

# PhishStrike Lab(郵件)

身為教育機構的網路安全分析師，您收到一封針對教職員的網路釣魚郵件警報。該郵件看似來自一位可信任聯絡人，聲稱購買了一筆價值 62.5 萬美元的商品，並提供了下載發票的連結。

您的任務是使用威脅情報工具調查該郵件。分析郵件標題並檢查連結中是否有惡意內容。識別任何入侵指標 (IOC) 並記錄您的發現，以防止潛在的詐欺行為，並幫助教職員工識別網路釣魚。

使用工具：<https://eml-analyzer.herokuapp.com/#/>

## 問題 1

使用特定的 SPF 和 DKIM 值識別寄件者的 IP 位址有助於追蹤釣魚郵件的來源。SPF 值為softfail且 DKIM 值為fail的寄件者 IP 位址為何？

**EML分析器** 家 快取 API GitHub

快取 電子郵件回覆 VirusTotal 調查 url

7 2603:10b6:a03:3d2::9 · ds7pr01mb7855.prod.exchangelabs.com https  
sj0pr01mb7512.prod.exchangelabs.com

安全標頭

身份驗證結果

spf=softfail ( 寄件者 IP 為 18.208.22.104 ) smtp.mailfrom=uptc.edu.co; dkim=fail ( 無簽署金鑰 )  
header.d=uptc.edu.co;dmARC=none action=none header.from=uptc.edu.co;dmARC=none action=none  
header.from=up

18.208.22.104

## 第二季

了解電子郵件的返回路徑對於追蹤其來源至關重要。這封電子郵件中指定的返回路徑是什麼？

19gIK9J0Q+C+eZD00HjaAELlyneOV07712uIFwLnqC  
j/CWX+lwFDa7BshiFOZK9wzuNbOwPt1oqhV7hOwK/c

回程  
路徑

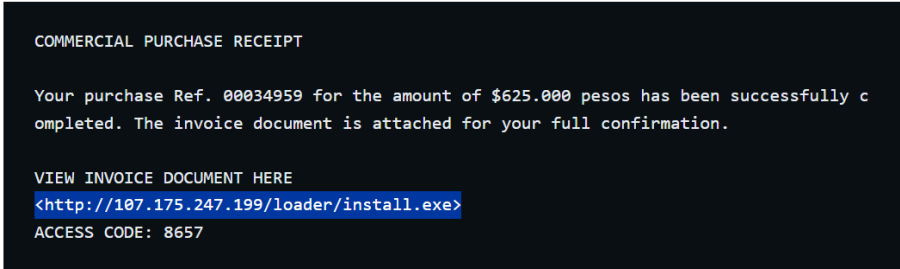
erikajohana.lopez@uptc.edu.co

erikajohana.lopez@uptc.edu.co

## 第三季

識別惡意軟體的來源對於有效緩解和應對威脅至關重要。託管與惡意軟體傳播相關的惡意檔案的伺服器的 IP 位址是什麼？

內容



107.175.247.199

第四季

識別利用系統資源進行加密貨幣挖礦的惡意軟體，對於確定威脅緩解工作的優先順序至關重要。惡意 URL 可以傳播多種惡意軟體類型。哪個惡意軟體家族負責加密貨幣挖礦？

2022年10月22日 12:39:04

http://107.175.247.199/loader/install.exe

離線

異步RAT

比特幣特

CoinMiner

abuse\_ch

URLhaus

from ABUSE<sup>ch</sup> | SPAMHAUS

🔍 Browse

🔔 Hunting Alerts

🗄 Access

ID:	2381718
URL:	🔗 http://107.175.247.199/loader/install.exe
URL Status:	Offline
Host:	🔗 107.175.247.199
Date added:	2022-10-22 12:39:04 UTC
Last online:	2022-12-12 07:XX:XX UTC
Threat:	🚫 Malware download
Reporter:	abuse_ch
Abuse complaint sent (?):	📧 Yes (2022-10-22 12:40:12 UTC to abuse{at}hudsonvalleyhost{dot}com)
Takedown time:	1 month, 20 days, 18 hours, 19 minutes ⓘ (down since 2022-12-12 07:00:08 UTC)
Tags:	AsyncRAT bitrat CoinMiner

CoinMiner

問5

識別惡意軟體請求的具體 URL 是破壞其通訊管道並降低其影響的關鍵。根據先前對加密貨幣惡意軟體樣本的分析，該惡意軟體請求的 URL 是什麼？

URLhaus

from ABUSE.ch | SPAMHAUS

🔍 瀏覽

🐾 狩獵警報

💾 存取數據

🗨 常問問題

📄 關於

🚪 登出

上次在線:	2022-12-12 07:XX:XX UTC
威脅:	☹️ 惡意軟體下載
記者:	📧 abuse_ch
已發送濫用投訴 ( ? ):	📧 是 ( 2022-10-22 12:40:12 UTC 發送至 abuse(at)hudsonvalleyhost(dot)com )
刪除時間:	1 個月 20 天 18 小時 19 分鐘🕒 ( 自 2022 年 12 月 12 日 07:00:08 UTC 以來 )
標籤:	🚫 異步RAT 🚫 比特幣特 🚫 CoinMiner

有效載荷交付

下表記錄了 URLhaus 從該特定 URL 檢索到的所有有效負載。

首次亮相	檔案名稱	文件類型	酬載 ( SHA256 )	室性心搏過速	市場	簽名
2022年10月26日	無	EXE文件	🔗 bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539	無	📧	BitRAT
2022年10月25日	無	EXE文件	🔗 5ca468704e7ccb8e1b37c0f7595c54df4e2f4035345b6e442e8bd4e11c58f791	無	📧	異步RAT
2022年10月22日	無	EXE文件	🔗 453fb1c4b3b48361fa8a67dcedf1eaec39449cb5a146a7770c63d1dc0d7562f0	無	📧	CoinMiner

🔍 453fb1c4b3b48361fa8a67dcedf1eaec39449cb5a146a7770c63d1dc0d7562f0

56 / 72

Community Score

🕒 56/72 security vendors flagged this file as malicious

453fb1c4b3b48361fa8a67dcedf1eaec39449cb5a146a7770c63d1dc0d7562f0

Size

192.50 KB

install.exe

🟢 peexe 🔴 detect-debug-environment 🔴 checks-network-adapters 🔴 direct-cpu-clock-access 🔴 shellcode 🔴 spreader 🔴 asser

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 9

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Contacted URLs (2) 🕒

Scanned	Detections	Status	URL
2025-04-08	11 / 97	-	http://ripley.studio/loader/uploads/Qanjttrbv.jpeg

http://ripley.studio/loader/uploads/Qanjttrbv.jpeg

問6


了解惡意軟體新增至自動執行鍵的登錄項目對於識別其持久性機制至關重要。根據對BitRAT惡意軟體樣本的分析，添加到註冊表自動運行鍵的第一個值中的可執行檔名稱是什麼？

上次在線：	2022-12-12 07:XX:XX UTC
威脅：	✖️ 惡意軟體下載
記者：	abuse_ch
已發送濫用投訴 ( ? )：	✉️ 是 ( 2022-10-22 12:40:12 UTC 發送至 abuse(at)hudsonvalleyhost[dot]com )
刪除時間：	1 個月 20 天 18 小時 19 分鐘⌚ ( 自 2022 年 12 月 12 日 07:00:08 UTC 以來 )
標籤：	異步RAT 比特幣特 CoinMiner

## 有效載荷交付

下表記錄了 URLhaus 從該特定 URL 檢索到的所有有效負載。

首次亮相	檔案名稱	文件類型	酬載 ( SHA256 )	室性心搏過速	市場	簽名
2022年10月26日	無	EXE文件	🔗 bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539	無	📄	BitRAT



### Names ⓘ

- install.exe
- bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539.exe
- unknown
- xSzQcEkCtN
- Jzwvix.exe

Jzwvix.exe

### 問7

識別從惡意 URL 下載的檔案的 SHA-256 雜湊值對於追蹤和分析惡意軟體活動至關重要。根據BitRAT分析，先前下載並新增到自動執行金鑰中的檔案的 SHA-256 雜湊值是多少？

如前面題目：`bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539`

### 問8

分析惡意軟體發出的 HTTP 請求有助於識別其通訊模式。載入程式用來檢索 BitRAT 惡意軟體的 HTTP 請求中的 URL 是什麼？

bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539

Score

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate

Contacted URLs (2)

Scanned	Detections	Status	URL
2022-11-01	15 / 90	200	http://ripley.studio/loader/uploads/Hjvnp.png
2025-01-23	9 / 96	200	http://107.175.247.199/loader/server.exe

http://107.175.247.199/loader/server.exe

問9

在惡意軟體執行過程中引入延遲有助於規避檢測機制。根據 BitRAT 分析，PowerShell 指令造成的延遲（以秒為單位）是多少？

使用網站：<https://tria.ge/221026-l8jr6afdel/behavioral2>

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

進程號：3696

「C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe」-enc UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==

UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==解碼

這串經過 Base64 編碼的字串為：

ini

複製編輯

UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==

解碼後為 UTF-16 Little Endian（Unicode 編碼），對應的原始字串是：

sql

複製編輯

Start-Sleep -Seconds 50

Start-Sleep -Seconds 50

Q10

追蹤惡意軟體使用的命令和控制 (C2) 網域對於偵測和阻止惡意活動至關重要。BitRAT 惡意軟體使用的 C2 域是什麼？

tria.ge/221026-l8jr6afdel/behavioral2

透 漏洞利用參考 反彈參考 Github 解碼 鑑識/SOC相關 AI 72 Discord 恆益課程 找工作

MAGE:WIN10V2004-20220812-EN

LOCALE:EN-US

WINDOWS10-2004-X64

SYSTEM

ed

022, 10:12 UTC

ing

Copy URL

Twitter

E-mail

gh9st.mywire.org:5000

Malware Config

Extracted

Family

bitrat

Version

1.38

C2

gh9st.mywire.org:5005

Attributes

communication\_password

803355ca422bf9b37bc523a750e21842

install\_dir

svcsvc

install\_file

svcsvc.exe

tor\_process

tor

問11

了解惡意軟體如何竊取資料對於偵測和預防資料外洩至關重要。根據AsyncRAT分析，該惡意軟體使用的 Telegram Bot ID 是什麼？

網站：<https://tria.ge/221025-mz5tpscdf8/behavioral2>

	得到	<a href="https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...">https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...</a>	34793C6520DC...	^
<p>遠端位址： 149.154.167.220:443</p> <p>要求 GET /bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offset=-5 HTTP/1.1 接受：*/ 接受編碼：gzip, deflate 用戶代理：Mozilla/4.0 ( 相容；MSIE 7.0；Windows 7.0； 6.2；WOW64；Trident/7.0；.NET4.0C；.NET4.0E；.NET CLR 2.0.50727；.NET CLR 3.0.30729；.NET CLR 3.5.30729) 主機：api.telegram.org 連線：保持活動活動。</p> <p>回覆 HTTP/1.1 200 正常 伺服器：nginx/1.18. 日期：2022 年 10 月 25 日星期二 10:57:21 GMT 內容類型：application/json 內容長度：23 連線：保持活動 嚴格傳輸安全：max-age=31536000；includeSubDomains；預先載入 存取控制允許來源：* 存取控制允許方法：GET、POST、OPTIONS 存取控制公開標頭：內容長度、內容類型、日期、伺服器、連線</p>				
	得到	<a href="https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...">https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...</a>	34793C6520DC...	▼
	得到	<a href="https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...">https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offs...</a>	34793C6520DC...	▼

bot5610920260