Guest Blog: Ox Security on learning from the Recent GitHub Extortion Campaigns

By The Gurus

Published: 2024-06-13 · Archived: 2026-04-05 14:34:31 UTC

A new threat actor group known as Gitloker has launched an alarming campaign that wipes victims' GitHub repositories and attempts to extort them. Victims are finding their repositories erased, replaced only by a solitary README file bearing the message: "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." This note is followed by instructions to contact the attackers via Telegram to negotiate the return of their data.

These attackers appear to be using the stolen GitHub credentials of users who have not enabled two-factor authentication (2FA). Over recent months, GitHub-related security incidents have increased. GitHub, along with GitLab and other popular development platforms, have increasingly become prime targets for threat actors, given the sensitivity of the data created and stored there. These platforms are exploited under the strategy known as LOTS (Living Off Trusted Sites), where attackers leverage the credibility of well-known sites to carry out their malicious activities.

Monitor Access Controls for Safer Dev Environments

These attacks are far from isolated events; they're part of a broader and troubling trend. Our data shows that between 93-97% of OX Security users have activated two-factor authentication (2FA), which helps keep accounts, data, and secrets private. But looking at 2FA use in isolation doesn't tell the whole story; according to the 2024 Verizon Data Breach Investigations Report (DBIR), 61% of breaches involve stolen credentials—including breaches on GitHub/GitLab and Bitbucket. While large businesses are more likely to deploy and require 2FA/MFA, data from the Cyber Readiness Institute shows that only 54% of SMBs do not implement MFA and only 28% of SMBs require it. This missing control leaves businesses' repositories vulnerable.

What's more, we know that breaches, especially those involving credentials, are increasing. The Gitlocker campaign is just one glaring example. And it shows that, when it comes to your code and your secrets, one set of compromised credentials could expose thousands (if not millions) of data points. One set of compromised credentials could lead to millions of lines of lost code, productivity, and competitive advantage.

This trend highlights a critical vulnerability within the software development community: the reliance on centralized systems that are often not sufficiently secured. These platforms are integral to developers' daily operations, making them prime targets for cyber adversaries. To counteract such threats, organizations must adopt a proactive approach to security, ensuring these essential systems are well-protected.

Understanding the New Attack Methods

The methods used in these scenarios are diverse and growing more complex, encompassing tactics from simple repository wipes to sophisticated extortion campaigns. Also, the frequency of these attacks is on the rise, which makes management and response efforts more challenging. Adversaries are consistently employing tried-and-true methods of social engineering to gain personal and professional information or manipulate individuals into granting access to sensitive systems.

The industry has recently witnessed a marked increase in “man-in-the-middle” attacks, in which attackers intercept and manipulate ongoing transactions and data transfers. Further, supply chain attacks are becoming more common, since a single compromised component can affect entire networks of dependencies. These incidents underscore the need for organizations to adopt a holistic and layered approach to security, emphasizing continuous monitoring, employee training, and the adoption of cutting-edge security technologies.

Backing Up Repository Data: Who’s Responsible?

When it comes to protecting GitHub data, it is crucial to understand who is responsible for creating backup. GitHub’s built-in features may not be adequate for restoring older versions, especially during major data loss incidents. It’s advisable for organizations to implement their own backup solutions that can capture daily snapshots of repositories and securely store them across multiple locations. This dual approach not only provides redundancy but also ensures that backups remain accessible even if the primary cloud service is compromised.

The decision between using GitHub’s backup capabilities and managing your own comes down to control, compliance, and risk management. Organizations, particularly those dealing with sensitive or regulatory-bound data, should consider third-party backups essential. The backup process can be automated and integrated into the development workflow, ensuring that even in the event of a breach, recovery will be swift and complete, minimizing downtime and loss while limiting cumbersome manual processes.

By understanding and implementing backup strategies, companies can protect themselves against the most catastrophic outcomes of cyber attacks, ensuring business continuity and safeguarding their valuable intellectual property.

Moving Forward

The reality is, GitHub-related attacks are evolving, but so are our methods to combat them. The Gitloker extortion campaign is a poignant reminder of the vulnerabilities inherent in relying on single-factor authentications and centralized systems. As attackers refine their strategies and broaden their targets, the potential damage from compromised credentials and data breaches could be devastating.

To effectively combat these threats, organizations must enforce stringent security protocols, including the widespread adoption of multi-factor authentication and regular audits of access controls. Additionally, the implementation of comprehensive backup solutions, continuous monitoring and access reviews are paramount to ensure that sensitive data remains protected across all fronts.
