JOINT NEWS RELEASE BY SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON THE DISTRIBUTION OF RANSOMWARE "DEADBOLT" TARGETING QNAP NETWORK-ATTACHED STORAGE DEVICES

The Police and the Cyber Security Agency of Singapore (CSA) would like to alert QNAP users on the distribution of a ransomware[1] variant, known as "Deadbolt", targeting internet-connected QNAP Network-Attached Storage (NAS) devices.

2. NAS devices are storage devices connected to a network that allows for storage and retrieval of data from a central location. Authorised users can access data remotely using a network connection.

3. In recent weeks, the Police and CSA have observed incidents where victims' data stored on QNAP NAS devices were encrypted by the "Deadbolt" ransomware variant. The encrypted files would typically have a (*.deadbolt)* extension added to each file. A ransom note would then be displayed on the "login page" of the NAS device to demand for payment in the form of cryptocurrencies such as Bitcoin, in exchange for access to their data.

4. The "Deadbolt" ransomware variant exploits unpatched vulnerabilities found in devices running outdated QTS [QNAP's NAS Operating System (OS)] versions, and/or vulnerabilities in outdated internet-enabled applications, such as Photo Station, running on QNAP NAS devices.

---

[1] Ransomware is a type of malware designed to encrypt files on a device until a ransom is paid to decrypt the files.

5. Administrators and users of QNAP NAS devices are advised to update their QTS and all applications running on their NAS devices to the latest versions to protect their devices from known vulnerabilities. Detailed patching instructions and recommended best practices for enhancing your NAS security, such as disabling port forwarding to prevent exposing the NAS to the Internet, can be found on QNAP's website[2][3][4].

6. In the event that your QNAP NAS device has been infected by the "Deadbolt" ransomware, members of the public are advised to take the following steps:

a. Lodge a police report immediately to receive assistance from the relevant authorities;
b. The Police and CSA do not recommend paying the ransom as demanded by the attacker, as it does not guarantee that your data would be decrypted, and encourages the attacker to continue their criminal activities and target more victims;
c. Take a screenshot of the "Deadbolt" ransom note and save the screenshot to keep a record of the information (e.g. Bitcoin address) within;
d. Follow detailed instructions by QNAP to update the firmware to the latest version and perform a malware scan to remove the malware at https://www.qnap.com/en/how-to/faq/article/what-should-i-do-if-i-found-the-nas-encrypted-by-deadbolt;
e. Check if your decryption key is available, and follow the unlocking instructions through the website https://deadbolt.responders.nu, which was created by cyber security vendor responders.nu in collaboration with the Dutch Police and Europol for "Deadbolt" ransomware victims. Please be advised to upload any files to this website using non-production computers;
f. If your decryption key is not available in the website above, visit the "No More Ransom" website (https://www.nomoreransom.org) for more decryption keys.

[2] https://www.qnap.com/en/security-advisory/QSA-22-19
[3] https://www.qnap.com/en/security-advisory/QSA-22-24
[4] https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

7. Besides QNAP NAS devices, other brands of NAS devices, such as ASUSTOR NAS devices, may also be targeted by “Deadbolt” ransomware variant. In general, members of the public are advised to follow the steps below to ensure that your devices are adequately protected against malware:

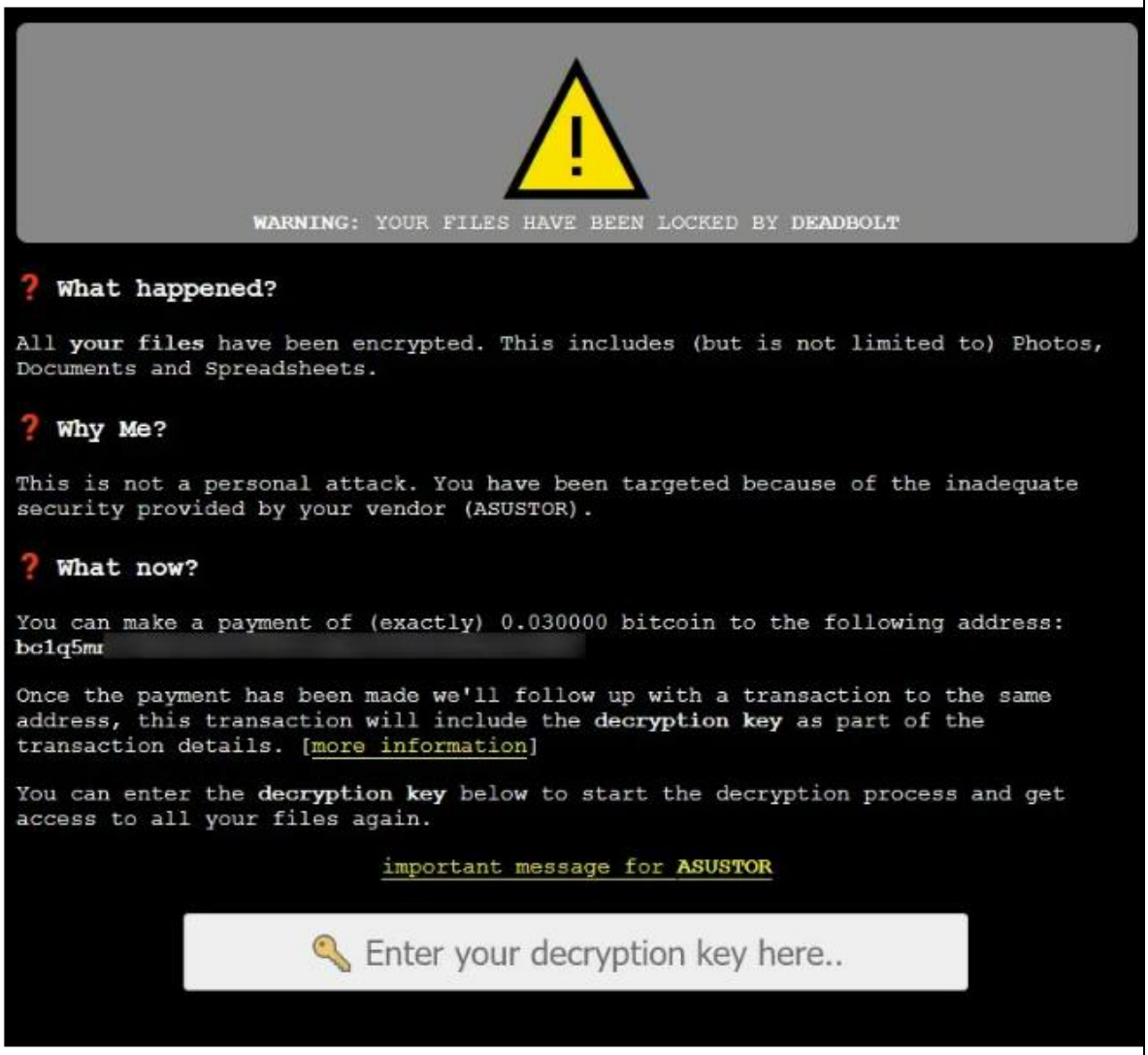
a. Ensure that your mobile phones and computing devices are updated regularly with the latest OS versions and install anti-virus applications that can detect and remove malware;
b. Download files, including applications and updates, directly from official verified sources as this ensures that downloaded files are free from malware or viruses;
c. Backup your data regularly in a separate system and keep it offline to retain access to your data in the event of a ransomware incident. Such data backups can be done using an external hard disk that is disconnected from your devices or in the Cloud;
d. Avoid clicking on suspicious looking links and pop-up ads or opening files and email attachments from unknown senders.

8. To find out more about ransomware and how preventive steps can be taken to protect your systems and data, you may wish to refer to CSA's SingCERT advisory at https://www.csa.gov.sg/en/singcert/Advisories/ad-2021-009.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
23 NOVEMBER 2022 @ 5:45PM

Annex A

Screenshot of Deadbolt Ransom Note



Source: BleepingComputer.com