RansomHub：源自於 Knight 的新型勒索軟體

2024 年 6 月 5 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

新的運作方式已迅速發展成為最多產的勒索軟體威脅之一

RansomHub 是一種新的勒索軟體即服務 (RaaS)，它已迅速成為目前最大的勒索軟體集團之一，很有可能是舊版「Knight 」勒索軟體的更新和重命名版本。

博通公司旗下的賽門鐵克公司對 RansomHub 有效載荷的分析表明，這兩種威脅具有高度的相似性，說明 RansomHub 是源自於「Knight 」。

儘管有共同的起源，但「Knight」的建立者現在不太可能經營 RansomHub。因為在 2024 年 2 月 Knight 的開發者決定關閉其業務後，Knight(原名 Cyclops) 的原始碼已在地下論壇上出售。可能是其他行為者購買 Knight 的原始碼，並在推出 RansomHub 之前對其進行更新。

RansomHub 和 Knight 的比較

這兩種有效載荷都是用 Go 語言編寫，每個系列大多數變種都使用 Gobfuscate 進行混淆處理。只有 Knight 的某些早期版本未進行混淆處理。

這兩個系列的程式碼重疊程度很高，因此很難區分它們。在許多情況下，只能透過檢查嵌入到資料外洩網站的連結來確認。

這兩個系列的命令列幫助選單幾乎完全相同。唯一的區別是 RansomHub 增加睡眠命令。

```
C:\malware\knight_VT>36e5be.exe --help
USAGE: 36e5be.exe [OPTIONS]
OPTIONS:
  -disable-net
        Disable network before running
  -host value
        Only process smb hosts inside defined host. -host //10.10.10.10/ -host //10.10.10.11/
  -only-local
        Only encrypt local disks
  -pass string
        Pass
  -path value
        Only process files inside defined path. -path C:// -path D:// -path//10.10.10.10/d/
  -safeboot
        Reboot in Safe Mode before running
  -safeboot-instance
        Run as Safe Mode instance
  -verbose
        Log to console

C:\malware\knight_VT>
```

圖 1. Knight 命令列幫助選單

```
C:\malware\Primary_sample>ransomhub.exe --help
USAGE: ransomhub.exe [OPTIONS]
OPTIONS:
  -disable-net
        disable network before running
  -host value
        only process smb hosts inside defined host. -host 10.10.10.10 -host 10.10.10.11
  -only-local
        only encrypt local disks
  -pass string
        Pass
  -path value
        only process files inside defined path. -path C:// -path D:// -path //10.10.10.10/d/
  -safeboot
        reboot in Safe Mode before running
  -safeboot-instance
        run as Safe Mode instance
  -sleep int
        sleep for a period of time to run (minute)
  -verbose
        log to console

C:\malware\Primary_sample>
```

圖 2. RansomHub 命令列幫助選單

這兩種威脅都採用獨特的混淆技術，即每個重要字串都用唯一密鑰編碼，並在運行時解碼。例如：在『cmd.exe /c iisreset.exe /stop』指令中，只有 iisrest.exe 字串使用唯一金鑰加密。

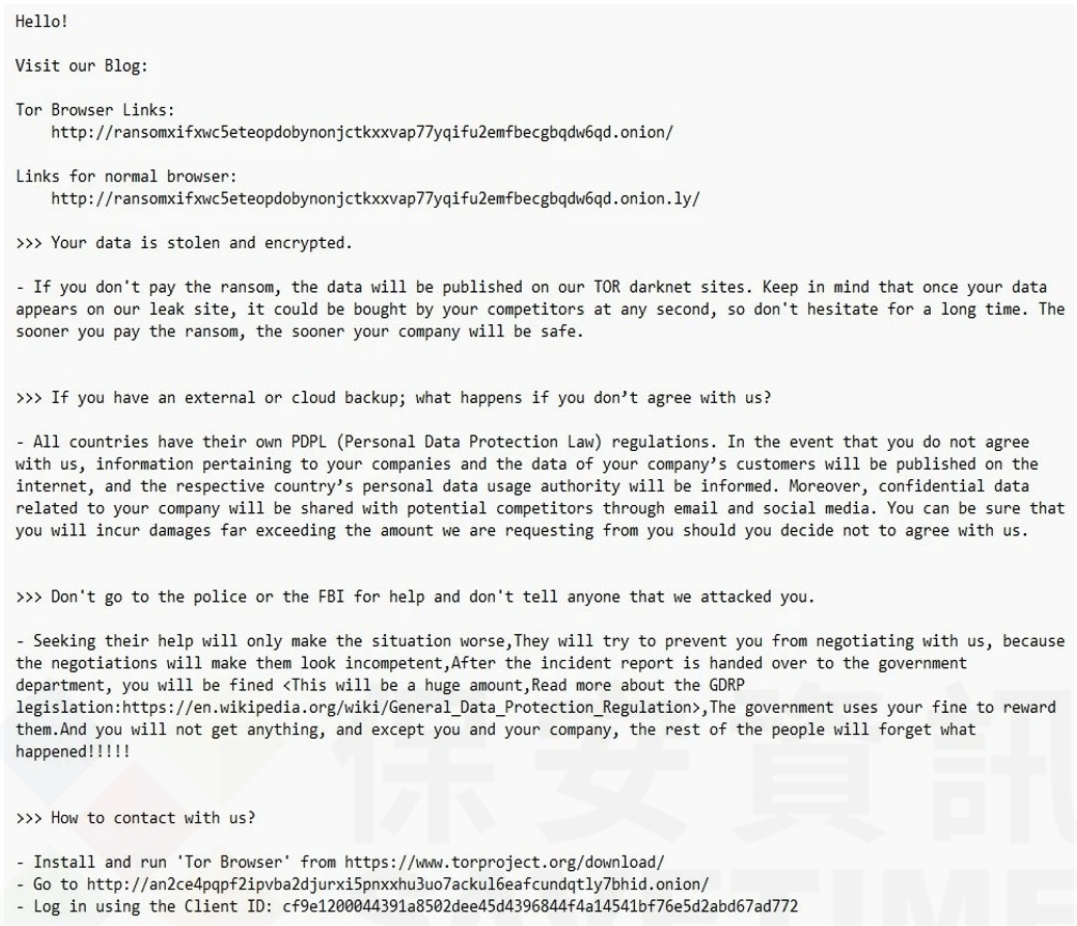
```
string_key = 0xeb1ebdaf401f7dab;
local_48 = 0x22cb4c2a;
iisreset.exe = 0x8947b6b63254ecbe;
local_3c = 0x43ad1904;
for (i = 0; i < 0xc; i = i + 1) {
  *(&iisreset.exe + i) = *(&string_key + i) + *(&iisreset.exe + i);
}
runtime::runtime.slicebytetostring(0x0,&iisreset.exe,0xc);
/c_/stop._8_8_ = 2;
/c_/stop._0_8_ = &/c;
local_18._8_8_ = 5;
local_18._0_8_ = &/stop;
FUN_0054b9c0(&cmd.exe,7,/c_/stop,3,3);
FUN_0054cd40(CONCAT17(in_stack_ffffffffffffff88,0x5aa6));
```

圖 3. RansomHub 字串編碼。只有 iisrest.exe 字串使用唯一金鑰加密

這兩種有效載荷留下的贖金說明有很明顯相似之處，Knight 使用的許多詞語都逐字出現在 RansomHub 說明中，這表明開發者只是對原始說明進行編輯和更新。

```
>> What happens?
 Your data is stolen and encrypted.If you don't pay the ransom, the data will be published on our
blog(http://knight3xppu263m7g4ag3xlit2qxpryjwueobh7vjdc3zrscqlfu3pqd.onion). Keep in mind that once
your data appears on our blog, it could be bought by your competitors at any second, so don't
hesitate for a long time.
>> How to contact with us?
  1. Download and install TOR Browser (https://www.torproject.org/).[If you don't know that, Google
search!]
  2. Open
http://f3r6nz2bopxnotodfcp4qztpr3mmapnkioa3ho7j2cuovb32nlf3zcyd.onion/621d81ec62c879476a39fb0bde573
5ce7c95e59d562bdcf2e48b9dd90a4a3d1fa6dae6e1d655248cd12d6ba66f5b5a15/
>>> Warning! Recovery recommendations.
 Do not MODIFY or REPAIR your files, Or they will be lost forever.
 Do not hire a recovery company.Can't solve anything without us,They always think they're expert
negotiators, but the truth is they don't care about you and business
 Do not report to the Police, FBI,They don't care about your business and it's going to get
worse.(You could be hit with a hefty fine.)
```

圖 4. Knight 的勒索說明



```
Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data
appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The
sooner you pay the ransom, the sooner your company will be safe.


>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree
with us, information pertaining to your companies and the data of your company's customers will be published on the
internet, and the respective country's personal data usage authority will be informed. Moreover, confidential data
related to your company will be shared with potential competitors through email and social media. You can be sure that
you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.


>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because
the negotiations will make them look incompetent,After the incident report is handed over to the government
department, you will be fined <This will be a huge amount,Read more about the GDRP
legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward
them.And you will not get anything, and except you and your company, the rest of the people will forget what
happened!!!!!


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID: cf9e1200044391a8502dee45d4396844f4a14541bf76e5d2abd67ad772
```

圖 5. RansomHub 的勒索說明

這兩個勒索軟體家族主要區別之一是透過 cmd.exe 運行的命令。這些命令可以在建置有效載荷時設定，也可以在配置過程中設定。雖然命令本身不同，但它們相對於其他操作的呼叫方式和順序是相同的。

Knight 和 RansomHub 的一個獨特功能是能夠在開始加密前以安全模式重新啟動端點。Snatch 勒索軟體曾在 2019 年使用過這種技術，它允許加密不受作業系統或其他安全程序的阻礙。Snatch 也是使用 Go 語言編寫，有許多類似功能，這表明它可能是開發 Knight 和 RansomHub 原始程式碼的另一個分支。不過，Snatch 與它們有很大不同，包括明顯缺乏可設定命令或任何混淆。

另一個在加密前以安全模式重新啟動受影響電腦的勒索軟體家族是 Noberus ，有趣的是，該加密程式將其配置儲存在一個 JSON 中，其中關鍵字與 RansomHub 中觀察到的一致。

RansomHub 攻擊

在賽門鐵克最近調查 RansomHub 攻擊中，攻擊者利用 Zerologon 漏洞 (CVE-2020-1472) 獲得初始存取權限，該漏洞可讓攻擊者獲得網域管理員權限並控制整個網域。

在部署勒索軟體之前，攻擊者使用幾種兩用工具。Atera 和 Splashtop 被用於促使遠端存取，

而 NetScan 則被用於發現和檢索網路設備資訊。RansomHub 酬載利用 iisreset.exe 和 iisrstas.exe 命令列工具來停止所有網際網路資訊服務 (IIS)。

迅速成長

儘管 RansomHub 在 2024 年 2 月才首次出現，但它的發展速度非常快，在過去三個月中，就公開宣稱攻擊次數而言，它是第四大最多產的勒索軟體運營商。該組織上週聲稱對英國 Christies 拍賣行所遭受的攻擊負責。

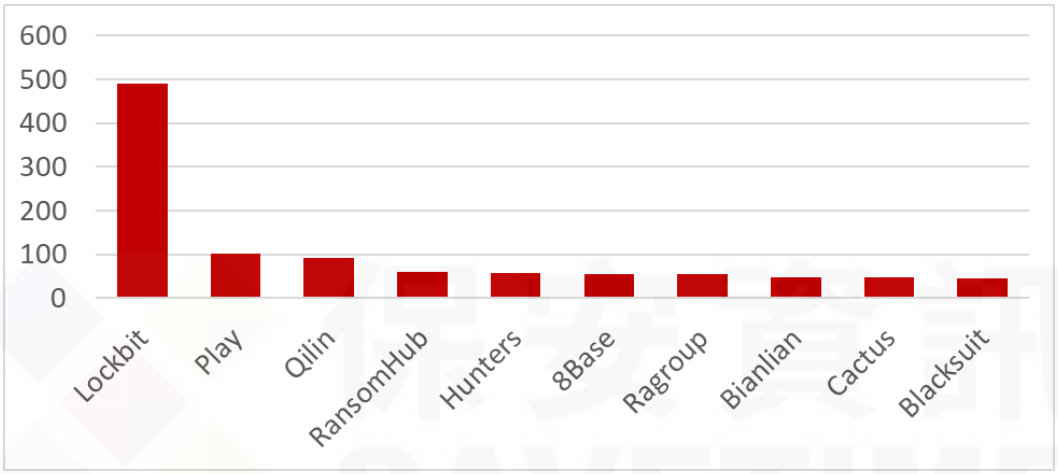


圖 6. 2023 年 3 月至 5 月依照聲稱攻擊次數統計的勒索軟體營運商

促進 RansomHub 成長的一個因素可能是該組織成功吸引 Noberus(又名 ALPHV、Blackcat) 勒索軟體組織的一些大型前附屬機構，該組織已於今年稍早關閉。據報道，一個名為『Notchy』的前 Noberus 附屬機構現在正在與 RansomHub 合作。除此之外，在最近一次 RansomHub 攻擊中，還使用以前與另一個名為 Scattered Spider 的 Noberus 附屬機構有關的工具。

RansomHub 建立業務的速度表明，該組織可能由在地下網路中擁有經驗和人脈的資深操作員組成。

防護方案／緩解措施

有關 Alpha 最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292--RansomHub

34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087--RansomHub

7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a--RansomHub

8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7--RansomHub

ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00--RansomHub

104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2--Knight

2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad--Knight

36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e--Knight

595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb--Knight

7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2--Knight

e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23--Knight

fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e--NetScan

f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3--Splashtop

a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2--Atera

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/6

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。