JOINT ADVISORY BY SINGAPORE POLICE FORCE, THE CYBER SECURITY AGENCY OF SINGAPORE (CSA) AND THE PERSONAL DATA PROTECTION COMMISSION (PDPC) SINGAPORE

JOINT ADVISORY ON RANSOM INCIDENTS INVOLVING NETWORK ATTACHED STORAGE (NAS) SYSTEMS

In recent weeks, the Cyber Security Agency of Singapore (CSA), Personal Data Protection Commission (PDPC) and the Singapore Police Force (SPF) have observed incidents where victims' data stored on their Network Attached Storage (NAS) systems were targeted by threat actors. Files on the NAS were removed, and a ransom note was left behind, demanding a ransom in the form of cryptocurrency such as Bitcoin.

2 This joint advisory highlight the observed Tactics, Techniques and Procedures (TTPs) employed by the threat actors to compromise their victims' networks, how victims can respond to such incidents, and provides some recommended measures for organisations and individuals to mitigate the threat posed.

<u>What are Network Attached Storage (NAS) Systems</u>

3 A NAS system is a specialised hardware appliance or server that is dedicated to storing and managing data in both home and business environments. These systems are connected to a network to facilitate storage and retrieval of data to multiple users and client machines from a central location. They often come equipped with their own operating systems and can offer features such as file sharing, data backup, media streaming, and remote access. Authorised users can also access NAS data remotely after authenticating to the corporate network.

Observations of Threat Actor Activity Targeting NAS Systems

4 Threat actors were observed to have performed logins to the NAS system through several methods such as using the administrator account(s) through valid user credentials, exploiting vulnerabilities identified in the NAS systems, and phishing attacks. Thereafter, a ransom note would be left in the system after deleting data stored on victims' NAS. This is different to typical ransomware activities, where data is encrypted for ransom. As there were no authentication failures of the victims' NAS systems observed, it is likely that the threat actors used the default or previously leaked credentials to carry out such attacks. An example of the ransom note that was left in the NAS system demanding a ransom to be paid within 15 days for recovery of the data can be found in the **Annex**.

Measures to Prevent Ransom Incidents Involving NAS Systems

5 Adopting proper cyber hygiene measures can contribute to a more robust system against breaches, improving the organisation's cybersecurity posture and safeguarding sensitive information. The following steps provide some measures that organisations and individuals should consider to secure their NAS systems:

1) Implement a Strong Password Policy

Changing the default password and having a strong password policy would drastically improve the security of user accounts, preventing unwanted access to the corporate network. This includes:

a) Password length of a minimum 12 characters
b) Complexity requirement (uppercase, lowercase, numbers, special characters)
c) Implement password expiration (e.g. change password every 90 days)
d) Implement account lockout after consecutive incorrect login attempts

2) Implement Multi-factor Authentication (M-FA)

a) Implement M-FA to prevent unauthorised logins in the event of a credential leak, especially if the NAS system is used to store confidential or sensitive personal data, or large volumes of personal data. As M-FA requires users to provide multiple forms of verification, it helps to mitigate the risks of unauthorised logins and adds an additional layer of protection beyond passwords.

3) Enforce Access Control

It is not recommended to expose the NAS system directly to the internet, even if doing so will provide convenience to users/clients. Users are advised to limit access to their NAS system via the following measures:

a) Reconfigure the existing firewall by adopting a whitelist approach, detailing authorised sources (i.e. trusted IP addresses, approved locations etc.) of network traffic. Only whitelisted sources should be allowed to communicate and exchange information with the NAS system.
b) Require the use of VPN for remote access to the NAS system as an additional layer of encryption and authentication for NAS access.
c) Segregate the corporate network to limit communications between internet facing services and internal servers, such as those containing sensitive data.
d) Do not use default configurations, such as default admin or user credentials, to access the NAS system.
e) Connect the NAS to the network via ethernet and disable its Wi-Fi feature, if possible. Otherwise, ensure that the Wi-Fi is configured securely.

4) Regularly Update Software

a) Ensure that all systems are regularly patched and updated. Source code reviews also help to detect web application vulnerabilities that may be exploited prior to performing lateral movement to the NAS system. These include those in the Open Web Application Security Project (OWASP) "Top Ten" list.

b) Deploy anti-virus and anti-malware solutions on devices and NAS connected to the network as it can help to prevent and detect ransom incidents.

5) Regularly Back Up Critical Data

a) Regularly back up critical data onto offline media (e.g. external hard disk) that are isolated from the NAS system. This will allow for system restoration which would help mitigate the impact of ransom incidents and minimise data loss. Backup media should be regularly tested to ensure that the backup data can be recovered and restored in time to help the business or individual recover from data corruption or destruction.

6) Regularly Review Logs

a) Reviewing perimeter logs can allow system administrators to spot malicious activities (e.g. active scanning of web servers and SQLi attempts). If malicious activities are detected, the source IP addresses can then be filtered, and organisations or individuals can conduct scoping on their internal networks for any signs of possible compromise.

7) Seek External Assistance

a) Organisations and individuals may wish to hire a professional firm to routinely perform web application penetration testing and vulnerability scanning to identify vulnerabilities that may enable threat actors to gain initial access to their network. Organisations and individuals should also seek professional assistance from cybersecurity service providers for incident response and remediation if a cybersecurity incident is confirmed.

How to Respond to Such Incidents

6 If your NAS system was compromised and data within was deleted and/or exfiltrated, you are advised to:

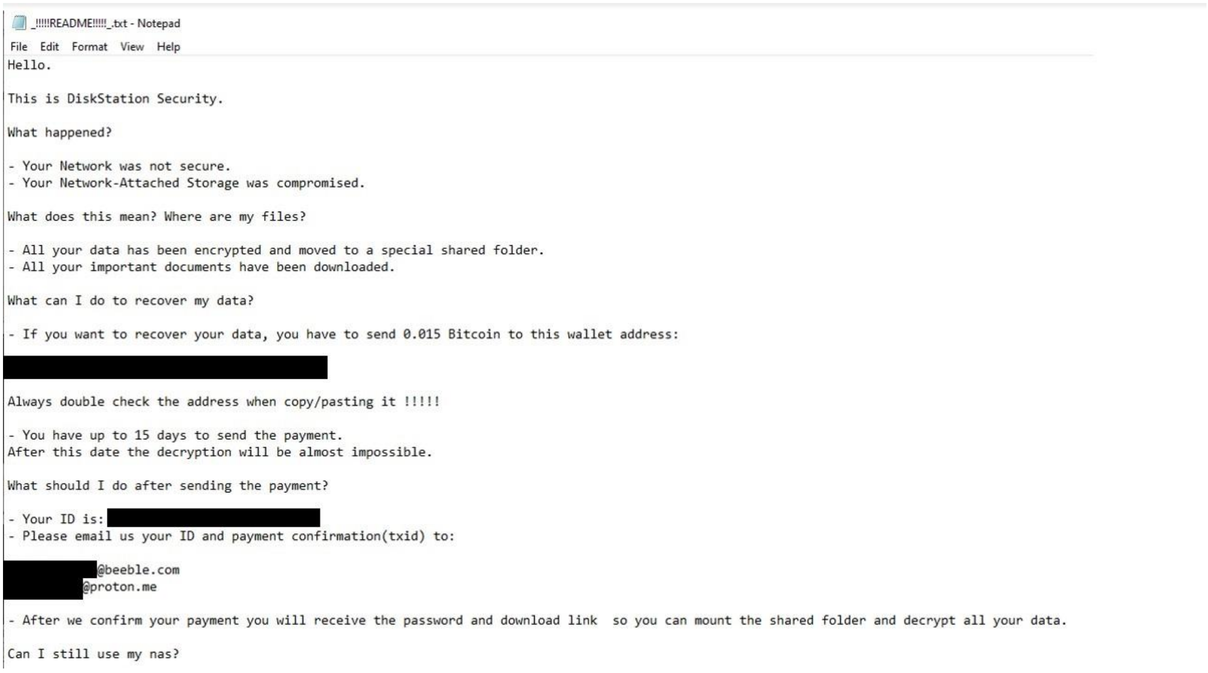
a) Lodge a report with SPF and the Singapore Cyber Emergency Response Team (SingCERT) immediately to receive assistance from the relevant authorities.
b) If you believe your employees'/customers' PII was compromised, report the incident to PDPC at https://eservice.pdpc.gov.sg/case/db. PDPC has also developed a guide to help organisations manage data breaches.
c) Take a screenshot of the ransom note and save the screenshot to keep a record of the information (e.g., Bitcoin address) within.
d) Prevent further unauthorised access to the system. Disable or reset the credentials of compromised accounts. If unsure, implement an organisation wide credential reset.
e) Contact your company's IT department and inform them of the incident. Follow the company's cyber-incident response plan, if any.
f) Conduct an internal investigation to determine how the incident occurred. Organisations may wish to consider engaging professional services from a cybersecurity provider if the incident occurred because of an intrusion into the company's system, to properly clean up and remediate the incident.

7 The CSA and SPF do not recommend paying any ransom as paying the ransom does not guarantee that the data will be recovered. It also encourages the threat actors to continue their criminal activities and target more victims. Threat actors may also see your organisation or you as a soft target and may strike again in the future.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY SINGAPORE
PERSONAL DATA PROTECTION COMMISSION
17 FEBRUARY 2024 @ 9.00AM

Annex

Snippet of the Ransom Note



```
Hello.

This is DiskStation Security.

What happened?

- Your Network was not secure.
- Your Network-Attached Storage was compromised.

What does this mean? Where are my files?

- All your data has been encrypted and moved to a special shared folder.
- All your important documents have been downloaded.

What can I do to recover my data?

- If you want to recover your data, you have to send 0.015 Bitcoin to this wallet address:

[redacted]

Always double check the address when copy/pasting it !!!!!

- You have up to 15 days to send the payment.
After this date the decryption will be almost impossible.

What should I do after sending the payment?

- Your ID is: [redacted]
- Please email us your ID and payment confirmation(txid) to:

[redacted]@beeble.com
[redacted]@proton.me

- After we confirm your payment you will receive the password and download link  so you can mount the shared folder and decrypt all your data.

Can I still use my nas?
```