From fake interviews to malicious repositories: Disrupting Contagious Interview

By Ramazan Uysal, Parthiban Rajendran, Dawid Osojca, Atlassian Trust and Security

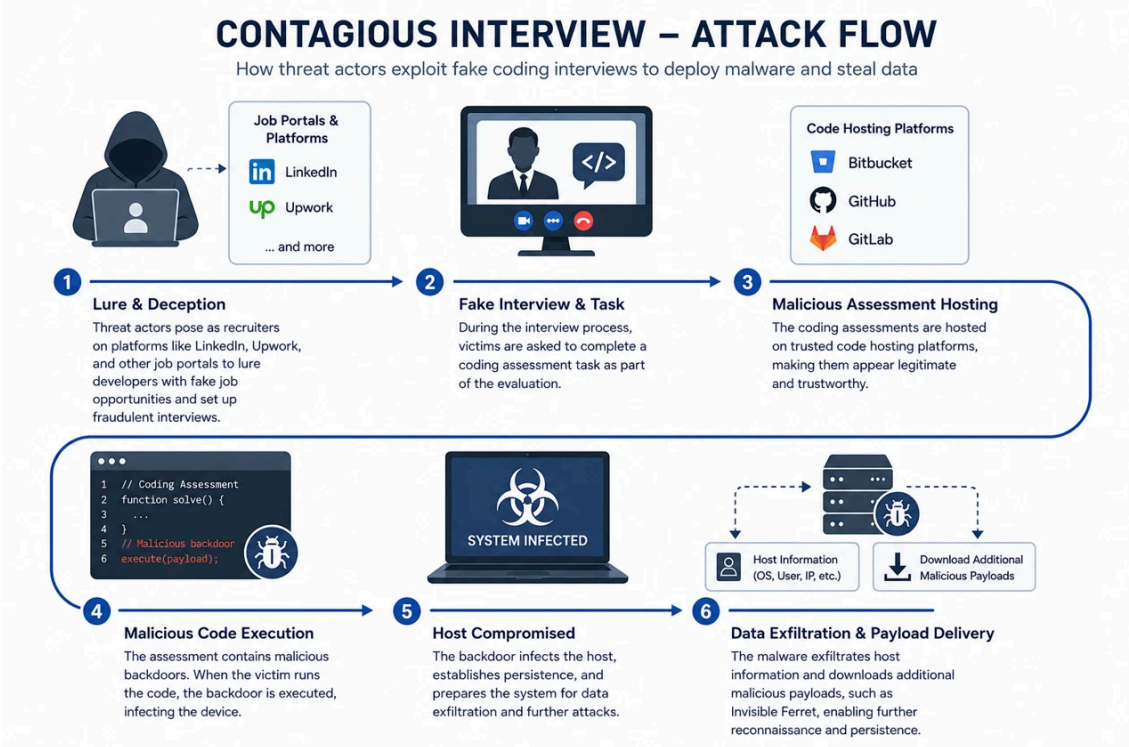
Published: 2026-09-21 · Archived: 2026-09-25 02:00:51 UTC

Software developers and IT professionals are increasingly being targeted through fraudulent recruitment processes that exploit their trust in established development platforms. Candidates are invited to complete seemingly legitimate coding assessments hosted in publicly accessible repositories on services such as Bitbucket, GitHub, and GitLab. The repositories appear to be fully developed applications, with thousands of lines of plausible-looking code and malicious payloads concealed in only a few lines.

Contagious Interview is a persistent campaign using this tactic, attributed with high confidence to North Korean threat actors. When executed, the malicious payloads can steal credentials, cryptocurrency wallets, API tokens, and access to corporate systems.

Atlassian has been working alongside industry peers and the broader security community to track and disrupt activity associated with Contagious Interview. This blog post is being published alongside the full research report, which covers the campaign's tradecraft, indicators of compromise (IOCs), and security best practices to help individuals and organizations strengthen their defenses.

No action is required from Bitbucket customers. Protecting the platform from malicious activity remains an ongoing priority for Atlassian.



Actions Atlassian is taking

Atlassian detects and responds to attempts to abuse its platforms. Our Acceptable Use Policy prohibits malicious content, and we take action when it is violated. To date, hundreds of Contagious Interview repositories and associated accounts have been taken down. Detection continues to improve through industry collaboration and threat intelligence. In-product reporting has also been simplified, allowing visitors to report malware and abuse directly through the Bitbucket interface while viewing a repository.

Publishing this research supports broader threat intelligence exchange and helps maximize disruption efforts across the industry.

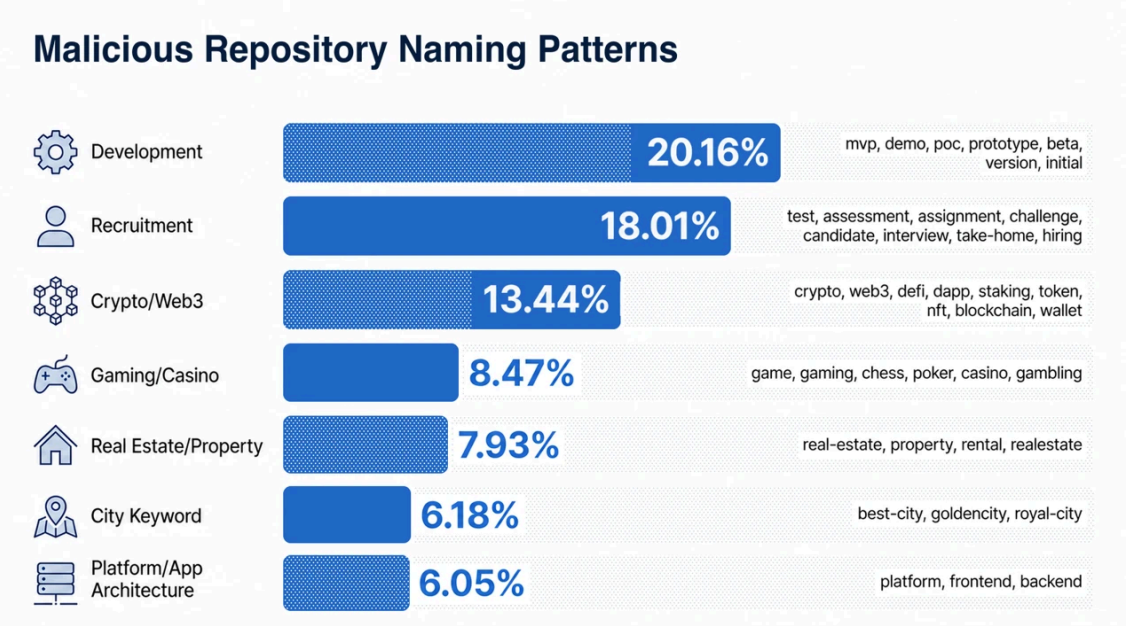
Notable patterns observed across malicious repositories

Atlassian's analysis identified recurring patterns across the campaign, including reused repository themes and code structures, convincing front companies and recruiter personas, infrastructure overlaps with other North Korea-attributed activity, and evolving payload execution techniques.

The research also found that some victims unintentionally became distributors by uploading copies of malicious repositories from legitimate accounts. The full report examines these findings in detail.

Repository themes

Malicious repositories repeatedly used similar naming conventions and recurring project themes. Many also contained the same or nearly identical applications, code, and file structures, with only a small number of files differing—often the files concealing the malicious code.

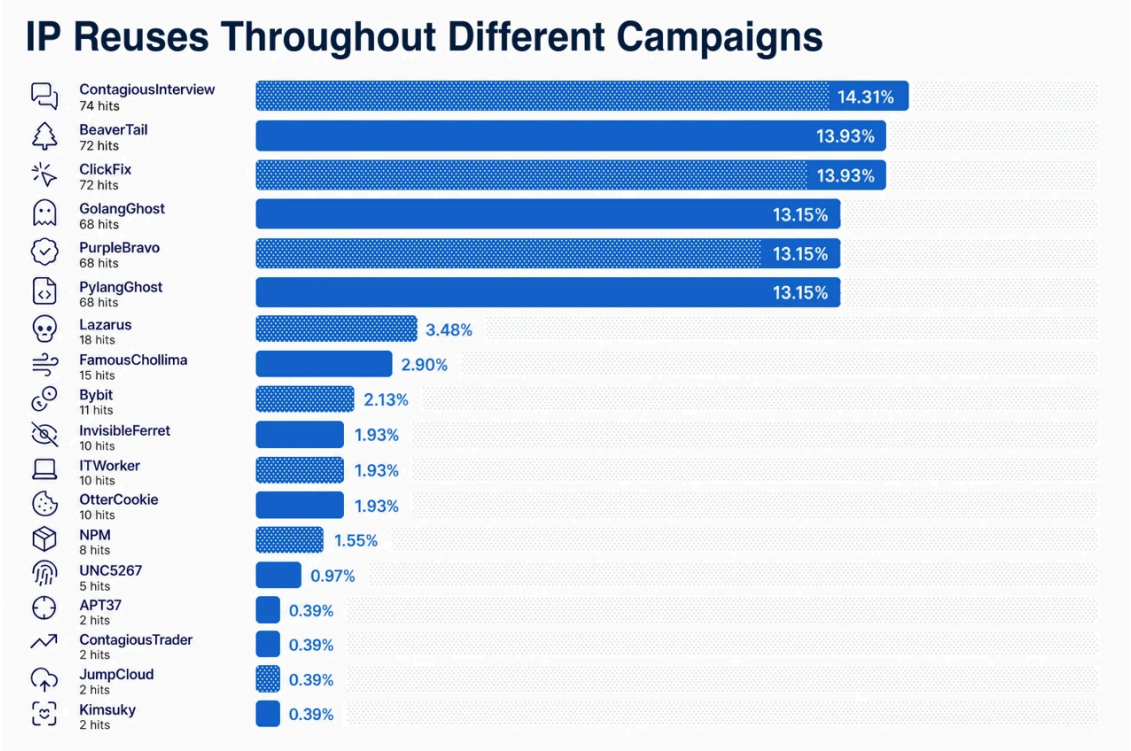


Front companies and fake recruiters

Threat actors established realistic-looking front companies, complete with custom domains, company websites, and seemingly well-established LinkedIn profiles, to make fraudulent recruitment outreach appear credible. Recruiter accounts used both common email providers and addresses tied to newly registered domains, further reinforcing the appearance of legitimacy.

Infrastructure overlaps across different threat actors and campaigns

Analysis of IP addresses used to create malicious Bitbucket accounts and repositories found matches with IOCs publicly shared by external security researchers and organizations. Most matches related to BeaverTail and Contagious Interview, as expected, while dozens were linked to other North Korea-attributed campaigns. These overlaps suggest that some North Korea-attributed groups share operational tradecraft across campaigns.



Evolution of payload execution techniques

The analysis focused on how the initial loader (BeaverTail) concealed in these repositories was executed. Once the loader ran on a victim's device, later-stage malware was delivered outside Bitbucket. The actors continually changed and combined ways of triggering the loader, with almost half of the repositories using two or more techniques. The quarter-by-quarter analysis shows techniques being added, changed, and retired over time.

Evolution of payload execution techniques

	2025Q2	2025Q3	2025Q4	2026Q1	2026Q2
Obfuscated payload in code	84%	100%	99%	100%	100%
Fake fonts	0%	11%	8%	6%	8%
VS Code task	3%	11%	63%	14%	25%
Infected NPM dependencies	13%	0%	6%	0%	4%
NPM lifecycle scripts	16%	11%	16%	26%	9%
Git hooks	0%	0%	0%	0%	8%

Victims as unintended distributors

Threat actors have started asking candidates to record themselves walking through coding assessments and upload their copies to GitHub or Bitbucket. Infected victims can therefore become part of the distribution chain, creating new copies of malicious repositories from legitimate accounts.

Security best practices

While no action is required from Bitbucket customers, the guidance below can help individuals and organizations reduce risk and respond if they encounter a malicious coding assessment.

best practices

Before opening or running an unfamiliar repository

- Use a dedicated, isolated environment for coding assessments and take-home tests.
- Do not use a corporate workstation with access to production credentials.
- Disable Visual Studio Code automatic tasks by setting `task.allowAutomaticTasks` to `off`.

For individuals who may be affected

- Disconnect the device from the network and notify the organization’s security team. Preserve the repository URL, recruiter messages, and commands that were run.
- From a known-clean device, revoke active sessions and rotate passwords, source-control tokens, SSH keys, cloud credentials, API keys, and other accessible secrets.

- If cryptocurrency keys or seed phrases may have been exposed, transfer assets to a new wallet created on a clean device.
- Reformat or reimage the affected device. Deleting the repository or running an antivirus scan alone may not remove follow-on malware or persistence.
- Report the repository and recruiter account to the relevant hosting and recruitment platforms.

For organizations

- Monitor for integrated development environments (IDEs) or terminal applications spawning unexpected shells and scripting runtimes, particularly when commands reference `.vscode`, hidden directories, temporary files, or downloaded dependency scripts.
- Alert on scripting processes accessing browser profiles, password stores, cryptocurrency wallets, keychains, `.ssh`, cloud configuration, environment files, or shell history—especially when followed by HTTP uploads or WebSocket connections.
- When compromise is suspected, isolate and reimage the endpoint, revoke exposed sessions and credentials, investigate downstream access, and hunt across the environment.
- For additional security best practices, review Atlassian's guidance on keeping your organization secure.

If you are seeking a deeper technical analysis, please download the full research report, which provides additional detail on the campaign's infrastructure and evolving tradecraft, along with a complete list of IOCs to support detection and response efforts.
