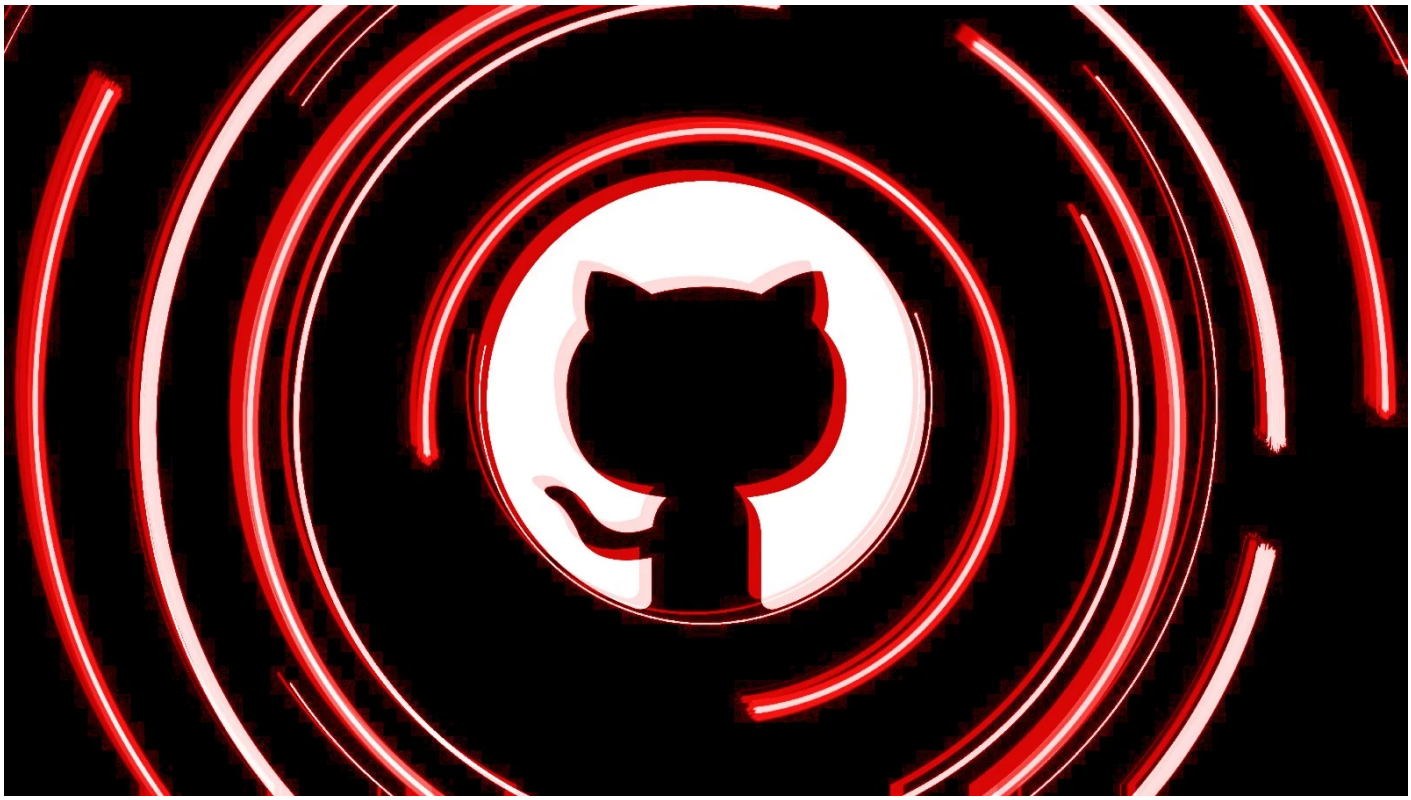
New Gitloker attacks wipe GitHub repos in extortion scheme

By **Sergiu Gatlan**

June 6, 2024 01:53 PM 1



Attackers are targeting GitHub repositories, wiping their contents, and asking the victims to reach out on Telegram for more information.

These attacks are part of what looks like an ongoing campaign first spotted on Wednesday by Germán Fernández, a security researcher at Chilean cybersecurity company CronUp.

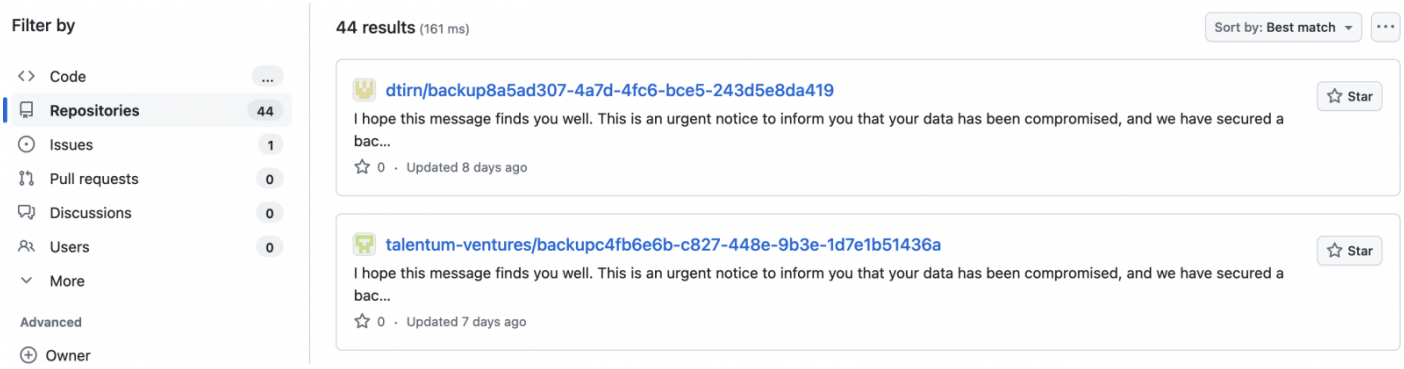
The threat actor behind this campaign—who has the Gitloker handle on Telegram and is posing as a cyber incident analyst—is likely compromising targets' GitHub accounts using stolen credentials.

Subsequently, they claim to steal the victims' data, creating a backup that could help restore the deleted data. They then rename the repository and add a single README.me

file, instructing the victims to reach out on Telegram.

"I hope this message finds you well. This is an urgent notice to inform you that your data has been compromised, and we have secured a backup," the ransom notes read.

When BleepingComputer contacted GitHub earlier today for more details regarding the Gitloker extortion campaign, a spokesperson was not immediately available for comment.



Dozens of GitHub repos already impacted (BleepingComputer)

After previous attacks against GitHub users, the company advised users to change their passwords to secure their accounts against unauthorized access. This should protect against malicious actions such as adding new SSH keys, authorizing new apps, or modifying team members.

To prevent attackers from compromising your GitHub account and detect suspicious activity, you should also:

- Enable two-factor authentication.
- Add a passkey for secure, passwordless login.
- Review and revoke unauthorized access to SSH keys, deploy keys, and authorized integrations.
- Verify all email addresses associated with your account.
- Review account security logs to track repository changes.
- Manage webhooks on your repositories.
- Check for and revoke any new deploy keys.
- Regularly review recent commits and collaborators for each repository.

Commonly targeted in data theft attacks

This isn't the first time GitHub accounts have been compromised to steal data from users' private repositories.

Around March 2020, hackers also compromised the account of Microsoft, the developer platform's parent company since June 2018, stealing more than 500GB worth of files from Redmond's private repositories.

While the stolen files contained mostly code samples, test projects, and other generic items (nothing significant for Microsoft to worry about), security experts were concerned that private API keys or passwords might have also accidentally been exposed in the breach.

A now-notorious threat actor known as ShinyHunters also confirmed the inconsequential nature of the stolen data by leaking it on a hacker forum for free after first planning to sell the stolen files to the highest bidder.

In September 2020, GitHub warned of a phishing campaign targeting users to compromise their accounts. The campaign used emails pushing fake CircleCI notifications to steal their GitHub credentials and two-factor authentication (2FA) codes by relaying them through reverse proxies.

GitHub said that the attackers almost immediately began exfiltrating data from victims' private repositories after the compromise, adding new user accounts to the organizations to maintain persistence if it used management permissions.

EXTORTION GITHUB GITLOKER RANSOM REPOSITORY

SERGIU GATLAN

Sergiu is a news reporter who has covered the latest cybersecurity and technology developments for over a decade. Email or Twitter DMs for tips.

PREVIOUS ARTICLE

NEXT ARTICLE

Comments

petteyg - 2 days ago

This is just stupid. Change your password, push your repository again, and be done with it. Surely you weren't doing something stupid like having nothing but shallow clones?