الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Cyber Security Guidelines

Ransomware Attacks

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "Cyber Security Guidelines for Ransomware Attacks" - V 1.0 - Currently Confidential to be made Public after approval, to help organizations, understand and mitigate against Ransomware attacks.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "Cyber Security Guidelines for Ransomware Attacks".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

LEGAL MANDATE(S)

Emiri decree No. (1) of the year 2021 regarding the establishment of National Cyber Security Agency, sets the mandate for the National Cyber Security Agency (hereinafter referred to as "NCSA"). The NCSA has the authority to supervise, regulate and protect the security of the National Critical Infrastructure via proposing and issuing policies and standards and ensuring compliance.

This document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), shall take precedence. Any such term (specific provision or clauses), to that extent shall be deemed omitted from this Document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Table of Content

1. Introduction

1.1 Context

Information systems today face unprecedented risks from a range of threat actors. These risks include unauthorized disclosure of information, unauthorized modification of information, and non-availability of information amongst others. This risk is perpetrated through several attacks such as Malwares, Ransomware that may either wipeout the data or render it unusable by encrypting it, Denial or Distributed Denial of Services attacks, physical attacks on the information systems and its processing facilities etc.

Ransomware is one such threat amongst the latest breed of attacks that has caused sleepless nights from small and medium enterprises to large corporate enterprises, and the government organizations. Organizations across a spectrum of sectors and diverse verticals have been a victim of such attacks.

To summarize, Information systems nowadays are more vulnerable to data leaks and service interruptions than ever before. Ransomware is a major danger to businesses of all sizes. It has been growing, in terms of size, complexity, and malice. It has the capability to cause unauthorized information disclosures (data leakages), integrity violations (data has been encrypted and rendered useless), eventually leading to non-availability of information. Organizations may use this guide to understand and prevent ransomware threats

2. Purpose, Scope, and Usage

2.1 Purpose

This document aims to provide organizations in the state of Qatar with the knowledge they need to better understand and defend against Ransomware attacks

2.2 Scope

All Organizations that use computers and digital devices to transact their business.

2.3 Usage

The guidance provided in this document will help organizations secure their digital infrastructure against Ransomware attacks. The document provides an understanding of different kind of Ransomware attacks and remediation against the same.

3. Key Definition

Organization	Refers to any business (including for-profit and not-for-profit) organization operating in the State of Qatar
Computer Hardware	Any computer hardware device, peripheral device, network device, server. etc., owned or leased by the client
Deep Web	It is any part of online information on the internet that is not indexed by search engines. This includes but is not restricted to websites that gate their content behind paywalls, password protected websites and contents of emails amongst other things.
Dark Web	Dark web is a subset of the deep web and it is commonly linked to criminal behavior. Generally, the content on the dark web is intentionally hidden and requires special software like anonymizing and encrypting tool e.g. Tor Browser to access. These sites tend to keep their users and their locations anonymous and are primarily used for malicious activities.
Decryptor	Decryptor is a specific piece of software used to remove the encryption that ransomware has applied to data.
Malware	Refers to any software intentionally designed to cause disruption to a computer, server, client, or computer network to deliver harmful undesired result such as leak of private or confidential information, gain unauthorized access to information or systems, deprive access to information. Viruses, worms, trojans, spyware, and adware are all examples of malware.

4. Guidelines

4.1 What is a Ransomware?

Ransomware is a type of malware that is used by malicious actors, primarily to extort money from their victims. It can also be considered as a form of Cyber Extortion. Currently Ransomware ranks amongst the top threats faced globally and we have also seen cases targeting organizations and their vendors in Qatar as well.

Typically, such malwares act in two ways, either blocking access to the system (Locker Ransomware) or encrypting the files (Crypto Ransomware).

Within the larger scope of information security, Ransomware attacks typically impact the integrity and availability pillars of the CIA (Confidentiality, Integrity and Availability) Triad. However, in some cases it has been noted that the attacker also exfiltrate information and publish the information on public domain if the ransom is not paid, thereby also impacting the pillar of confidentiality.

4.2 Types of Ransomware Attacks

4.2.1 Locker Ransomware

This type of malware blocks basic computer functions, locking victims out of their computers. Victims can only see the lock screen or interact with a screen that contains the ransomware. The mouse and keyboard are partially activated to make the payment to the attacker. Apart from this, the computer is not operational. Locker malware usually does not destroy data nor does it target critical files, as its primary aim is to prevent victims from accessing the data. A timer with a deadline is displayed to pressure the victim to pay. Complete destruction of data is generally unlikely.

Some well known families of these ransomware type include Bad Rabbit, Petya/NotPetya etc.

4.2.2 Crypto Ransomware

This type of ransomware primarily encrypts the data, information or files on the victim's device, but does not interfere with basic computer functions. The victim can usually see the data and even use the system. However, they cannot access the data because of the encryption. Crypto Ransomware may also ask victims to make the payment within a certain time period, failing which all encrypted data is permanently deleted or disclosed publicly.

Some well-known families of these ransomware type include Cryptolocker, Wannacry, Locky, etc.

A variant of ransomware known as doxware or leakware is where the attacker instead of destroying the data, exfiltrates it, and then threatens to release it on public domains.

4.3 Understand the Risk:

Any computing device connected to internet is at risk of being infected with the ransomware. Usually such incident occurs through malicious attachments spread through phishing emails, drive by downloads through malicious websites, exploit kits that exploit unpatched software

Over the years, we have seen that the malicious actors have not spared anybody and such attacks have occurred for individual end users, as also small, medium, government, and large corporate organizations. In the recent past there have been incidents at a major shipping container organization as well as well several hospitals (even during peak CoVID times), amongst others.

Ransomware has become rampant due to a number of factors, primarily being factors such as efforts versus returns, crypto currency which provided some level of anonymity, willingness of the organizations to pay ransoms especially in case of availability of cyber insurance. Another important factor is the ease facilitated by dark services such as Ransomware As A Service (RAAS).

4.3.1 Likelihood of being attacked:

The risk likelihood is based on factors such as criticality of the organization and financial health of the organization, which will strongly influence the likelihood of the business owner paying up the ransom. It has also been noted that occurrences of Ransomware have increased with the adoption of Cyber Insurance and that cyber insurance could make organizations attractive targets for threat actors. Certain threat actors have actually tried to identify if their potential victim had cyber insurance as this increases the likelihood of target organizations paying the ransoms.

4.3.2 Who may attack your Organization?

The threat actor that can perpetrate a ransomware attack could be either internal or external. Internal threat agents include internal employee/s, contractors etc. These are primarily employees / contractors who are disgruntled due to various reasons, or have malicious intents. External threat agents include cyber criminals, and state-sponsored actors. The external threat actor profiles commonly associated with ransomware attacks are financially motivated cybercriminals, or nation-state actors.

Defining your threat actors helps Organizations to understand the attacker's motivation, capabilities and the attack complexity. It also helps in deciding on the Organization's mitigation strategies.

4.3.3 Attacker Motivation:

Although the primary motivation for Ransomware attacks is financial gain, political or ideological motives may also exist especially in the case of state-sponsored attacks.

Nevertheless, it has been observed that in some of the cases the victim organization ended up losing data in spite of paying the ransom (as the attacker did not provide the key or provided the wrong key), furthermore in some cases the victim organizations were ransomed again after paying the ransom.

4.3.4 Identify Areas of Risk:

For an organization to identify the areas of risk they need to:

1. Understand overall industry risks in context of their business.
2. Understand capabilities of threat actors.
3. Identify business critical systems and critical data assets, and the risk mitigation controls in place.
4. Understand the surface area of exposure i.e. the number of entry points or attack vectors that threat actors could potentially exploit.
5. Assess the maximum tolerable period of downtimes and the cost of downtime to business.

The factors above will help the organization assess the risk posed by threat of Ransomware attacks.

4.3.5 Why are Ransomware attacks so effective?

Several factors have helped in making Ransomware Attacks wide spread, its easiness comes on top of the list as there are established platforms (Ransomware as a Service (RAAS)) available in the dark web that can be rented by malicious actors to launch such attacks. Another factor is the growth of cryptocurrency which provides avenues for cyber criminals to amass money in potentially anonymous ways.

In some strange ways, cyber insurance also contributed to the increase in attacks as such policies included a provision for the cyber company to pay the ransom amounts, which in ways contributed to the decision of paying ransoms easier for the organizations.

4.3.6 Ransomware Impact:

Depending on the type of Ransomware attack, the impact could be one or more of the following:

Disruption of services / systems:

A ransomware attack will render your system unusable, unless the infection is disabled or the systems restored. This will cause a disruption of services provided by the infected computers. Imagine if the infected system is a critical infrastructure the impact could be multifold and may extend beyond your organization to other sectors or event at a national/international level.

Loss of Data:

In the eventuality of the organization being not able to unlock the system, the organization will stand to lose its data. Even if the data was successfully recovered from the backup, there will be a delta (the period between the last good backup and time now), a period for which the data will be lost.

Data Breach (loss of confidentiality):

Certain threat actors have been known, to not only encrypt the data, but also exfiltrate it to raise the threat and threaten victims of leaking their data on internet if the ransom is not paid. So not only there is a risk of losing data, but also the possibility of it getting leaked into public or sold in underground forums.

Once the data is leaked it further raises the risk of this data being used by other malicious actors to launch new attacks, business competitors to get access to confidential information such as financial records, customer information, patent or confidential business insights etc.

Financial Loss:

Any incident leads into some direct and indirect loss of money to the organization. Direct losses could include ransom (if any paid by self), cost of recovering the systems, resultant fines if any, increased insurance premiums etc. Indirect financial losses include loss of productivity, loss of potential revenues due to system unavailability, loss of competitive advantage to business competitors, etc.

Reputation Loss:

Incidents involving data disclosure by the attacker will impact the reputation of the organization as customers may lose confidence and trust in the organization.

Legal Impact:

Incidents involving data disclosure (especially personal data) may lead to regulatory investigations and potential fines. The incident could also open up the organization to potential legal suits from customers and vendors whose data may have been breached.

Indirect Impact:

Incidents such as Ransomware are also known to have psychological and emotional impact on individuals (employees within the organizations).

4.4 How to Mitigate Ransomware Attacks

4.4.1 General Controls - Being prepared

A threat such as a Ransomware needs a well thought of defense in depth strategy to be implemented by the organization.

1. **Design:**
    a. Ensure that the system is designed to be resilient against potential cyber-attacks.
    b. Use a multi-factor authentication system and password rotation to ensure protection against password compromises.
    c. Implement an access control system based on a Need-To-Know and Least Privileges basis.
    d. Segment the network based on the organization/business needs. Avoid using a flat network design. Use a firewall or web application firewall (WAF), Intrusion Prevention / Intrusion Detection Systems (IPS/IDS), and other controls to prevent ransomware from communicating with Command & Control centers.
    e. Install additional controls and monitoring at network gateway points such as Mail Gateways, Internet Gateways to scan for malicious traffic and automatically block suspicious emails, and block malicious links if user does end up clicking on them.
2. **Documentation:**
    a. Ensure that the organization has a documented set of policies and procedures in place to manage system monitoring, incident management, business continuity, crisis management, supply chain security, etc.
    b. Copies of critical documents including business continuity and disaster recovery plans should be stored offline so that they are accessible in case of a ransomware attack.
3. **Technical**:
    a. Harden your Infrastructure (Network. Platforms, Applications, Operating systems, Computing Hardware etc. by following the below:
        i. Limit the number of applications that are installed on the device. If possible implement whitelisting of applications installed on a corporate computing machine.
        ii. Configure/ enable browser security settings.
        iii. Disable Adobe Flash and other vulnerable browser plugins.
        iv. Disable macros on word processing and other vulnerable applications.
        v. Restrict user permissions for installing and executing software applications.

vi. Disable Remote Desktop Protocol.

vii. Ensure that the systems are patched and updated.

viii. Implement an endpoint security in place to detect and manage malicious attacks.

b. Make sure the organization has an effective backup strategy in place. Define playbooks to understand the frequency of backup needed, copies of rotation to be maintained, and the type of technology required to meet your organization's needs. Test the backups by restoring them on your test systems.

c. Make sure that the organization's resilience plans including business continuity plans (BCP), disaster recovery plans, and crisis management plans are tested regularly to ensure availability and continuity of systems.

d. Ensure the organization's detection tools are equipped with use cases that enables it to detect ransomware attacks.

e. Scan and monitor for suspicious file activities.

4. **Security Awareness:**

a. Implement a security awareness program in place to continuously make your users aware of the prevalent cyber threats, latest trends in phishing, vishing, social engineering and electronic scams. Test them from time to time to test the effectiveness of the awareness programs.

5. **Monitoring:**

a. Ensure that logs are enabled, collected, and analyzed.

b. Make sure the system (Log Management System) is configured with established use cases (for known attacks) to quickly detect any potential malicious attack.

c. Ensure that the organization subscribes to trusted threat advisories, that can update you on the latest threats and provide you with most updated indicators of compromises and TTPs (Tools, Tactics, and Procedures) of threat actors.

d. Configure your security infrastructure (devices such as firewalls, IDS/IPS etc.) to block known malicious IPs, domains etc.

e. Baseline your infrastructure's performance so that anomalies can be identified quickly.

6. **Emergency Contact:**

a. Create a Contact list to reach out to personnel (internal teams and support vendors) during an incident. Refer to Section 4-8 Incidents Management in the NIAS.

b. Establish contact with NCSA, Law Enforcement Organizations, and your ISP

7. **Evaluate Third Party offerings:**
    a. Consider having special on call agreements with organizations that specialize in handling such incidents, and data recovery services.
    b. Subscribe to forums/services that can provide cyber threat intelligence on such attacks.
8. **Supply Chain Security**
    a. Ensure that your vendors understand cyber security and have assessed the related risks and managed them through suitable controls. For critical functions, systems within the organization, third party risk assessments should be mandated.
    b. The vendors must be apprised of your organization's security policy and procedures.
    c. The standard contract with any vendor must:
        i. Incorporate cybersecurity requirements into vendor contracts and agreements,
        ii. Include an obligation for the vendor to report any data breach / system compromise to the organization within twelve (12) hours of a discovery. The vendor should be liable to update of any impact on the organization as well as the final report upon incident closure.

4.4.2 When the Attack Begins:

1. Once an attack has been detected, the immediate focus should be on containing the incident and restricting its spread in the network to minimize the damage.
2. Report the incident to National Cyber Security Agency. Refer to section 6.4 for contact details. If you want to register a cyber-crime, you may also need to report to Law Enforcement Agency (ECCC Department in MOI)
3. Identify which systems have been impacted and isolate them by disconnecting it from the network as Ransomware spreads rapidly on the network.
4. Identify what strain of ransomware has infected your systems and check if there are Decryptor available online. In recent years some governments and organizations have come together to help organizations battle the menace of ransomware by providing resources and even decryption keys online.
5. From an incident management and digital forensics perspective it is important to collect all relevant information that might help you analyze, and investigate the case. Consider appropriate chain of custody for the digital evidence that is collected to be admissible in the court of law if you decide to pursue the law enforcement and judiciary
6. The digital evidence, and logs to be collected and secured should include amongst other things:
    a. Partial portions of the ransomed data that might exist.
    b. All available log information.
    c. Ransomware variant name.

d. What systems are affected.

e. Original emails with full headers and any attachments, if attack was executed by phishing.

f. Copies of executables or other files dropped onto the system after accessing malicious attachments, including a splash page.

g. Any domains or IP addresses communicated with just prior to or during infection.

h. Virtual currency addresses to which payment is requested, and the amount being requested.

i. Any forensic analysis or incident response reports completed.

j. Any memory captures taken during execution of the malware.

k. Status of the infection.

l. Provide network topology.

7. Prioritize restoration of systems based on the criticality of the systems. While restoring systems, make sure that the backup copy used is clean and does not have the malicious files.
8. Make sure that the network is cleared of the threat. Scan all the systems, network, and logs using the identified Indicators of Compromise and the TTP's (Tools, Tactics, and Procedures) of the attacker to ensure that it is clean. Use the root-cause-analysis to identify the vulnerabilities that were compromised by the attacker and fix them.
9. Fix any other potential vulnerabilities that may be discovered and used to compromise the systems in future. There have been cases in the past, where ransomware victims have been targeted again in quick succession because the underlying vulnerability was not fixed.
10. If your organization is a victim of an attack, don't pay the ransom. Paying ransoms might seem to be a quick fix to resolve the problems but there is no guarantee that the attacker will release the key even after paying the ransom. Moreover, there have been cases where the attacker ransomed the victim again, even after paying the ransom since the underlying vulnerability was not fixed.
11. Also note that Qatar Central Bank vide its Circular Nos 6 of 2018 and Circular Nos 46 of 2019, has declared that trading in bitcoin is illegal, further no financial institutes should facilitate in any way the purchase, sale, or dealing in any virtual assets. As such the act of paying ransoms could be deemed a financial crime, and QCB would take a legal action against it
12. Further, please also note that in October 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC), USA issued an advisory prohibiting ransomware payments. The OFAC advisory further warned that the facilitators of such payments on behalf of the victims like financial institutions, cyber insurance firms and other companies involved in incident response and digital forensics may be doing so in violation of OFAC regulations. As a result, a number of Cyber Insurance providers around the world have now stopped providing ransom payment as part of their coverage.
13.

4.4.3 When the Attack Stops:

1. After the incident is over and the systems have been recovered, document what happened, perform a root-cause-analysis to identify what went wrong? Identify vulnerabilities in technology (e.g. outdated software, unpatched systems, or weak access controls, etc.), gaps in processes (e.g. inadequate or lack of procedures, undefined SLAs or OLAs etc.), and shortcomings in people behavior (e.g. work culture, lack of training etc.), that may have contributed in the systems being compromised.
2. Put in place a plan to remediate the vulnerabilities in technology, gaps in processes, and shortcomings in people behavior to prevent a recurrence of any such event in the future.
3. Identify areas of improvement that will help your organization avoid any such incidents in future and also improve your response and recovery during any such incidents.

5. Compliance and Enforcement

5.1 Compliance and Enforcement

This guideline is published to help organizations better understand the threat of Ran-somware attack and how to mitigate against such threats.

The guideline complements National Information Assurance Standard V2.1

6. Annex

6.1 Acronyms

NCSA	National Cyber Security Agency
OLA	Operational Level Agreement
RAAS	Ransomware As A Service
SLA	Service Level Agreement
TTP's	Tools, Tactics, and Procedures

6.2 References

National Information Assurance Standard v2.1 (NIAS)

6.3 Online Resources

Decryption Keys

https://www.nomoreransom.org/en/index.html

https://noransom.kaspersky.com/

https://www.avast.com/en-au/ransomware-decryption-tools#pc

https://www.emsisoft.com/en/ransomware-decryption/

https://www.trellix.com/en-au/downloads/free-tools/ransomware-decryption.html

https://www.cisa.gov/stopransomware

Identification of Ransomware strain

https://id-ransomware.malwarehunterteam.com/index.php

https://www.nomorweransom.org/crypto-sheriff.php?lang=en

6.4 Reporting Incidents to NCSA

Organizations that are experiencing an attack or are noticing any suspicious activities, may report an incident to NCSA in one of the following ways:

Call NCSA Hotline at 16555 (24 x 7 service)

Email NCSA at ncsoc@ncsa.gov.qa

Organizations may also reach out to NCSA if they need to investigate or require assis-tance to look if there is any data leakage related to them or their vendors.

Organizations may also find the following guidelines useful to prepare themselves to face an attack / incident.

Guidelines for Incident Management - Pre-requisite Measures