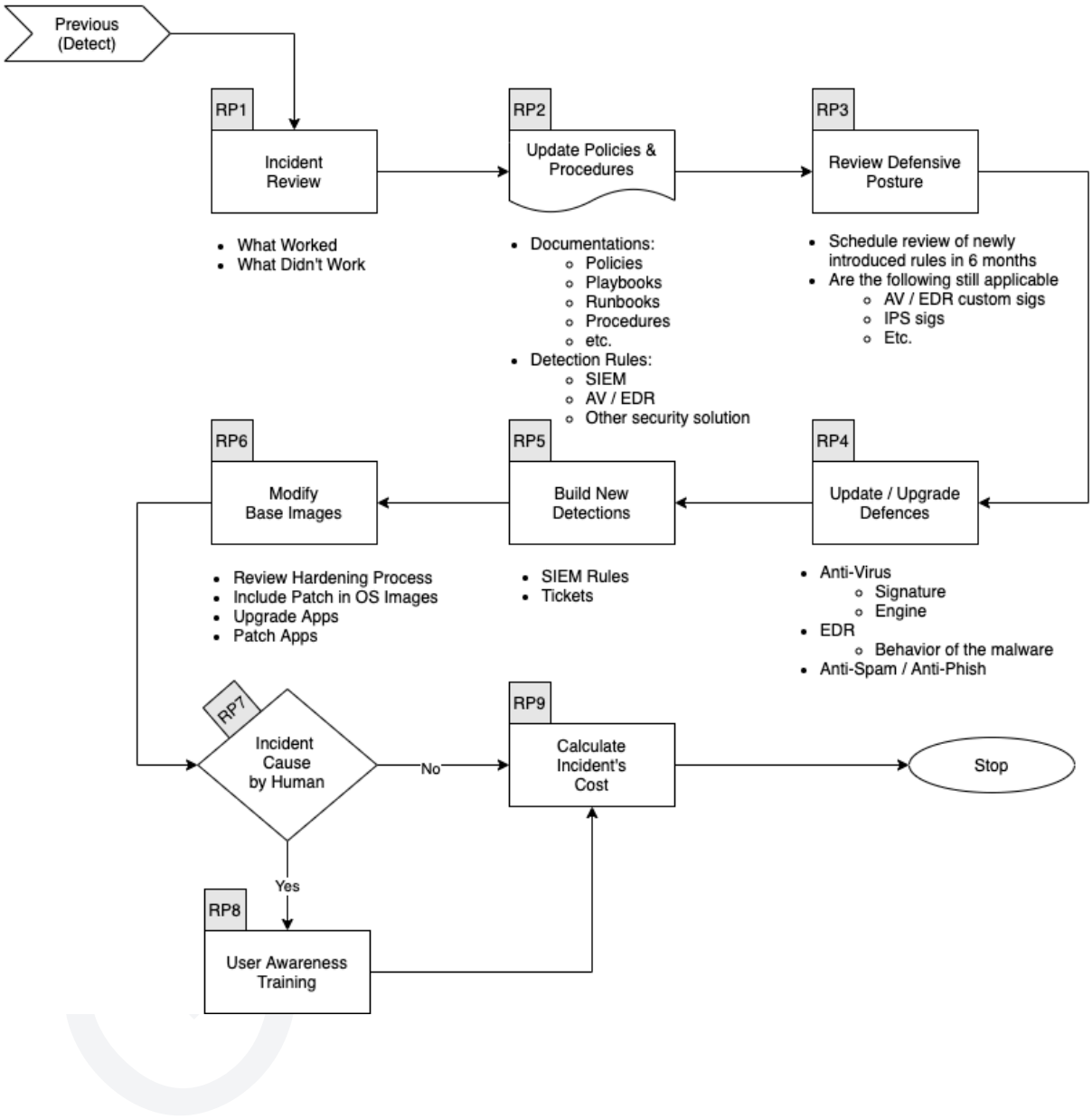
6. Post Incident

Post-Incident Activities Phase		
Phase objectives	The post-incident activities phase has the following objectives: ● Complete an incident report including all incident details and activities; ● Complete the lessons identified and problem management process; ● Publish appropriate internal and external communications.	
Activity	**Description**	**Stakeholders**
Incident reporting	Draft a post-incident report that includes the following details as a minimum: ● Details of the cause, impact and actions taken to mitigate the cyber incident, and including timings, type and location of incident as well as the effect on users; ● Activities undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to resume; ● Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar Cyber incident from reoccurring, as part of a formalised lessons identified process.	● Senior Stakeholders ● Head of Information Governance ● Head of IT ● Audit Committee ● Information Security Manager ● Resilience Lead ● Business Continuity Lead
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	● Information Security Manager ● CIRT
	Consider sharing lessons identified with the wider Scottish Public Sector.	● Information Security Manager ● CIRT ● Resilience Lead ● Business Continuity Lead
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	● Information Security Manager ● Core IT CIRT ● CIRT
Human Resources	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	● Information Security Manager ● HR
Communications	Activities may include, but are not limited to:	

Post-Incident Activities Phase		
	Publish internal communications to inform and educate employees on ransomware attacks and security awareness.	• Information Security Manager • CIRT • Communications
	Publish external communications, if appropriate, in line with the communications strategy to provide advice to customers, engage with the market, and inform press of the cyber incident. These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further ransomware attacks.	• Head of IT • Information Security Manager • Communications Team

Groot279

Ransom - Post Incident



Appendix A

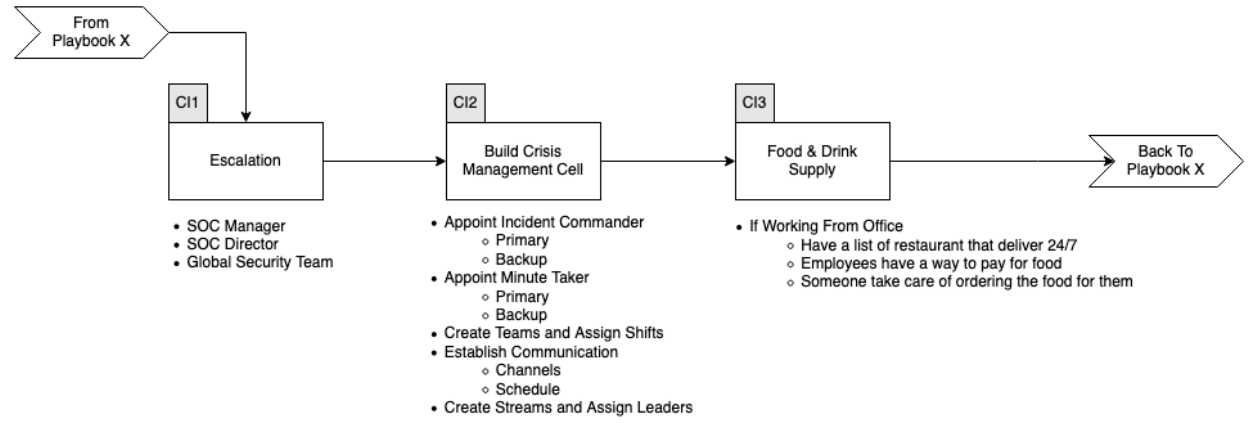
Define Escalation Paths

Effective incident response is a team sport. Maintain clear escalation paths based on the severity of the incident.

Severity	Escalation Path					
Tier	Note: Escalations are cumulative as the severity tier increases					
04 Crisis	CEO	CFO	Board	–	–	–
03 High	HR	Legal	COO	Privacy	PR	Cybersecurity Insurance
02 Medium	CISO	CIO	–	–	–	–
01 Low	Incident Handler	CSIRT	–	–	–	–

Source: Gartner

Critical Incident



Appendix D

EXAMPLES

TOP-IOC Annotation Statements

IOC NEGATIVE
TOP-IOC: Attack surface DOES NOT exist
TOP-IOC: Attack surface vulnerability DOES NOT exist
TOP-IOC: Mitigating controls DO EXIST and ARE currently protecting the asset
TOP-IOC: Subsequent attack activity DOES NOT exist
TOP-IOC: Corroboration from other assets DOES NOT exist
TOP-IOC: NOT CONSISTENT with unusual egress network traffic
TOP-IOC: NOT CONSISTENT with unusual lateral movement
TOP-IOC: NOT CONSISTENT with login anomalies
TOP-IOC: NOT CONSISTENT with suspicious domain controller activity
TOP-IOC: NOT CONSISTENT with suspicious byte counts

IOC POSITIVE
TOP-IOC: Attack surface DOES exist
TOP-IOC: Attack surface vulnerability DOES exist
TOP-IOC: Mitigating controls DO NOT EXIST or ARE NOT currently protecting the ass
TOP-IOC: Subsequent attack activity DOES exist
TOP-IOC: Corroboration from other assets DOES NOT exist
TOP-IOC: CONSISTENT with unusual egress network traffic
TOP-IOC: CONSISTENT with unusual lateral movement
TOP-IOC: CONSISTENT with login anomalies
TOP-IOC: CONSISTENT with suspicious domain controller activity
TOP-IOC: CONSISTENT with suspicious byte counts

NOTES

TOP Indicators Of Compromise (TOP-IOC)

Threat Analysis Model

1. Analysts shall use a TAM similar to the TOP-IOC
2. Analysts shall annotate cases using one or more TOP-IOC annotation statements

3. All ticket annotation shall start with IOC-NEGATIVE -or- IOC-POSITIVE
4. Evidence that intelligence assets were searched and analyzed is required
5. Annotations should indicate the COA related to the specific activities conducted

General TOP-IOC

1. Attack Surface Vulnerability Exists
2. Corroboration From Multiple Intelligence Assets
3. Unusual Egress Network Traffic
4. Unusual Ingress Network Traffic
5. Anomalies In Privileged User Account Activity
6. Geographical Irregularities
7. Log-In Anomalies
8. Volume Increase For Database Reads
9. HTTP Response Size Anomalies
10. Large Numbers Of Requests For The Same File
11. Mismatched Port-Application Traffic
12. Suspicious Registry Or System File Changes
13. DNS Request Anomalies
14. Unexpected Patching Of Systems
15. Mobile Device Profile Changes
16. Data In The Wrong Places
17. Unusual Lateral Movement
18. Velocity Increase For Share / Mount Activity
19. Time Based Anomalies
20. Suspicious Byte Counts
21. Suspicious Domain Controller Activity
22. Subsequent Activity By Attacker Address / GEO
23. HTTP Response Code Success

Insider Threat TOP-IOC

Root279

1. Logons To New Or Unusual Systems
2. New Or Unusual Logon Session Types
3. Unusual Time Of Day Activity
4. Unusual GEO
5. Unlikely Velocity
6. Shared Account Usage
7. Privileged Account Usage
8. Unusual Program Execution
9. New Program Execution
10. High Volume File Access
11. Unusual File Access Patterns
12. Cloud-based File Sharing Uploads
13. New IP Address Association
14. Bad Reputation Address Association
15. Unusual DNS Queries
16. Bandwidth Usage
17. Unusual Or Suspicious Application Usage
18. Dark Outbound Network Connections
19. Known Command And Control Connections
20. Building Entry And Exits
21. High Volume Printing Activity
22. Unusual Time Period Printing
23. Endpoint Indicators Of Compromise
24. Sensitive Table Access
25. Sensitive Data Movement Combined With Other Risk Indicators

Network and Packet Analysis Observation TOP-IOC

1. Known Signatures
2. Reputation
3. IP Addresses
4. Domains
5. DNS Queries

Gloot279

6. DLP Indicators
7. Anomalous Traffic Patterns
8. Protocols
9. Inconsistent Protocols
10. Malformed Protocols
11. Masquerading Protocols
12. Prohibited Protocols

Suspicious Domain TOP-IOC

1. Domain registered date is recent
2. Domain registrant is anonymous or non-reputable
3. Domain shares similar characteristics with prior known bad
4. Domain has a suspicious email infrastructure
5. Domain has a suspicious website infrastructure
6. Domain has a disreputable history
7. Domain has suspicious IP addresses / DNS data

Azure & Office 365 TOP-IOC

1. Privileged account logon from foreign address
2. Creation of accounts in Azure AD
3. Traffic restrictions loosened on Virtual Network
4. Storage account accessed via stolen key from foreign address
5. Subscription Administrator added
6. Windows level intrusion of VM
7. High priority target's mailbox is accessed

Tactics, Techniques & Procedures

Protecting Against Ransomware

1. Prioritize software updates for internet facing systems and systems having access to

Root279

the internet

2. Practice least privilege principles including role based access controls and access limitations

3. Implement end point detection / host based intrusion technologies

4. Maintain backups of mission critical data

5. Educate the user community

6. Create a response / MISSION plan and assign a strike force to execute that plan when it becomes necessary

Groot279