NAS 感染勒索病毒 AgeLocker 攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 09 月

一、事件簡介

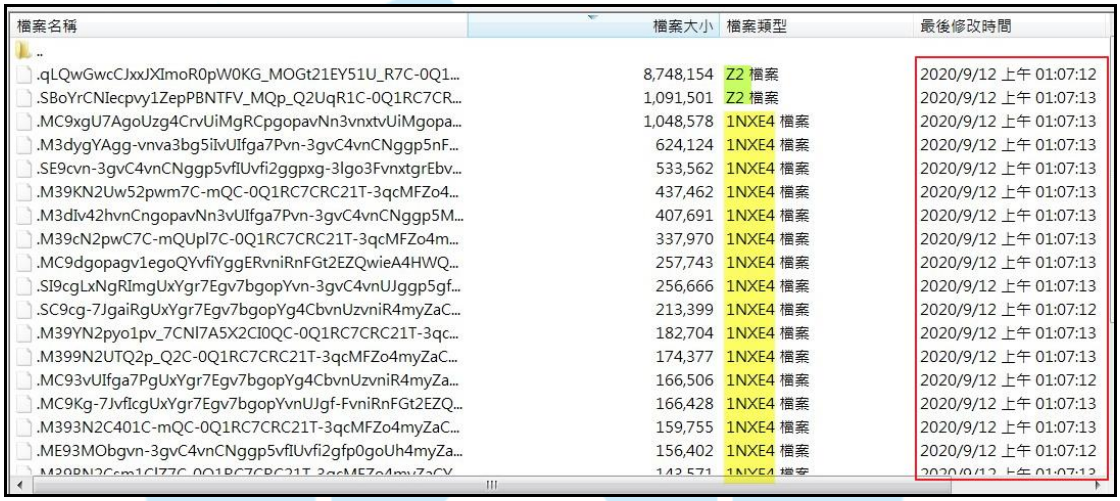
1. 由於存取的方便性，在學術網路中儲存裝置 NAS 是許多學校常用的設備。但因其為長期不關機的連網設備，又本身儲存著大量學校資料，因此 NAS 作為被勒索的設備之機率升高。
2. 2020/9 TACERT 接獲某學校通報該校存放資料的 NAS 感染勒索病毒，而且以 Web 平台登入 NAS 後看到每一個資料內原先存放的檔案都消失，僅有一封勒索通知信存在。
3. 透過 FTP 傳檔軟體連線 NAS 的資料夾時，可看到已被加密的檔案。
4. 由於學校無法判斷出所感染的勒索病毒名稱請求 TACERT 協助，故本中心取得學校所提供的勒索通知信與被加密的 2 個檔案後進行分析。

二、事件檢測

1. 由學校所提供的截圖可得知 NAS 內檔案在 2020/9/12 上午 12:34 至上午 1:07 之間被進行加密，而且被加密的檔案最後呈現兩種副檔名 1NXE4 與 Z2。由截圖也發現勒索通知信 HOW_TO_RESTORE_FILES.txt 在 2020/9/11 下午 10:48 曾被駭客修改過。

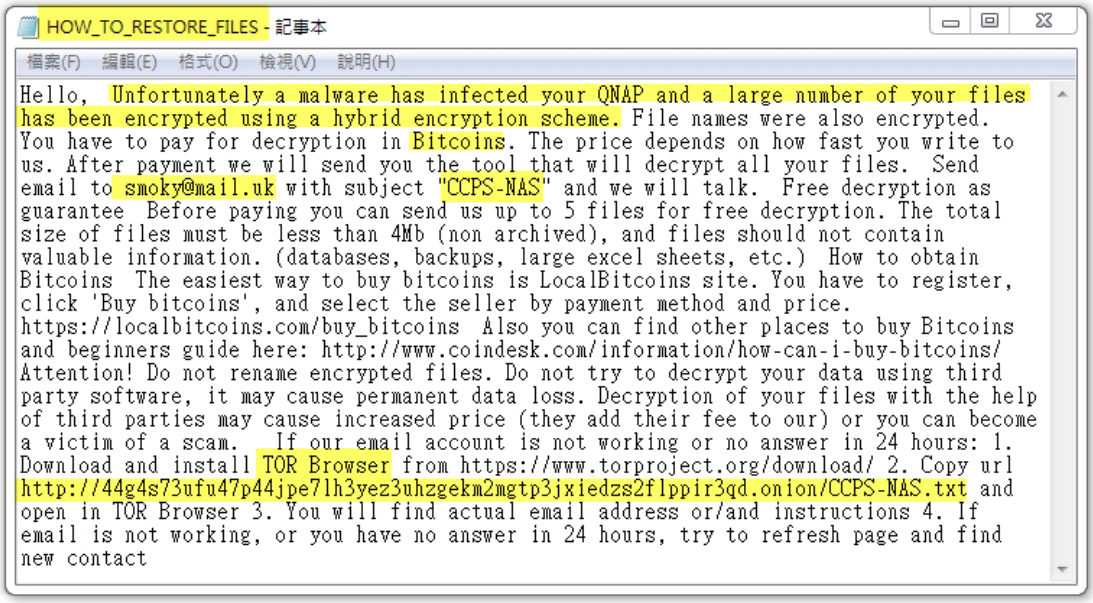
檔案名稱	檔案大小	檔案類型	最後修改時間	權限
..				
HOW_TO_RESTORE_FILES.txt	1,721	文字文件	2020/9/11 下午 10:48:03	-rw-rw-...
.vaQ3gvQ6vaQrgUxugoQYMObgMFq3MEgZLxSY4HWQ1i...	15,166	1NXE4 檔案	2020/9/12 上午 12:34:21	-rwxrwx...

檔案名稱	檔案大小	檔案類型	最後修改時間	權限
..				
.MObcMFNx4Aota3YcLmlXSb@@.1nxe4	37,107	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFNt4Aota3YcLmlXSb@@.1nxe4	30,093	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFNK4Aota3YcLmlXSb@@.1nxe4	30,464	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFNd4Aota3YcLmlXSb@@.1nxe4	38,050	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFNc4Aota3YcLmlXSb@@.1nxe4	34,450	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFNB4Aota3YcLmlXSb@@.1nxe4	32,969	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFN94Aota3YcLmlXSb@@.1nxe4	27,336	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFN34Aota3YcLmlXSb@@.1nxe4	36,975	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGY4Aota3YcLmlXSb@@.1nxe4	33,724	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGx4Aota3YcLmlXSb@@.1nxe4	29,476	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGt4Aota3YcLmlXSb@@.1nxe4	40,631	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGK4Aota3YcLmlXSb@@.1nxe4	26,658	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGg4Aota3YcLmlXSb@@.1nxe4	35,520	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGd4Aota3YcLmlXSb@@.1nxe4	30,416	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGc4Aota3YcLmlXSb@@.1nxe4	34,808	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFGB4Aota3YcLmlXSb@@.1nxe4	34,683	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...
.MObcMFG94Aota3YcLmlXSb@@.1nxe4	34,833	1NXE4 檔案	2020/9/12 上午 12:38:35	-rwxrwx...

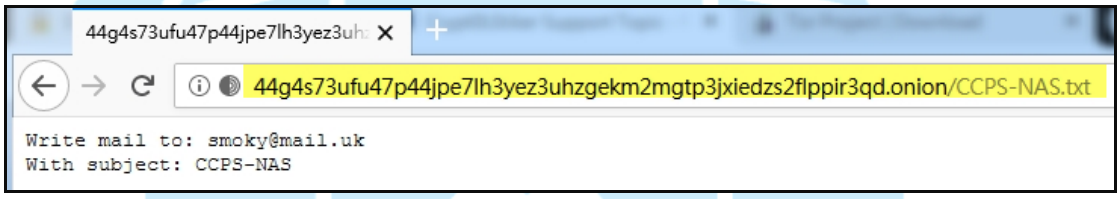


檔案名稱	檔案大小	檔案類型	最後修改時間
..			
.qLQwGwcCJxxJXImoR0pW0KG_MOGt21EY51U_R7C-0Q1...	8,748,154	Z2 檔案	2020/9/12 上午 01:07:12
.SBoYrCNIecpvy1ZepPBNTFV_MQp_Q2UqR1C-0Q1RC7CR...	1,091,501	Z2 檔案	2020/9/12 上午 01:07:13
.MC9xgU7AgoUzg4CrvUiMgRCpgopavNn3vnxtvUiMgopa...	1,048,578	1NXE4 檔案	2020/9/12 上午 01:07:13
.M3dygYAgg-vnva3bg5iIvUIfga7Pvn-3gvC4vnCNggp5nF...	624,124	1NXE4 檔案	2020/9/12 上午 01:07:13
.SE9cvn-3gvC4vnCNggp5vflUvfi2ggpxg-3lgo3FvnxtgrEbv...	533,562	1NXE4 檔案	2020/9/12 上午 01:07:13
.M39KN2Uw52pwm7C-mQC-0Q1RC7CRC21T-3qcMFZo4...	437,462	1NXE4 檔案	2020/9/12 上午 01:07:13
.M3dIv42hvnCngopavNn3vUIfga7Pvn-3gvC4vnCNggp5M...	407,691	1NXE4 檔案	2020/9/12 上午 01:07:13
.M39cN2pwC7C-mQUpl7C-0Q1RC7CRC21T-3qcMFZo4m...	337,970	1NXE4 檔案	2020/9/12 上午 01:07:13
.MC9dgopagv1egoQYvfiYggERvniRnFGt2EZQwieA4HWQ...	257,743	1NXE4 檔案	2020/9/12 上午 01:07:13
.SI9cgLxNgRImgUxYgr7Egv7bgopYvn-3gvC4vnUJggp5gf...	256,666	1NXE4 檔案	2020/9/12 上午 01:07:13
.SC9cg-7JgaiRgUxYgr7Egv7bgopYg4CbvnUzvniR4myZaC...	213,399	1NXE4 檔案	2020/9/12 上午 01:07:12
.M39YN2pyo1pv_7CNl7A5X2CI0QC-0Q1RC7CRC21T-3qc...	182,704	1NXE4 檔案	2020/9/12 上午 01:07:13
.M399N2UTQ2p_Q2C-0Q1RC7CRC21T-3qcMFZo4myZaC...	174,377	1NXE4 檔案	2020/9/12 上午 01:07:13
.MC93vUIfga7PgUxYgr7Egv7bgopYg4CbvnUzvniR4myZa...	166,506	1NXE4 檔案	2020/9/12 上午 01:07:12
.MC9Kg-7JvfIcgUxYgr7Egv7bgopYvnUJgf-FvniRnFGt2EZQ...	166,428	1NXE4 檔案	2020/9/12 上午 01:07:13
.M393N2C401C-mQC-0Q1RC7CRC21T-3qcMFZo4myZaC...	159,755	1NXE4 檔案	2020/9/12 上午 01:07:13
.ME93MObgvn-3gvC4vnCNggp5vflUvfi2gfp0goUh4myZa...	156,402	1NXE4 檔案	2020/9/12 上午 01:07:12

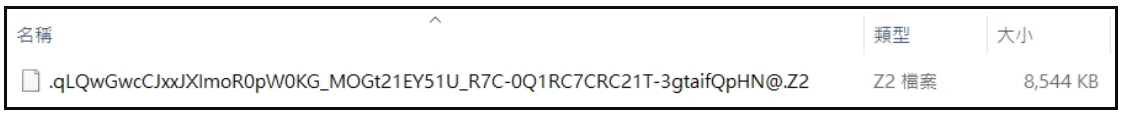
2. 查看勒索通知信內容，駭客告訴學校 QNAP NAS 內的檔案已被加密，如要解密需支付比特幣，取得支付贖金的資訊需以 CCPS-NAS 為主旨寫信至 smoky@mail.uk。若駭客在 24 小時內沒有回信，請學校安裝 Tor 洋蔥瀏覽器，到駭客所提供網址取得聯絡駭客的方式。在信中也提到駭客可以免費幫助學校解開 5 個小於 4Mb 的檔案，也告訴學校如何購買比特幣。



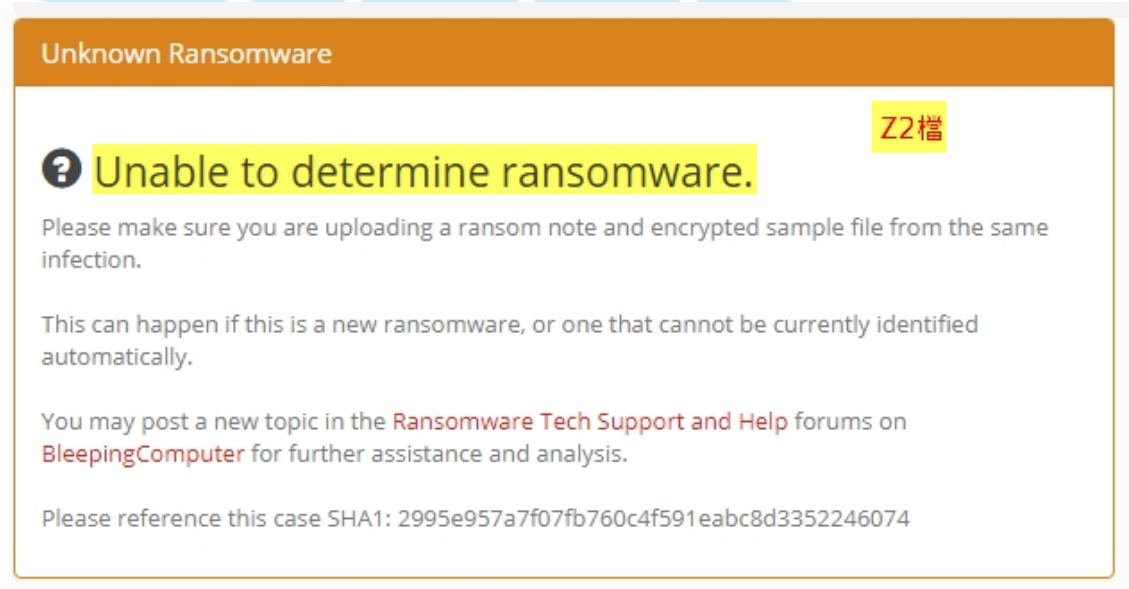
3. 安裝 Tor 瀏覽器開啟駭客所提供網址後，可看到寫信聯絡駭客的 E-mail 信箱與信件主旨 CCPS-NAS 的資訊。在此事件中駭客並未直接提供贖金資訊給受害者，而信件主旨 CCPS-NAS 會告訴駭客被勒索軟體加密的設備為 NAS。



4. 將學校所提供的勒索通知信與被加密的兩種檔案(1NXE4 檔案與 Z2 檔案)送至 ID Ransomware (https://id-ransomware.malwarehunterteam.com/)進行勒索病毒種類的判定。

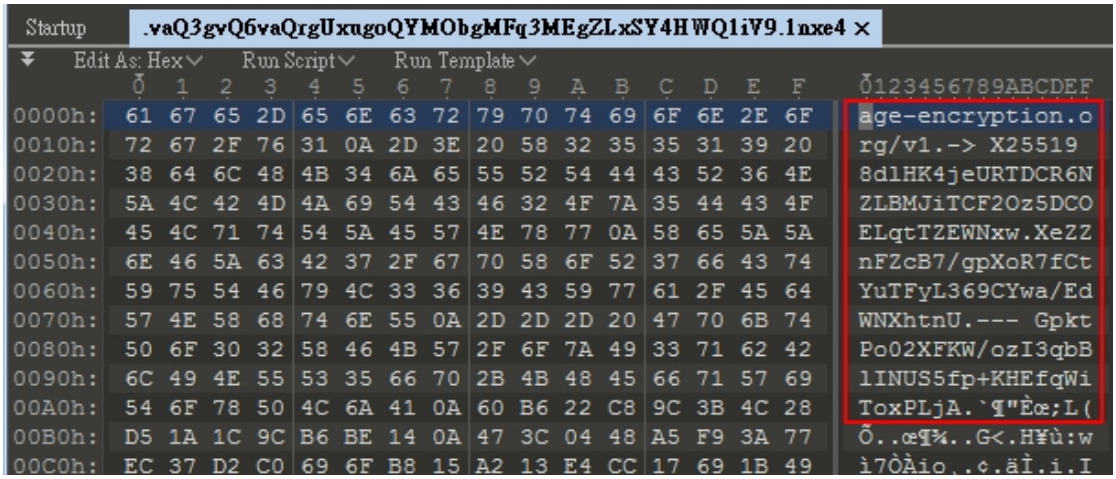


勒索通知信與副檔名 1nxe4 檔案檢測結果判定為 AgeLocker 勒索病毒，而副檔名 Z2 檔案則無法檢測出其勒索病毒的類型。檢測結果也告知目前勒索病毒 AgeLocker 尚未有解密器產生，故無法將被加密的檔案解密。

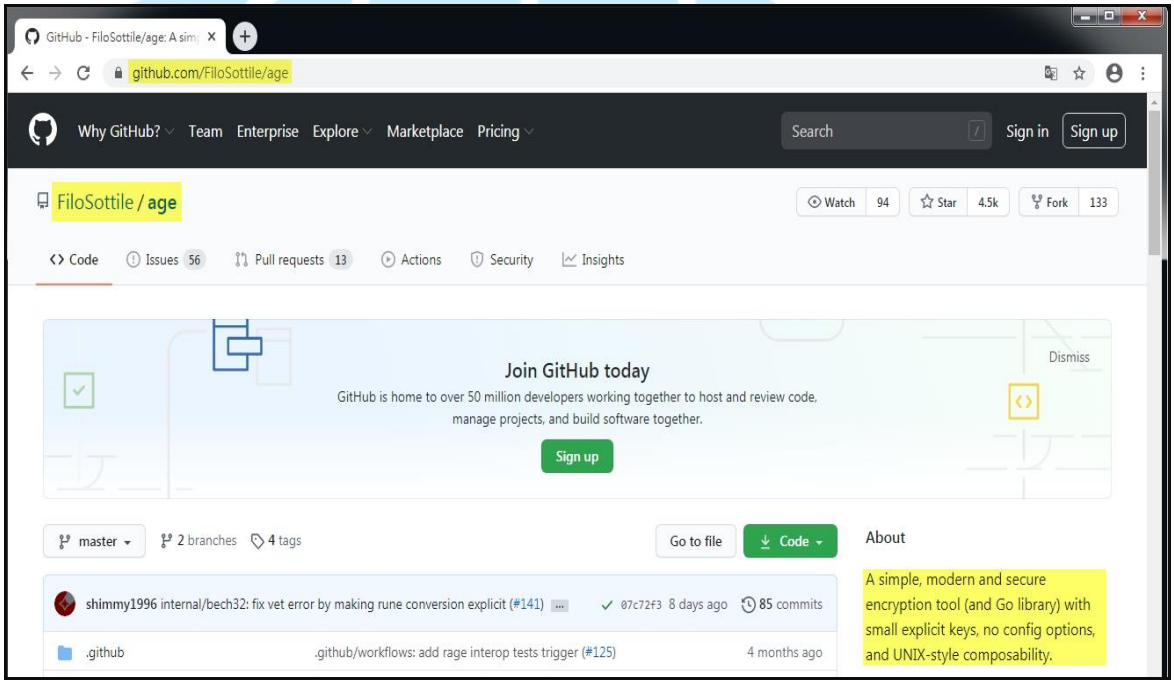


5. 檢視學校所提供的 1nxe4 檔案發現文字標題以 URL:「age-encryption.org」開始。文字標題內容如下:

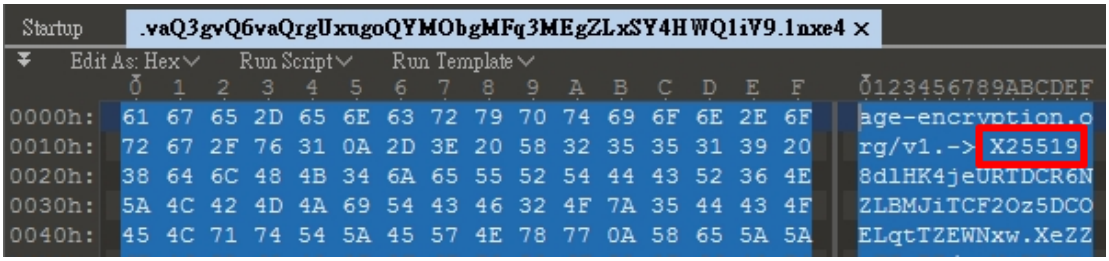
```
age-encryption.org/v1.-> X25519
8d1HK4jeURTDCR6NZLBMJiTCF2Oz5DCOELqtTZEWNxw.XeZZnFZcB7/
gpXoR7fCtYuTFyL369CYwa/EdWNXhtnU.--- GpktPo02XFKW/
ozI3qbBlINUS5fp+KHEfqWiToxPLjA
```



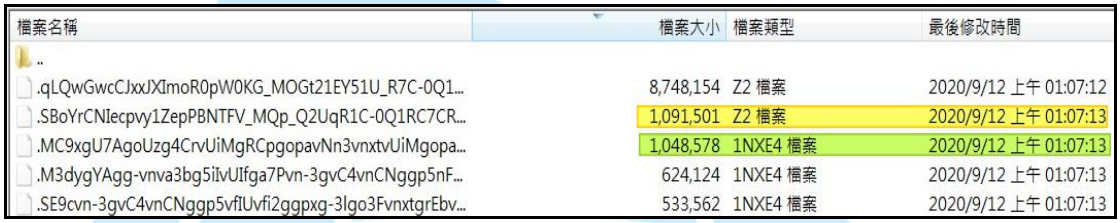
6. 透過瀏覽器連線 age-encryption.org 會發現在 GitHub (網址: github.com/FiloSottile/age)上有一個叫 Age 的介紹網頁。Age 這個檔案加密工具是由密碼學家 Filippo Valsorda 所創與開發。



7. 由文件標題內容可以看到 1nxe4 檔案使用 X25519 的加密法，而勒索軟體解密專家 Michael Gillespie 曾經研究 Age 後提出「Age 使用 X25519、ChaChar20-Poly1305 和 HMAC-SHA256 等三種加密演算法」。由此可知該檔案是感染 AgeLocker 勒索病毒無誤。



8. NAS 內有些檔案被加密成 Z2 檔案，由於勒索通知信僅產生一封，故推測不可能同一時間執行兩種勒索病毒。又加密工具 Age 的加密演算法有三種，加上 Z2 檔案的加密時間與 1nxe4 檔案幾乎同時，故推測會造成此現象有可能勒索病毒 AgeLocker 有設定達到某種條件時則使用某一種的加密演算法。



9. 根據 NAS 管理者所述，經檢視 NAS 的 Log 紀錄發現事件發生時間點的紀錄不存在，故無法透過 Log 紀錄追蹤該時段連線 NAS 的 IP 資訊，推測此 Log 紀錄被刪除疑似駭客為抹除自己的足跡所為。

三、事件攻擊行為示意圖

1. 駭客從 NAS 的 WEB 介面駭入 NAS。
2. 執行勒索病毒 AgeLocker 來加密檔案。
3. 檔案加密完成後，駭客在登出 NAS 前刪除 NAS 的 Log 紀錄來消滅自己的登入 IP 資訊。

四、總結與建議

1. 在 2020/7 BLEEPINGCOMPUTER 網路安全專家報導新的勒索病毒 AgeLocker 使用 Googler 員工所寫的 Age 加密工具來加密受害者的檔案。
2. 設計 AgeLocker 的駭客未使用傳統常用的加密演算法(如 AES+RSA)來加密檔案，而是使用 Age 這種命令列工具來加密檔案。Age 作為一個合法的檔案加密工具，不曾想會被當作勒索病毒的加密工具。
3. 本事件發生在 2020/09/12 凌晨駭客駭入 NAS 執行勒索病毒，導致 NAS 內的檔案被加密且加密後被隱藏，而受害者只看到勒索通知信的資訊，容易造成受害者的恐慌。
4. 本次事件學校所使用的 NAS 開放校內外任意 IP 連線存取 NAS 內檔案，未進行連線來源 IP 的控管，降低駭客攻擊的困難度。
5. 該 NAS 設備讓資料夾如同網路磁碟機一般掛載於教師所用主機內，當教師主機感染病毒時，則 NAS 資料夾感染病毒的風險升高。
6. 本次事件學校所使用的 NAS 廠牌 QNAP 在 2020/6 有資安新聞報導勒索軟體以 QNAP 的 NAS 裝置為攻擊目標，而在 2020/7 Help Net Security 報導 62000 台 QNAP NAS 裝置感染勒索病毒 QSnatch，建議使用者定期更新與修補 QNAP NAS 設備的漏洞，以降低被駭客駭入的風險。
7. 透過 NAS 設備來存取檔案雖然方便，但一旦感染勒索病毒則解密檔案的機率很低，因此建議使用者定期異地備份 NAS 內重要的資料。
8. 勒索病毒 AgeLocker 目前尚未有解密器產生，對於已被加密的重要檔案建議使用者可備份檔案，以待未來有解密器產生時進行解密。
9. 針對 NAS 設備的管理與安全防護建議如下:

   (1) 定期更新 NAS 的應用軟體與韌體。

   (2) 加強管理者的密碼強度。

(3) 啟用網路存取的保護機制來避免帳號被暴力攻擊。

(4) 若無使用 SSH 與 Telnet 服務的需求建議停用這些服務。

(5) 在存取 Web 平台方面避免使用預設的 port (如 443port 或 8080port)。

(6) 若 NAS 有快照功能可啟用它進行資料備份。

(7) 如非必要盡量避免掛載 NAS 資料夾於使用者主機上。

(8) 對於連線 NAS 的來源 IP 進行控管。