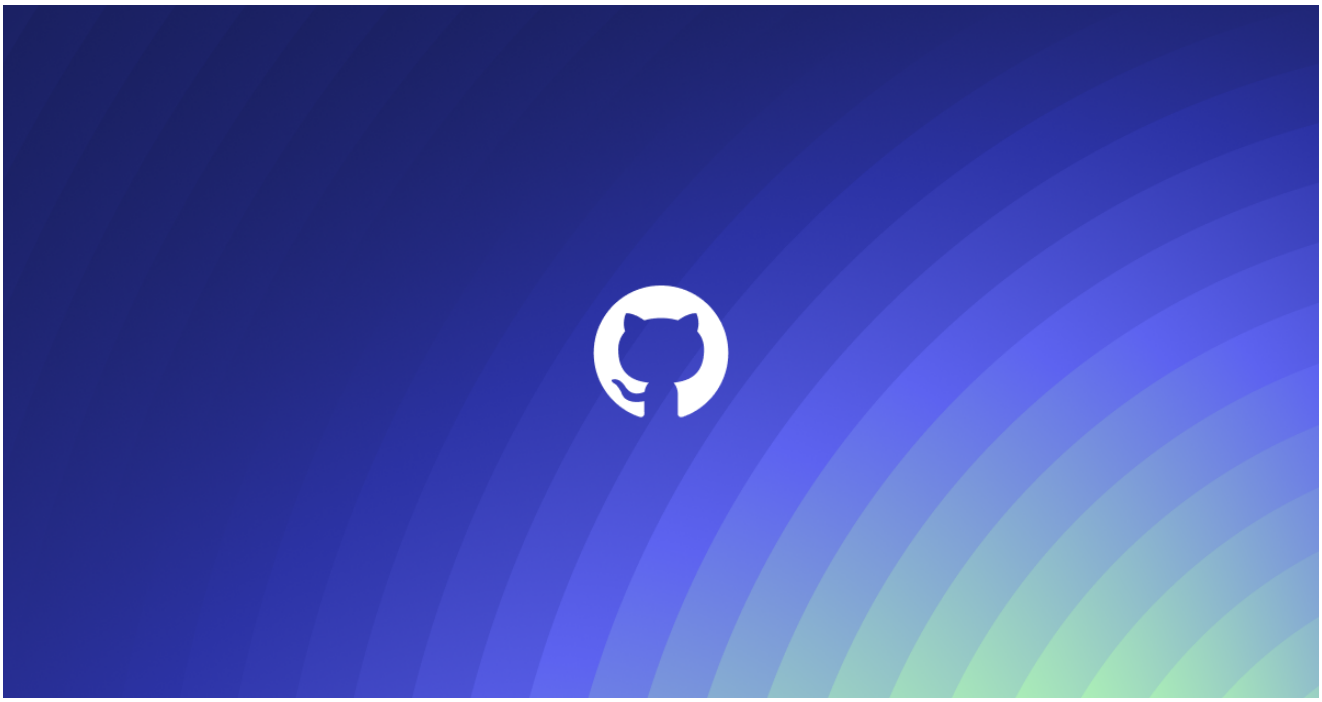
Security alert: social engineering campaign targets technology industry employees

github.blog/2023-07-18-security-alert-social-engineering-campaign-targets-technology-industry-employees

July 18, 2023



GitHub has identified a low-volume social engineering campaign that targets the personal accounts of employees of technology firms, using a combination of repository invitations and malicious npm package dependencies. Many of these targeted accounts are connected to the blockchain, cryptocurrency, or online gambling sectors. A few targets were also associated with the cybersecurity sector. No GitHub or npm systems were compromised in this campaign. We're publishing this blog post as a warning for our customers to prevent exploitation by this threat actor.

Threat actor profile

We assess with high confidence that this campaign is associated with a group operating in support of North Korean objectives, known as Jade Sleet by Microsoft Threat Intelligence and TraderTraitor by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Jade Sleet mostly targets users associated with cryptocurrency and other blockchain-related organizations, but also targets vendors used by those firms.

Attack chain

The attack chain operates as follows:

1. Jade Sleet impersonates a developer or recruiter by creating one or more fake persona accounts on GitHub and other social media providers. Thus far, we have identified fake personas that operated on LinkedIn, Slack, and Telegram. In some cases these are fake personas; in other cases, they use legitimate accounts that have been taken over by Jade Sleet. The actor may initiate contact on one platform and then attempt to move the conversation to another platform.
2. After establishing contact with a target, the threat actor invites the target to collaborate on a GitHub repository and convinces the target to clone and execute its contents. The GitHub repository may be public or private. The GitHub repository contains software that includes malicious npm dependencies. Some software themes used by the threat actor include media players and cryptocurrency trading tools.
3. The malicious npm packages act as first-stage malware that downloads and executes second-stage malware on the victim's machine. Domains used for the second-stage download are listed below.

The threat actor often publishes their malicious packages only when they extend a fraudulent repository invitation, minimizing the exposure of the new malicious package to scrutiny.

In some cases, the actor may deliver the malicious software directly on a messaging or file sharing platform, bypassing the repository invitation/clone step.

The mechanics of the first-stage malware are described in detail in a blog by Phylum Security.

Phylum's work, conducted completely independent of GitHub, mirrors our own research.

What GitHub is doing

- We have suspended npm and GitHub accounts associated with the campaign.
- We are publishing indicators below.
- We have filed abuse reports with domain hosts in cases where the domain was still available at time of detection.

What you can do

- If you were solicited, by anyone, to clone or download content associated with one of the accounts noted below, then you were targeted by this campaign.
- You can review your security log for `action:repo.add_member` events to determine if you ever accepted an invite to a repository from one of the accounts noted below.
- Be wary of social media solicitations to collaborate on or install npm packages or software that depends on them, particularly if you are associated with one of the targeted industry sectors listed above.

- Examine dependencies and installation scripts. Very recently published, net-new packages, or scripts or dependencies that make network connections during installation should receive extra scrutiny.
- If you were targeted by the campaign, we recommend you contact your employer's cybersecurity department.
- If you executed any content as a result of this campaign, it may be prudent to reset or wipe potentially affected devices, change account passwords, and rotate sensitive credentials/tokens stored on the potentially affected device.

Indicators

Domains

npmjscloud[.]com
npmrepos[.]com
cryptopriceoffer[.]com
tradingprice[.]net
npmjsregister[.]com
bi2price[.]com
npmaudit[.]com
coingeckoprice[.]com

Malicious npm packages

assets-graph
assets-table
audit-ejs
audit-vue
binance-prices
coingecko-prices
btc-web3
cache-react
cache-vue
chart-tablejs
chart-vxe
couchcache-audit
ejs-audit
elliptic-helper
elliptic-parser
eth-api-node
jpeg-metadata
other-web3

price-fetch
price-record
snykaudit-helper
sync-http-api
sync-https-api
tslib-react
tslib-util
ttf-metadata
vue-audit
vue-gws
vuewjs

Malicious GitHub accounts

GalaxyStarTeam
Cryptowares
Cryptoinnowise
netgolden

Malicious npm accounts

charlestom2023
eflodzumibreathbn
galaxystardev
garik.khasmatulin.76
hydsapprokoennl
leimudkegoraie3
leshakov-mikhail
linglidekili9g
mashulya.bakhromkina
mayvilkushiot
outmentsurehauw3
paupadanberk
pormokaiprevdz
podomarev.goga
teticseidiff51
toimanswotsuphous
ufbejishisol

External References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a
https://blog.phylum.io/sophisticated-ongoing-attack-discovered-on-npm/

Subscribe to The GitHub Insider

A newsletter for developers covering techniques, technical guides, and the latest product innovations coming from GitHub.