Security Incident Analysis and Action Plan: Attack on the GitHub Repository "LukeStriderGM/BLOX-TAK-SERVER-IUCP"

Executive Summary

This analysis confirms that the observed activity is a deliberate and active attempt to impersonate (phishing/spoofing) the legitimate GitHub repository LukeStriderGM/BLOX-TAK-SERVER-IUCP. The attacker is using cloud infrastructure located in China, hosting a malicious copy of the site on a server with the IP address 175.178.70.242, which belongs to the provider Tencent Cloud. Particularly alarming is the fact that the malicious URL has been successfully indexed by the Google search engine, significantly increasing the risk of reaching unsuspecting users and amplifying the attack's reach.

The specific nature of the project, TAK Server (Team Awareness Kit), which is a tool used by uniformed services, government agencies, and crisis response teams, suggests that the attack is highly targeted and may aim to compromise systems of critical importance. This elevates the incident's significance beyond standard cybercrime. The recommended action plan comprises three key pillars: immediate reporting of the abuse to the hosting provider (Tencent Cloud) and to Google to remove the malicious content from public access; transparent communication with potential victims and the project community; and the implementation of long-term measures to strengthen the security of the project and its digital footprint.

1. Incident Analysis and Attack Vector

1.1. Attack Chain Reconstruction

An analysis of the provided evidence allows for the reconstruction of a multi-stage attack chain that exploits the trust in the GitHub platform and the popularity of the targeted project.

1. **Cloning and Spoofing:** The attacker created a website that visually and structurally mimics the GitHub repository page for LukeStriderGM/BLOX-TAK-SERVER-IUCP. The malicious URL, http://175.178.70.242:1111/LukeStriderGM/BLOX-TAK-SERVER-IUCP/, precisely imitates the path to the legitimate project to deceive the user.
2. **Hosting Malicious Content:** The fake page was placed on a server with the IP address 175.178.70.242. Access is provided via the non-standard port 1111. Using an unusual port may be a deliberate technique to evade basic security scanners and firewall rules that often monitor only standard traffic on ports 80 (HTTP) and 443 (HTTPS).
3. **Increasing Credibility and Reach (Discovery & Delivery):** A key element of the attack is the successful indexing of the malicious URL by the Google search engine [Image 3]. This step transforms a passively hosted page into an active and scalable attack vector. Users searching for information about the project via popular search engines may unknowingly land on the fake version, believing it to be authentic. This tactic is characteristic of "repo confusion" campaigns, where the trust in well-known platforms is used as a weapon against users.[1]
4. **Potential Goal Execution:** A user who lands on the malicious page is exposed to several threats. The attacker's goal is most likely to persuade the victim to download modified source code or a compiled application. Such code may contain hidden malware, such as remote access trojans (e.g., AsyncRAT, Quasar), info-stealers (e.g., LummaC2, RedLine Stealer) that steal credentials and data from browsers, or backdoors that allow the attacker to take control of the victim's system.[3] Alternatively, the page could be used for classic phishing, attempting to steal credentials for a GitHub account or other services.

1.2. Adversary Infrastructure Analysis

The infrastructure used in the attack has been identified and analyzed using OSINT (Open-Source Intelligence) tools.

- **IP Address:** 175.178.70.242
- **IP Reputation:** Security scanners, including those visible in the provided screenshots (VirusTotal, G-Data, Emsisoft), unequivocally flag this address as malicious, associated with phishing or other harmful activities [Image 1, Image 2].
- **Autonomous System (ASN):** 45090
- **ASN Owner:** Shenzhen Tencent Computer Systems Company Limited, operating as Tencent Cloud [Image 1].

An analysis of ASN 45090's reputation in public threat databases confirms that it is frequently abused for criminal purposes. The ThreatFox database contains numerous Indicators of Compromise (IOCs) from this ASN, associated with Command & Control (C2) servers for popular offensive tools like Cobalt Strike and GoPhish.[6] The CleanTalk service indicates that a significant percentage (nearly 8%) of IP addresses within this ASN exhibit spam activity.[7]

Choosing a large, global cloud provider like Tencent Cloud is a strategic decision by the attacker. It allows them to "hide in the crowd" of millions of legitimate services, making detection more difficult. Furthermore, the abuse reporting processes at such large operators can be more bureaucratic and slower, giving the attacker a valuable window of time to carry out the attack before the infrastructure is blocked. The notorious use of this ASN for hosting C2 servers suggests that the attacker may be part of a larger cybercrime ecosystem or is simply using ready-made, so-called "bulletproof" hosting solutions.[3]

1.3. Probable Attacker Goals and Motivations

The repository name, BLOX-TAK-SERVER-IUCP, indicates that the project is related to **TAK Server (Team Awareness Kit)** software. This is an advanced geospatial and communication platform, originally developed for the U.S. military and now widely used by armed forces, government agencies, emergency services, and crisis response teams worldwide.[8]

This context is crucial for understanding the attacker's motivation. Users and administrators of TAK systems are potentially high-value targets, and the data processed by these systems is extremely sensitive. Therefore, an attack on a repository providing tools for this community is far more serious than typical, mass-market phishing. Probable motivations include:

1. **Targeted Espionage:** The most likely scenario. The goal is to distribute a modified, malicious version of the TAK server that would allow the attacker to gain access to real-time operational data, such as personnel locations, communication content, mission plans, or sensor data. Compromising a TAK server could give the attacker "eyes and ears" inside the organization that uses it.
2. **Credential Theft:** The attack may be aimed at developers and administrators of TAK systems to steal their credentials, which could then be used for further, more advanced attacks.
3. **Software Supply Chain Attack:** The repository author, as a trusted source of software for a specific and sensitive community, has become a target. By compromising one source, the attacker hopes to reach many end targets.

The gravity of the incident shifts from the category of financial cybercrime towards a potential intelligence operation, possibly state-sponsored (APT) or conducted by a highly specialized criminal group.

1.4. Risk Assessment and Potential Impact

Based on the above analysis, the risk level associated with the incident is as follows:

- **Risk to End Users: Critical.** Downloading and running malicious software from the fake site could lead to the complete compromise of systems and networks, theft of highly sensitive operational data, and in extreme cases, even a threat to the physical safety of personnel relying on the TAK system.
- **Risk to the Author's and Project's Reputation: High.** Even if the original repository is 100% secure, the existence of a malicious clone can undermine trust in the project. Users may start to avoid it for fear of making a mistake, which would harm its development and adoption.
- **Risk to the GitHub Ecosystem: Medium.** This incident is part of a broader, disturbing trend of using trusted developer platforms to distribute malware and conduct phishing campaigns, which gradually erodes overall trust in the open-source ecosystem.[1]

The most significant factor amplifying the risk is the indexing of the malicious page by Google. This makes the attack passive, scalable, and does not require the attacker to actively distribute links. Victims find the malicious trap themselves. Therefore, it is crucial not only to block the server but also to "cleanse" the public information space—the search results—as quickly as possible.

2. Action Plan: Immediate Response and Damage Containment & Eradication Phase

The following plan outlines the precise steps to be taken to neutralize the immediate threat as quickly as possible. Actions should be carried out simultaneously on several fronts.

2.1. Reporting Abuse to the Hosting Service Provider (Tencent Cloud)

The goal is to have the IP address 175.178.70.242 immediately blocked or the malicious content removed by the infrastructure provider.

Procedure:

1. **Fill out the online form:** Use the official Tencent Cloud form for reporting illegal content: https://www.tencentcloud.com/report-platform/illegalcontentcomplaint.[11] In the form, precisely state the malicious URL, select the threat category (e.g., Phishing/Malware), and provide a detailed explanation of the situation in the description, attaching evidence (e.g., screenshots).
2. **Send a formal email report:** To increase the chances of a swift response, send a report directly to the departments responsible for security and compliance.
   - **Recipients:** compliance@tencent.com [12], cloud_sec@tencent.com [13]
   - **Suggested Subject:** URGENT: Phishing and Malware Hosting on Tencent Cloud Infrastructure (IP: 175.178.70.242, ASN: 45090)
   - **Suggested Content:** The message should include a detailed description of the incident, the full malicious URL, the IP address, a link to the original, legitimate GitHub repository, and an explanation that the target of the attack is specialized software (TAK Server) used by official services, which increases

the severity of the threat.

Contact Type	Address / Link	Source	Notes
Online Form	https://www.tencentcloud.com/report-platform/illegalcontentcomplaint	[11]	The primary and official reporting method.
Email (Security)	cloud_sec@tencent.com	[13]	Direct contact for the cloud security team.
Email (Compliance)	compliance@tencent.com	[12]	Contact for the department responsible for legal and policy compliance.

2.2. Reporting the Malicious URL to Google Safe Browsing and Removal from Search Results

The goal is to flag the malicious page as unsafe in popular web browsers (which use Safe Browsing lists) and to have it removed from the Google search index.

Procedure:

1. **Report Phishing:** Use the dedicated Google Safe Browsing form: https://safebrowsing.google.com/safebrowsing/report_phish/.[14] This is the fastest way to have the site marked as phishing.
2. **Report Malware:** Since the site may be distributing malicious software, it should also be reported using the malware reporting form: https://safebrowsing.google.com/safebrowsing/report_badware/.[15]
3. **Report Search Result Spam:** To inform Google's algorithms of the attempt to manipulate rankings, you can additionally report the page as spam in the search results.[16]

Reporting Goal	Form Link	Source
Report Phishing	https://safebrowsing.google.com/safebrowsing/report_phish/	[14]
Report Malware	https://safebrowsing.google.com/safebrowsing/report_badware/	[15]
Report Spam	Form available on Google Search help pages	[16]

2.3. Formal Incident Report to CERT Orange Polska

Leveraging the already established contact with the national incident response team can expedite the response and potentially lead to the blocking of the malicious IP address at the level of national telecommunication operators.

Procedure:

1. **Send an email to:** cert.opl@orange.com.[17]
2. **Message Content:** In the email, refer to the public LinkedIn post to provide context. All collected evidence and analysis should be provided, including the malicious URL, IP address, screenshots, and information about the specific target of the attack (TAK software). The more context the CERT team receives, the more effective their intervention can be.

2.4. Crisis Communication and Community Warning

Immediate and transparent communication with legitimate users is crucial for limiting damage and maintaining trust.

Procedure:

1. **Edit the README.md file:** At the very top of the README.md file in the authentic

GitHub repository, add a large, clear warning block. It should inform about the active phishing attempt, provide the malicious IP address/URL, and categorically state that the only official and safe source of the code is this specific GitHub repository.
2. **Create a SECURITY.md file:** Create a SECURITY.md file in the repository, describing the project's security policy and the procedure for reporting potential vulnerabilities (even if it's just a simple contact email address). This is a professional standard that enhances the project's credibility.
3. **Update on social media:** Publish an update to the original LinkedIn post, informing that the incident has been confirmed and remedial steps have been taken. Provide the link to the safe repository again and warn the community.

Proactive communication transforms the author from a victim into an active defender of their project. Placing a warning directly in the README.md file is an extremely effective way to reach the most interested individuals—developers and users who are most likely to visit the official project page.

3. Long-Term Actions: Strengthening Security and Monitoring (Post-Incident Activity)

After managing the immediate crisis, actions should be implemented to strengthen the project's security and minimize the risk of similar incidents in the future.

3.1. Security Audit of the Repository and GitHub Account

1. **Enable Two-Factor Authentication (2FA):** This is an absolute priority for securing access to the GitHub account.
2. **Review Personal Access Tokens:** Review all active tokens in the account settings and revoke any that are not recognized or no longer in use. Attackers often use stolen tokens to gain unauthorized access to the GitHub API and modify repositories.[2]
3. **Review SSH and Deploy Keys:** Verify the list of SSH keys and deploy keys associated with the account and repositories, removing any unauthorized entries.
4. **Sign Commits with a GPG Key:** Implementing this practice cryptographically

confirms that code changes come from a trusted author. GitHub visually marks such commits as "Verified," which increases user trust.

3.2. Strategy for Monitoring the Project's Digital Footprint

1. **Set up Google Alerts:** Create automatic alerts for key phrases such as "LukeStriderGM/BLOX-TAK-SERVER-IUCP", "BLOX-TAK-SERVER-IUCP" download, and other variations of the project name. This will allow for the quick detection of new impersonation attempts that get indexed by Google.
2. **Regularly Search on GitHub:** Periodically search the GitHub platform for repositories with similar or identical names. Attackers often create fake clones or forks directly on GitHub to increase their apparent legitimacy.[2]
3. **Monitor Discussion Platforms:** If the project has a community on platforms like Discord, Reddit, or specialized forums, it is worth monitoring them for links to unofficial versions of the software.

3.3. Implementing Security Best Practices in an Open Source Project

1. **Clearly Define Official Distribution Channels:** In the README.md file, clearly state that the only official source of the code is this specific GitHub repository. If compiled versions are published, emphasize that they should only be downloaded from the "Releases" tab on the official project page.
2. **Use Checksums:** For each published binary release, provide file checksums (e.g., SHA-256). This will allow users to independently verify the integrity of downloaded archives and ensure they have not been modified.
3. **Maintain a SECURITY.md Policy:** A formalized security policy should be a permanent part of the project.

4. Summary and Final Conclusions

The analyzed incident is not a random phishing attempt but a highly targeted software supply chain attack aimed at a specific and sensitive community of TAK Server users. The attacker's motivation is most likely espionage and the desire to gain access to critical data, rather than direct financial gain.

This incident is a symptom of a broader phenomenon where cybercriminals and state-sponsored actors are increasingly abusing trusted developer platforms like GitHub and global cloud providers to conduct advanced campaigns.[1] They leverage the reputation and scale of these platforms to hide their activities and effectively reach their victims.

The proactive stance of the project author—early detection of suspicious activity and publicizing the issue—is a key and commendable element of an effective defense. The actions described in the presented plan will help neutralize the immediate threat and strengthen the project's resilience for the future. However, it must be remembered that the security of an open-source project, especially one with such a sensitive application, is an ongoing process that requires constant vigilance, monitoring, and the implementation of best practices.

Works cited

1. Attack Demo #3: Github Abuse - Delivering Malware Using Trusted Platforms | RavenMail, accessed July 27, 2025, https://ravenmail.io/blog/github-malware-delivery
2. GitHub Repos Used for Distributing Malware - Checkmarx, accessed July 27, 2025, https://checkmarx.com/blog/github-repos-used-for-distributing-malware/
3. 2024 Malicious Infrastructure Report | Recorded Future, accessed July 27, 2025, https://go.recordedfuture.com/hubfs/reports/cta-2025-0228.pdf
4. Malicious code in fake GitHub repositories | Kaspersky official blog, accessed July 27, 2025, https://www.kaspersky.com/blog/malicious-code-in-github/53085/
5. Malware Distribution Service Exploits Thousands of GitHub Accounts - ChannelE2E, accessed July 27, 2025, https://www.channele2e.com/brief/malware-distribution-service-exploits-thousands-of-github-accounts
6. ThreatFox | AS45090 - Abuse.ch, accessed July 27, 2025, https://threatfox.abuse.ch/browse/tag/AS45090/
7. AS45090 Shenzhen Tencent Computer Systems Company Limited - CleanTalk, accessed July 27, 2025, https://cleantalk.org/blacklists/as45090
8. TAK-SERVER 5.0 - Rocky 8 made easy - YouTube, accessed July 27, 2025, https://m.youtube.com/watch?v=zZgb4KVKtF0&pp=0gcJCdgAo7VqN5tD
9. TAK Server install (Docker) - YouTube, accessed July 27, 2025, https://www.youtube.com/watch?v=h4PA9NN-cDk
10. Installing TAK Server 5.x (RPM Edition) - YouTube, accessed July 27, 2025, https://www.youtube.com/watch?v=r9HD46w1czY

11. Tencent Cloud, accessed July 27, 2025, https://www.tencentcloud.com/report-platform/illegalcontentcomplaint
12. Integrity Policy - Tencent 腾讯, accessed July 27, 2025, https://www.tencent.com/en-us/integrity-policy.html
13. Tencent Cloud - FIRST — Forum of Incident Response and Security Teams, accessed July 27, 2025, https://www.first.org/members/teams/tencent_cloud
14. Report Spam, Phishing, or Malware | Google Search Central | Support, accessed July 27, 2025, https://developers.google.com/search/help/report-quality-issues
15. Reporting Incorrect Data | Safe Browsing APIs (v4) - Google for Developers, accessed July 27, 2025, https://developers.google.com/safe-browsing/v4/reporting
16. reporting scam sites - Google Search Central Community, accessed July 27, 2025, https://support.google.com/webmasters/thread/264176403/reporting-scam-sites?hl=en
17. Kontakt - CERT Orange - Orange Polska, accessed July 27, 2025, https://cert.orange.pl/kontakt/
18. Terminologia - CERT Orange, accessed July 27, 2025, https://cert.orange.pl/warto-wiedziec/terminologia/