Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 16/2021

Datum: 27.04.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland
Ransomware QLocker

Derzeit ist ein deutlicher Anstieg an Erpressungen mittels der **Ransomware „QLocker“** zu verzeichnen. Die Schadsoftware nutzt hierbei aktuelle Sicherheitslücken in den IT-Geräten der Firma QNAP aus, um die Netzwerkspeicher zu verschlüsseln und Lösegeld von den Geschädigten zu erpressen.

Hierzu wird von den unbekannten Tätern die gängige Software „7ZIP“ verwendet und die Datei mit einem nur den Tätern bekannten Passwort zu verschlüsseln.

1. Vorsorge

Die Firma QNAP hat hierauf bereits reagiert und stellt verschiedene Firmware Updates zur Verfügung. Es ist generell dringend zu empfehlen, Software auf dem aktuellsten Stand zu halten und Updates zeitnah einzuspielen. Insbesondere sollten die Funktionen „Multimedia Console“, „Media Streaming Add-on“ und „Hybrid Backup Sync“ aktualisiert werden.

Des Weiteren bietet die Firma QNAP in ihrem „APP Center“ eine Software namens „Malware Remover“[1] an.

[1] **https://www.qnap.com/en/app_center/con_show.php?op=showone&internalName=MalwareRemover&version=4.6.1.0&qts=4.5.1&seq=57&os=qts**

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

2. Maßnahmen

Sollte das aktuelle Verschlüsseln auf dem System festgestellt werden gibt es zwei Methoden, um den Prozess zu verhindern und gegebenfalls die Daten zu entschlüsseln.

Methode 1:

1. Installieren Sie die oben erwähnte „Malware Remover“ Software.
2. Stellen Sie eine Verbindung zu dem QNAP Gerät über SSH her.[2]
3. Führen Sie folgenden Befehl aus:
   cp `getcfg MalwareRemover Install_Path -f /etc/config/qpkg.conf`/7z.log /share/Public
4. Wenn „No such file or directory“ erscheint, bedeutet dies, dass das Gerät neugestartet oder bereits vollständig verschlüsselt wurde. Leider ist in diesem Fall keine Hilfe möglich.
5. Wenn der Befehl ohne Fehlermeldung ausgeführt werden konnte, wird im Öffentlichen Ordner des Geräts eine Datei „7z.log“ angezeigt, welche das Passwort enthält.
6. Das Passwort sollte etwa in der Datei „7z.log“ wie folgt aussehen:
   a -mx=0 -sdel -pmFyBIvp55M46kSxxxxxYv4EIhx7rlTD [Dateipfad]
   mFyBIvp55M46kSxxxxxYv4EIhx7rlTD ist in diesem Fall das Passwort.
7. Nun kann das Gerät neugestartet werden und das Passwort zur Entschlüsselung verwendet werden.

Methode 2:

1. Stellen Sie wie unten beschrieben eine Verbindung zum Gerät über SSH her:
   https://www.qnap.com/en/how-to/knowledge-base/article/how-to-access-qnap-nas-by-ssh
2. Nutzen Sie folgenden Befehl, um herauszufinden, ob die Schadsoftware gerade ausgeführt wird:
   ps | grep 7z
3. Sollte hierbei kein Hinweis auf 7z erscheinen, bedeutet dies, dass das Gerät neugestartet wurde oder der Verschlüsselungsprozess abgeschlossen ist. Leider ist in diesem Fall keine Hilfe möglich.
4. Falls 7z läuft, geben Sie folgenden Befehl in einer Zeile ein:
   cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;
5. Warten Sie einige Minuten und geben Sie folgenden Befehl ein:cat /mnt/HDA_ROOT/7z.log
   Das Passwort finden Sie wie oben beschrieben.
6. Nun kann das Gerät neugestartet werden und das Passwort zur Entschlüsselung verwendet werden.

[2] **https://www.qnap.com/en/how-to/knowledge-base/article/how-to-access-qnap-nas-by-ssh**

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

3. Hinweise auf eine Verschlüsselung

Bei einem erfolgreichen Verschlüsselung des Geräts wird eine Datei namens „!!!READ:ME.txt“ erzeugt, in der man aufgefordert wird, eine Seite im TOR-Netzwerk aufzurufen und den in der Datei befindlichen, persönlichen Code einzugeben. Auf der Seite wird man dann aufgefordert, 0,01 BitCoin zu bezahlen, um das Passwort zu erhalten.

Die Polizei rät:

- **Überprüfen Sie, wenn sie Produkte von QNAP nutzen, ob Sie alle aktuellen Updates eingespielt haben. Falls dies nicht der Fall ist, updaten Sie sofort.**

- **Sind Sie betroffen, gehen Sie nicht auf die Forderung der Täter ein.**

- **Im Falle der Betroffenheit, sollte in jedem Fall Anzeige erstattet werden.**

4. Quellen:

https://www.qnap.com/en/app_center/con_show.php?op=showone&internalName=MalwareRemover&version=4.6.1.0&qts=4.5.1&seq=57&os=qts

https://www.qnap.com/en/how-to/knowledge-base/article/how-to-access-qnap-nas-by-ssh

https://www.heise.de/news/Jetzt-patchen-Erpresser-knoepfen-Qnap-NAS-Besitzern-bislang-230-000-Euro-ab-6027863.html

Mit freundlichen Grüßen,

i.A.
KHK M.O. Schmitt
Zentrale Ansprechstelle
Cybercrime Saarland

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken