RANSOMWARE PLAYBOOK

A Special Incident Response Guide for Handling Ryuk Ransomware (Triple-Threat) Attacks

Version 1.0

Release date: October 2019

Frankie Li, Mika Devonshire and Ken Wong
ir@dragonadvancetech.com

Overview

Ransomware is a very simple, but effective malicious software that affects both home users as well as government departments, courts, hospitals, universities, large enterprises, small medium enterprises or even non-government organizations (NGOs). Since 2013, it has become a key financial campaign of choice for cybercriminal organizations. It performs malicious actions to encrypt personal files (such as images, movies, documents, or text files) on the infected systems, encrypt files on shared network drives (including connected NAS or storage devices), lock systems' access, crash systems, or even display disruptive and indecent messages containing pornographic images to embarrass users and force victims to pay a ransom through bitcoin (or other crypto-currencies) by using elaborate techniques.

The return on investment (ROI) is so high that it has been turned into a business model known as the Ransomware-as-a-Service industry. Developers recruit affiliates to spread the ransomware in return for a cut of the profits. Researchers have published several ransomware projects in the name of education and freedom of knowledge that unfortunately allow novice hackers to easily acquire and run successful ransomware campaigns.

Ransomware is difficult to defend against because it uses common tools native to the Windows operating system, such as the standard Windows crypto API, PowerShell, Windows Management Instrumentation (WMI) or even JavaScript. It also makes use of exploit kits to deploy ransomware through web browsers, Adobe Flash plug-in and even Microsoft Office documents.

Unlike common malicious software, ransomware does not try to hide. Immediately after the infection, a ransom note is usually displayed to inform the victims that their machines were infected. Sometimes, a visible running timer, a bitcoin address to send payment, and instructions on how to buy bitcoin will be displayed on the victims machine. This note asks for ransom payment (either a few hundred US dollars or more in the case of government attacks) and in turn the attacker promises a key to decrypt their data.

Traditional preventive measures can be very useful to reduce damage from this kind of attack. Procedures such as backing up all critical data frequently, installing update anti-virus software, and maintaining good user awareness do help protect organizations from ransomware attacks. Additional prevention advice or even decryption tools can be found from an online project called: NO MORE RANSOM[1].

Before 2017, the infection vectors mainly came from phishing emails or vulnerable browser plug-ins contacting compromised web servers. The WannaCry ransomware, like a network worm, was an exception in that it used ETERNALBLUE to exploit SMB services running inside the Windows kernel on unpatched Windows systems.

[1] https://www.nomoreransom.org/en/ransomware-qa.html

Since 2018, some advance cybercriminals have changed their tactics and now direct their efforts toward sophisticated, longer-term attacks against specific enterprises to seek a larger ransom. We have encountered incidents of ransomware infections on internal servers through carelessly configured remote desktop (RDP[2]) connections. Ransomware, like Ryuk, has been used in the ***final stage of tailored attacks*** after the target's systems or networks have been compromised for a period of time. The attacker then ***manually plants*** Ryuk to encrypt only crucial assets in the target environment. In a security blog published on October 9, 2019, the researcher provides the following insight into Ryuk ransomware:

> *Many of these organizations have paid hefty fees to recover their files following a Ryuk attack, only to find that any number of files have been stolen, and some of the data left behind is beyond repair. What many people don't understand about Ryuk is that it is not the beginning of the attack, it is the end of the attack.*

On October 4 2019, a Toronto media[3] firm published that the same ransomware hit three Ontario hospitals, causing a delay for patients and creating a headache for the staff. Cybercrime analysts and specialized bloggers found this kind of ransomware is difficult to defend against because Ryuk is like a comic book character who "cannot be harmed by conventional human weapons" and traditional incident handling procedures, like "reimaging" computers to reset them to their previous configurations, do not always work because the malware has the ability to come back, called "persistence" mechanisms.

On October 17, 2019, the global shipping and ecommerce giant Pitney Bowes [4]revealed that their recent service disruptions were caused by Ryuk. The incident impacted the company's critical servers, including: mailing services, customer account access, the supplies web store, software and data marketplace downloads, and some commerce services.

This Ransomware Playbook is intended to be used as a general guideline for organizations faced with ransomware attacks. If you are currently experiencing a ransomware incident, it is highly recommended you immediately review the containment section below. If your organization is infected with ransomware like Ryuk, we can provide a detailed checklist upon request (an extract is provided in the Appendix secton) to help you to handle the incident in an expedited manner – this is crucial as you will not only have to handle Ryuk[5], but also two forms of malware called Trickbot and Emotet (Fig 2 – reproduced based on the findings from Kryptoslogic[6]).

[2] https://dragonadvancetech.com/reports/SME-RDP-final-draft-31.pdf and https://dragonadvancetech.com/reports/SME-RDP-RCE-final.pdf

[3] https://www.cbc.ca/amp/1.5308180?__twitter_impression=true

[4] https://maintenance.pb.com/pbcom/outage.html

[5] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[6] https://www.kryptoslogic.com/blog/2019/01/north-korean-apt-and-recent-ryuk-ransomware-attacks/

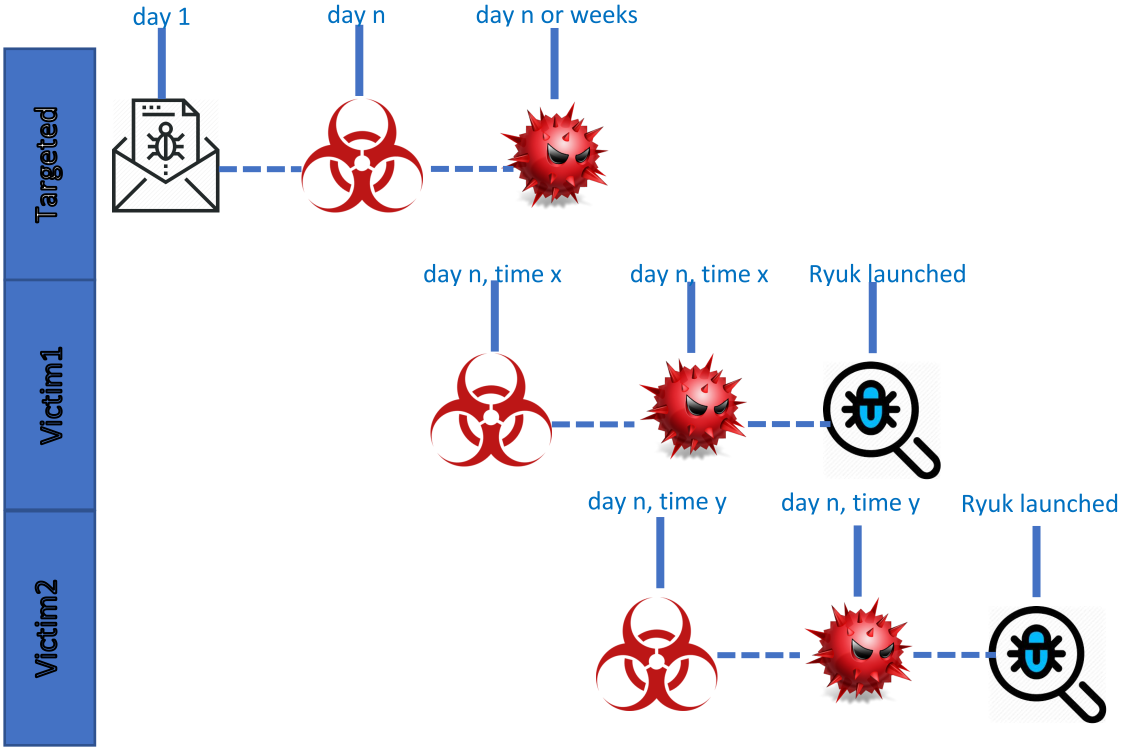


Fig. 2 – recent Emotet, Trickbot and Ryuk Ransomware (triple-threat) attacks

Incident Lifecycle

The incident response cyber is made up of many steps including intrusion detection, and intrusion response. By making reference to the model of NIST SP800-61 Computer Security Incident Handling Guide, the incident lifecycle (Fig. 1) can be classified into several phases. The initial phase involves the identification of security program's hygiene issues, this includes a comprehensive analysis of the environment focused on finding evidence of ongoing or past compromises, assessment of systemic risks and exposures, establishing and training an incident response team, and acquiring necessary tools and resources. During preparation, the organization should attempt to limit the number of incidents based on the results of their risk assessments.

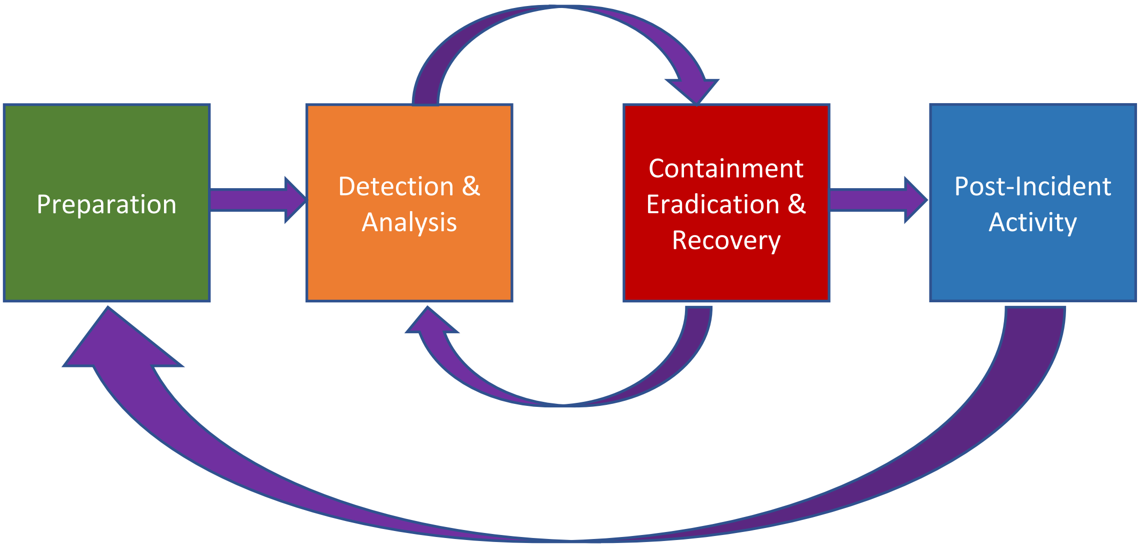


Fig. 3 – Incident Response Life Cycle

IR phase B and C may need to be performed iteratively and recursively.

The time window for the incident handling ransomware ***usually is limited to 48-72 hours***

The detection of security breaches is heavily dependent upon the protection solutions deployed, whether on premise or in the cloud. A baseline needs to be established to detect anomalies, for example, and events need to be monitored continuously to alert the organization the moment an incident occur. During the analysis phase of an incident, the incident response team will analyse endpoint, network, and log data to attempt to identify the root cause and pinpoint any additional compromised systems. After analysing the event and confirming the severity of the incident, the organization should perform necessary actions to limit the impact of the incident by containing the infection or behaviour and ultimately begin recovering from it.

After the incident is adequately handled, the organization should prepare a report that details the attackers' activities, a summary of the incident, procedures for remediation, and the steps the organization should take to prevent a future incident. The post-incident phase contains important organization-wide lessons to learn and apply across the people, processes, and technologies in place.

Preparation

This is the initial phase where organizations will perform preparatory measures to ensure that they can response effectively to the incidents if and when they are discovered. It involve all planning works such as: develop policies and procedures, setting up cyber incident response team (CIRT), setting incident reporting mechanism, issue tracking system, preparing systems (or a jump kit) that are installed with all necessary tools and hardware to acquire forensic images for the organization's all kinds of computing systems, including: RAID-5 servers and virtual machines created on Microsoft Hyper-V or VMware EXSI environment.

The first responder should be provided with the organization's incident response (IR) plan. If such document is not available, the responder should prepare one on the spot (we provide our Incident Reporting Form, in the Appendix, to help you in preparing the IR plan and triage processes). The IR plan and triage should contain the following documents:

- Contact information of the in-house IR team
- Communication plan
- Escalation & notification procedures and reporting mechanism
- Telemetry of the involved network – high-level network map and list of critical systems
- Information on how to access to images of clean OS, different versions of backups and application installations for restoration and recovery purposes
- Documents of current baselines, endpoint security, network security, malware prevention, user awareness and training, patch management and vulnerability policies
- In most of the ransomware cases we encountered in the past, the infected organization can only be able to provide limited information described in the above. In this case, the incident responder is required to obtain such information as much as possible or using our Incident Report Form as a help for your triage process.

Detection, Identification & Analysis

The second phase is where organizations should strive to detect and validate incidents quickly. Infections can spread through an organization rapidly. Taking corrective action immediately will minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains as a result of the incident.

Detection includes monitoring endpoints, network traffic, logs and SIEM data sources. Looking for anomalies on login/logoff, spikes in network activities for data exfiltration and raise alerts on suspicious events. Not every security “event” will need to be escalated as an “alert” and not every alert will be classified as an “incident”. All alerts need to be identified or categorized (malware, system compromise, PII, spam ransomware or any other kind of attack), then prioritized after triage. Incidents can be classified into multiple categories.

Incidents can occur in many ways. Different types of incidents require different response strategies. The attack vectors (email, web, removable device, network) combined with the initial observations will help the incident reporter correctly classify the incident.

Analysis includes the study of the indicators of compromise (IoCs) and the breadth and depth of the incident need to be analysed. Analysis of an incident, either successful or failed, can provide significant insight of possible threats to an organization. In some cases, like Ryuk ransomware, the intrusion is not an isolated case, but represents a part of the complex campaign. Before the artifacts or the signs of an incident can be analysed, we have to identifying how the attacker entering the network.

- Incident discovery (i.e. signs of the incidents) - ransomware can be discovered from:
  - Anti-spam or email filters alerts
  - Anti-virus software alerts
  - Anti-spam browser plug-in alerts
  - EDR solution alerts – most advance threats are polymorphic to bypass anti-virus or other protection layers deployed in an enterprises environment. By focusing on generic signature detection mechanism may not good enough to detect the attacks.
  - SIEM alerts and correlated event alerts
  - File integrity checking software alerts
  - Operating system, service and application logs
  - High volume of exceptional network or hard disk activities
  - Abnormal network flows and alerts
  - Alerts of Command and Control (C2) traffic from a compromised host
  - Informed by end users when they saw the ransom note or encrypted files
  - Informed by SOC analysts or law enforcement

- Detection and identification – ransomware usually does not try to hide:
  - Popped-up ransom note on screen

  - Personal files (images, movie, files, documents, text files) were encrypted with unique extension
  - Network drive folders or files on USB connected NAS devices encrypted
  - Infected system was locked due to some system libraries was encrypted
  - Infected system crashed due to some system libraries was encrypted
  - Services disrupted due to some application libraries was encrypted
  - Annoying message of pornographic images displayed and not able to remove
  - For a Windows system that is joined to an Active Directory (AD) domain, files in a users' roaming profiles[7] may also be encrypted. Responder needs to investigate if there are any other files (images, movie, files, documents, text files) of the investigating system were encrypted. If some files are not encrypted, there is a possibility that ransomware was not executed on this system.

- Incident validation – confirm and verify the possible delivery vector of the ransomware
  - For common ransomware, there are two delivery vectors, they are:
    - From a phishing email that was sent to an user's mail box, either a binary or .zip attachment was executed after a password was entered
    - From an vulnerable browser accessed a compromised web site and the ransomware was executed after automatic download
  - For WannaCry like ransomware, the unpatched system service in kernel land was exploited and the ransomware was downloaded from the C2 server or dropped from the exploits
  - For ransomware like Ryuk (online references can be found at our website), the malware was actually downloaded or copied to a share folder from a compromised system running inside the organization's internal network. Sometimes, the ransomware was indeed planted and executed manually by the attacker either through an valid authenticated remote session or stealthy remote access tool (RAT) coming from the Internet

- Incident categorization, prioritization and scoping
  - Follow the IR plan or any security policies of the investigating organization.
  - Determine the infection path by asking questions to identify how it was first found and which system was first being infected
  - Scope the incident to identify the number of infected machines and ask the organizations to provide a detailed network map and complete inventory of systems, including BYOD systems, used in the organization for determine and allocation of the resources
  - The scope may need to be further updated after the containment and eradication phases
  - Scoping needs to consider functional and information impacts of the incident
  - Estimate the time and resources to acquire forensics images of the infected systems and prioritization to acquire images for the critical systems

[7] https://www.virtualizationhowto.com/2011/02/beware-roaming-profiles-malware-infection/

    - Consider to initiate the organization’s business continuity plan (BCP) and discuss all the risks on limited scoping to the IR team and involving responsible senior management

- Incident analysis – Checking for the artifacts or IOCs
    - For common ransomware attacks, check the ransom note, capture the ransom note screen, identify the encrypted files with it unique extension and hash, anti-virus alerts, the timestamp of ransomware dropped, check the hash with online scanner and if live forensic is allowed, extract the ransomware for further analysis.
    - If the ransomware was downloaded from a web session, check the browser log for other artifacts such as: IP address, domain or URL involved in the communication.
    - If EDR or SIEM tools was available, check the process tree with timestamps to identify when or where the ransomware was executed.
    - For ransomware like Ryuk or cases without suspicious alert found, check the timestamp of ransomware and identify how the ransomware was delivered by checking the firewall or network device logs.
    - If the ransomware was copied by a RAT or other system utilities, such as PowerShell, try checking all system or event logs from the infected system
    - Continuous searching for the executable files by the identified hash and develop signature rules (such as yara rules) to scan all other unaffected systems for further malware hunting.
    - If additional infections found, consider to expand the original defined scope
    - Consider to deploy compromise assessment tools or threat hunting tools to monitoring all running endpoints
    - Consider to deploy network Intrusion Detection System (IDS) inside the internal subnets (not only putting the IDS at the egress point but between all internal subnets and the critical systems) to monitoring the abnormal network activities between the critical systems and all desktop machines

- Incident reporting – escalation notification and reporting of the incident to appropriate parties *(smart recipe: don’t hide)*
    - Implement the organization’s security IR plan, if any
    - Notification to appropriate persons that are defined by the organization’s communication and notification plans
    - During incident handling, the IR team needs to be provided the updated status. In some extreme cases the entire organization needs to be notified after consulting the responsible senior management
    - If the incident is confirmed, consider to give notification to law enforcement, insurer, employees or relevant regulatory bodies according to the IR plan *(smart recipe: don’t hide. Example: Pitney Bowes[8])*
    - Responsible senior management needs to be advised that there are serious inherence risks before consider to pay the ransom

[8] https://maintenance.pb.com/pbcom/outage.html

Containment, Eradication & Recovery

The third phase, containment, is the initial attempts to mitigate the actions of the attacker, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in pace for making containment-related decisions that reflect the level of risk acceptable to the organization.

Containment includes following procedures to stop spreading of the ransomware or carrying out necessary procedures to prevent the exfiltration of data. Containment can be performed concurrent with Analysis. Shutting down the critical servers infected with ransomware may have a significant impact on some organizations. Incident responders need to make a quick and reliable recommendations to the responsible senior management to determine the containment and recovery procedures in details.

Eradication consists of the longer-term mitigation efforts which include steps to remove ransomware from the systems or removing unknown malware or backdoors from the compromised systems. In Ryuk ransomware (Triple-Threat) attack case, because the ransomware was planted manually by the attackers through the compromised systems within the internal network, cleaning only the infected systems or servers through anti-virus scan will found the infections again in a short operational time. The ransomware will come back and "reimaging" the infected systems also found not work.

Containment and eradication often require drastic actions, but recovery is the process of getting the organization network back to a state before the incident. Recovery include steps to restore ***clean*** data backup back to the compromised systems after a fresh installation. Newly installed systems need to be hardened and monitored to prevent re-occurrence. Recovery should be designed to all the infected organization return its business to "normal". The organization should define acceptable risks in dealing with the incident when they take back the possible infected systems back online. If such decision is made, incident responder needs to consider to deploy endpoint and network threat hunting tools to keep continuous monitoring of the infected network and systems.

- Common ransomware are not known to move laterally, it is good practice to isolate affected machines from the network (by disabling the network switch port to which an infected system is connected) as soon as a ransomware infection or presence of any other threat is suspected.
- Isolating affected machines also helps prevent ransomware from encrypting data on shared folders or mapped drives through the network
- Immediately secure backup data or systems by calling them back to on-site from a remote backup tape storage location
- Isolate the infected computers from the network immediately or blocking access to malicious network resources such as a domain, URLs or IP addresses

- Isolate or power-off affected devices that have not yet been completely corrupted
- Temporarily locking a user accounts or even an account of administrator group (sometime the organization may found this is an unknown account created by the attacker) to control the intruder
- Disabling system services or software that the attacker has exploited
- If possible, change all online account passwords and network passwords after removing the system from the network
- Identify all autorun locations for ensure ransomware or unknown malware will not be executed after reboot
- Removing all ransomware, related malicious software and tools installed by the attacker. Please note that simply download an anti-virus tool to remove a particular ransomware on a ransomware infected machine may not be able to remove the threats completely. Ryuk is an example because it comes with other malware
- Resetting all infected users, third-party accounts and even services accounts
- Re-creating shared secrets including, VPN tokens, passwords or certificates
- If your organization is infected with ransomware like Ryuk, we have provided a special checklist under the appendix to help you to handle the incident in an expedited manner

Post-Incident Activity

Because the handling of a malware incident can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after the incident to prevent similar incidents from reoccurring.

Post-incident refers to the process of identifying lessons to be learned after actions and review. We need to answer basic questions like: (a) what happened? (b) have we done well in protecting the organization's network? (c) could we have done better? And (d) shall we do differently next time?

Policies and procedures may need to be modified.

- Prepare a detailed Incident Response Plan and established an Incident Response Team
- If ransomware was found coming from a phishing email, track the sender and message by marking the source of spam
- Check email header for unique X-Mailer or send IP address information and add message transport rules.
- Remind end-users to move the attack emails to the "junk" folder and report spam or malicious emails to the IR or Threat team
- Consider to deploy DMAC and install anti-phishing solution
- Set appropriate rules to your IDS, firewall or browsers' plug-ins to block malicious websites
- Sinkhole the C2 domain on internal DNS servers
- Ensure proper patch management policy
- Ensure proper vulnerability policy
- Deploy advance end-point solution to keep real time continuous monitoring
- Deploy SIEM for critical subnets for detail security analytic monitoring
- Deploy application white listing to critical systems
- Establish threat hunting capability
- Consider to take a proactive defence by implementation of Cyber Threat Intelligence (CTI) as a part of the Incident Response Cycle because once CTI fits into the incident response process, it help responders understand the adversaries in order to reduce the time it takes to detect, defence and remediate intrusions. (such as: handling Ryuk threat is different from common ransomware infections)

Incident Reporting Form

☐ Declaring an Incident ☐ investigation in progress (**by DAT**) ☐ Incident closed (**by DAT**)

What assistance do you require?

- ☐ Immediate on-site service ☐
- ☐ Root cause analysis
- ☐ Confirm of data leakage ☐
- ☐ Reporting to CERT ☐
  regulating bodies
- ☐ None needed at this time (notification only)

Type of Incident:

- ☐ Malware/Ransomware
- ☐ Denial of Service Attacks
- ☐ Intrusion/Compromised
- ☐ Account Takeover
- ☐ User Account Compromise
- ☐ Data/Intellectual Property Theft
- ☐ Business Email Compromised (BEC)
- ☐ Data Leakage/PII

Project	[*]	Date	DD/MM/YYYY	Email	[*]
Version		Contact	[*]	Mobile	[*]
Client Team:					

Description

This Incident Reporting Form is to be used as a template for your organization to report a suspected incident to Dragon Advance Tech Consulting Company Limited (“DAT”). Properly completing this form will allow DAT incident responders to perform effective triage on your incident and as a result, we can provide you a promptly and accurate identification and validation of the incident.

DAT incident responders should ensure this form be completed and if the information is collected during meeting with you, please make sure client’s IR team confirm the information.

Instructions

Please note that completed forms are classified as ***Confidential information***.

Section I – Incident Description (i.e. What happened? To be completed by the staff or DAT’s first responder)

1. Please provide an accurate description of the organization’s privacy commitment in local or international judications, including GDPR, on reporting incidents, even if they

are of a questionable or limited nature. You must also first notify your cybersecurity insurance broker and then to your in-house legal office, human resources (HR) or responsible senior management.

2. Print (or Type) clearly. Omit your name if you wish to remain anonymous.

3. The completed form should be distributed to DAT incident responders and copied or emailed to the following appropriate official:
    a. List Security Office mailing and/or <email address>.
    b. List Legal Office mailing and/or <email address>.
    c. List Responsible management mailing and/or <email address>.

Section II – Additional Comments (To be completed by the Legal Office Personnel or anyone in your organization who is assigned to take care the similar job in responding to the Report, in Hong Kong, please follow the Advisory Guidelines provided by PDPC)

1. What action was taken, by whom, and when, if known. Also, use the "Additional Comments" block to add any relevant or pertinent remarks regarding the incident.

2. The Legal Office Personnel needs to classify if the incident is a confirmed or suspected incident when completing this Form.

3. Forward the Form to the Chief Security Information Officer (CISO) or Chief Information Officer (CIO). Keep a copy of the form for your internal files. Incident reports with confidential information must be handled according to privacy and security policies and not transmitted electronically without the approved encryption method to secure confidential and other sensitive information.

4. If your organization keeps any personal data as defined under GDPR, please consult your legal counsel and CISO/CIO to consider if your organization is required to make a notification to the supervisory authority.

5. In Hong Kong, currently there is no requirement to report cybersecurity incidents to any government body, except you can voluntary report to the Hong Kong Computer Emergency Response Team (HKCERT) or the Hong Kong Police. If you are a financial institution, you may need to review and consult to relevant guidelines issued by Hong Kong Monetary Authority (HKMA) or Security Future Commission (SFC) from time to time.

6. If your organization has bought any kind of ***cyber insurance***, depends on the insurance contract, you may consider designating a person (i.e. insurance brokter) to take the role to make necessary notifications to the insurer and establish proper communication with your IR team before we can commence the incident response services.

Section III – Security Officer Comments (To be completed by the Security Officer. ie. CISO/CIO or similar role)

1. Provide comments in Section III describing the type of action taken in this particular incident.

2. Distribute copies of the completed form to the Human Resources Division, the Security Incident Team, and other officials involved in the incident.

References

ISO 27002: 13.1.1 Information security incident management
NIST SP 800-61r2 : Computer Security Incident Handling Guide (Draft)
NIST SP 800-53r4: IR-6 Incident Response Reporting
SANS.org Incident Handler's Handbook

Related Documents

Section I – Incident Description (To be completed by staff or DAT's first responder)			
1. Category of Incident or Responsible Parties		2. Name of Person Reporting Incident (Optional)	
3. Location of incident		4. Telephone No.	5. Office
		6. Date of Incident	7. Time of incident
8. Detailed Description of Incident (Include as many details as possible, including which systems were used or compromised.) [questions for ransomware: • When (date) was the incident first noticed? • Who noticed it first? • What was the initial indicator of the incident/issue? • What steps have you taken so fare? • Has any law enforcement organization been notified of this incident? • Has any other third party (other than that in above been notified of this incident? • What is the current status of the incident? • How would you best describe the incident?			

8. Individual(s) Notified (*Check all that apply*)	9. Time & Date Notified	10. Name/Title/Ph No/Address of Person(s)
□ Information Security Representative (A)		
□ Information Technology Representative (B)		
□ Security/Privacy Officer		
□ Senior responsible management		
□ Human Resources		
□ Corporate Legal Officer		
□ Outside organizations (please describe):		
□ Other (please describe):		

Section II – Additional Comments (To be completed by security personnel or DAT's first responder)

11A. Explain Action Taken, By Whom, and When, If Incident Was Corrected by Management. Add Any Other Pertinent or Relevant Remarks. Example questions:

- When was the incident first noticed?
- Who noticed it first?
- What was the initial indicator of the incident/alert?
- What steps have you taken so far?
- Has any other third party (including LE) involved?
- What is the current status of the incident?
  How would you best describe the incident?

11B. Incident Response Scoping Worksheet. Example questions:

- Are your critical systems cloud based, physically located in your environment, or both?
- What are the current geographical locations(s) of your system?
- What are the general hardware specifications (obtain an inventory list)?
- How is your network segmented (obtain a network map)?
- Do you have 3rd party vendors who have access to your infrastructure?
- What resources do you have on-hand and available, with regards to:
  - Cloud-based logs
  - Firewall/IDS logs
  - Firewall configuration files
  - VPN logs
  - System logs (in case of Windows environment, all event logs)
  - Centralized Anti-virus/EDR logs
  - Netflow
  - Network traffic captures, if any
- What are your goals going forward?
  - Is there a SOW of services we can send over?
  - Are backup systems and images clean?
- What is your desired timeframe for a response?
- What is the dress code at the location(s)?
- Additional notes from the interview/call

Section III – Security Officer Comments (To Be Completed by Security Officer or or DAT’s first responder)
12. Explain Type of Action Taken in This Incident (Document all communication, identification and containment actions with the helps with Chain of Custody Form, see attached)

Incident Communication Form		
Time & Date	Initiator / Receiver	Discussion details

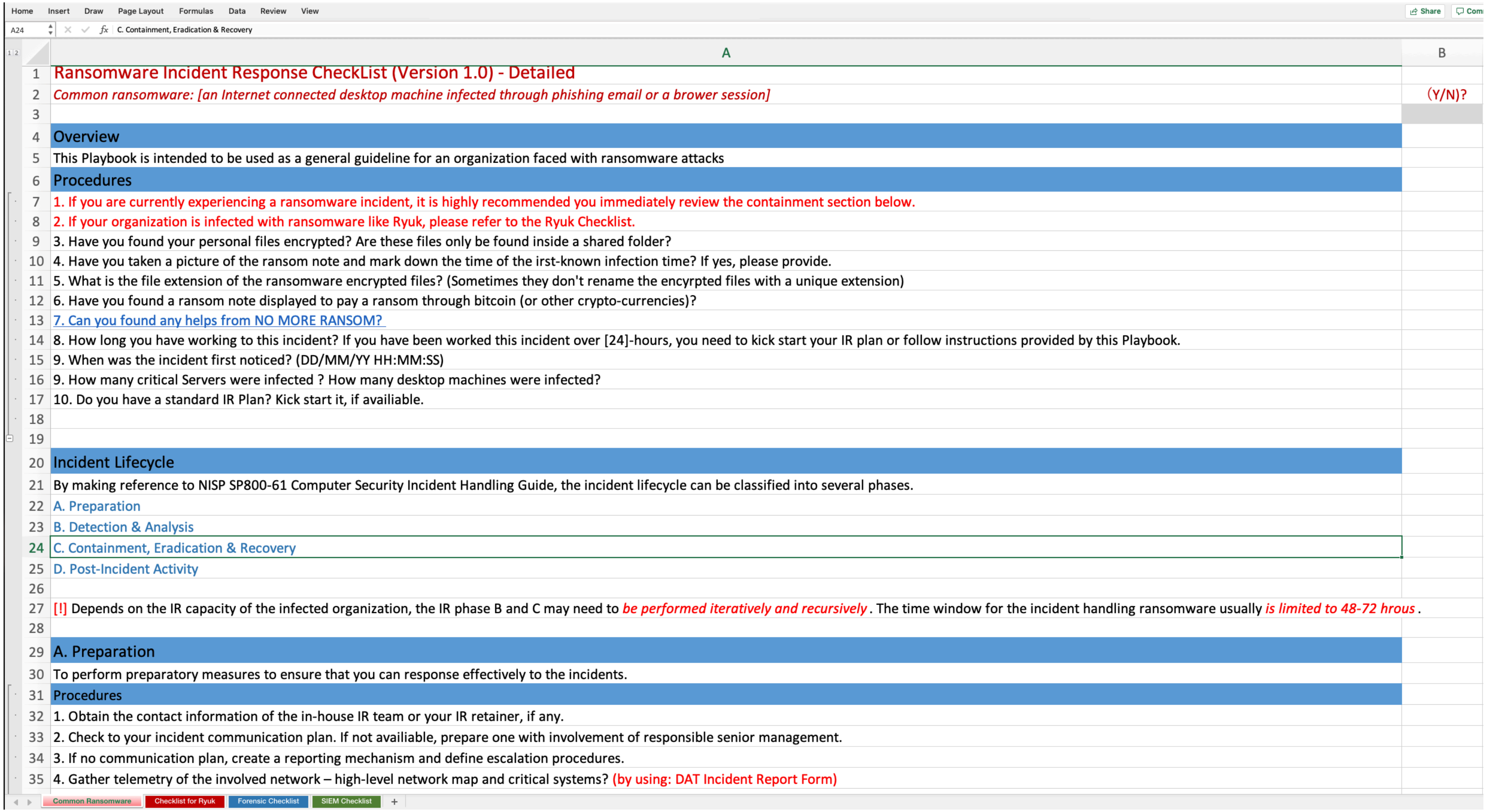
Incident Identification Form		
Time & Date	Internal IR or DAT Responders	Details Identified

Incident Containment/ Eradication Form		
Time & Date	Internal IR or DAT Responders	System Isolated and Actions Performed

<table>
<tr><th colspan="5">Evidence/Property Chain of Custody Form</th></tr>
<tr><td>Reference no.</td><td colspan="4">Description (Case Number)</td></tr>
<tr><td>Item no.</td><td>Quantity</td><td colspan="3">Description of Articles (If physical device, include manufacturer, model, and serial number)</td></tr>
<tr><td>Date/Time</td><td colspan="2">From</td><td>To</td><td>Purpose of Change of Custody</td></tr>
<tr><td></td><td colspan="2">Name
Organization
Signature</td><td>Name
Organization
Signature</td><td></td></tr>
</table>

Date/Time	From	To	Purpose of Change of Custody
	Name Organization Signature	Name Organization Signature	
Date/Time	From	To	Purpose of Change of Custody
	Name Organization Signature	Name Organization Signature	
Date/Time	From	To	Purpose of Change of Custody
	Name Organization Signature	Name Organization Signature	

Extracted Detailed Checklist



A24 | *fx* C. Containment, Eradication & Recovery

	A	B
1	Ransomware Incident Response CheckList (Version 1.0) - Detailed	
2	*Common ransomware: [an Internet connected desktop machine infected through phishing email or a brower session]*	(Y/N)?
3		
4	Overview	
5	This Playbook is intended to be used as a general guideline for an organization faced with ransomware attacks	
6	Procedures	
7	1. If you are currently experiencing a ransomware incident, it is highly recommended you immediately review the containment section below.	
8	2. If your organization is infected with ransomware like Ryuk, please refer to the Ryuk Checklist.	
9	3. Have you found your personal files encrypted? Are these files only be found inside a shared folder?	
10	4. Have you taken a picture of the ransom note and mark down the time of the irst-known infection time? If yes, please provide.	
11	5. What is the file extension of the ransomware encrypted files? (Sometimes they don't rename the encyrpted files with a unique extension)	
12	6. Have you found a ransom note displayed to pay a ransom through bitcoin (or other crypto-currencies)?	
13	7. Can you found any helps from NO MORE RANSOM?	
14	8. How long you have working to this incident? If you have been worked this incident over [24]-hours, you need to kick start your IR plan or follow instructions provided by this Playbook.	
15	9. When was the incident first noticed? (DD/MM/YY HH:MM:SS)	
16	9. How many critical Servers were infected ? How many desktop machines were infected?	
17	10. Do you have a standard IR Plan? Kick start it, if availiable.	
18		
19		
20	Incident Lifecycle	
21	By making reference to NISP SP800-61 Computer Security Incident Handling Guide, the incident lifecycle can be classified into several phases.	
22	A. Preparation	
23	B. Detection & Analysis	
24	C. Containment, Eradication & Recovery	
25	D. Post-Incident Activity	
26		
27	[!] Depends on the IR capacity of the infected organization, the IR phase B and C may need to *be performed iteratively and recursively* . The time window for the incident handling ransomware usually *is limited to 48-72 hrous* .	
28		
29	A. Preparation	
30	To perform preparatory measures to ensure that you can response effectively to the incidents.	
31	Procedures	
32	1. Obtain the contact information of the in-house IR team or your IR retainer, if any.	
33	2. Check to your incident communication plan. If not availiable, prepare one with involvement of responsible senior management.	
34	3. If no communication plan, create a reporting mechanism and define escalation procedures.	
35	4. Gather telemetry of the involved network – high-level network map and critical systems? (by using: DAT Incident Report Form)	