Contagious Interview | North Korean Threat Actors Reveal Plans and Ops by Abusing Cyber Intel Platforms

Aleksandar Milenkoski ⋮

Executive Summary

- North Korea-aligned threat actors actively monitor cyber threat intelligence to detect infrastructure exposure and scout for new assets. This analysis focuses on the abuse of cyber intelligence platforms by the actors behind the Contagious Interview campaign cluster employing the ClickFix social engineering technique.
- They operate in coordinated teams with real-time collaboration, likely using Slack and multiple intelligence sources such as Validin, VirusTotal, and Maltrail.
- Although aware their infrastructure is detectable, they make only limited changes to reduce detection and disruption risk, while rapidly deploying new infrastructure in response to service provider takedowns.
- This indicates a strategic focus on continuously replacing disrupted infrastructure with new assets to sustain operations and high victim engagement.
- Factors such as decentralized command and competitive internal incentives may limit the threat actors' ability to consistently protect existing infrastructure at scale.
- SentinelLABS' analysis suggests that the threat actors are effective at engaging targets; there were over 230 victims between January and March 2025, with the actual number likely being significantly higher.
- In partnership with SentinelLABS and Validin, Reuters provides further coverage of the human dimension of this threat, exploring victim engagement methods and their personal impact.

Overview

In collaboration with the internet intelligence platform Validin, SentinelLABS has been tracking activity on the platform which we attribute with high confidence to North Korean threat actors involved in the Contagious Interview campaign cluster. This activity, which took place between March and June 2025, involved the threat actors examining cyber threat intelligence (CTI) information related to their infrastructure. Our unique visibility has provided valuable insights into their operational practices, internal coordination, infrastructure management and deployment, and victimology.

SentinelLABS continuously tracks North Korean-aligned threat actors, including their persistent interest in cyber threat intelligence. As part of SentinelLABS' broader efforts to identify and disrupt North Korean operations in collaboration with partner organizations, SentinelLABS and Validin conducted a joint investigation, combining our threat intelligence expertise with Validin's visibility into the threat actors' activities on their platform, to better understand these activities and provide actionable intelligence supporting defensive actions.

SentinelLABS and Validin observed an intensive and coordinated effort by Contagious Interview threat actors to register and use Validin community access accounts within approximately 24 hours after Validin published a blog post on 11 March 2025. The post discusses the infrastructure of Lazarus, a suspected North Korean APT umbrella cluster associated with Contagious Interview activities. Validin's community access portal provides free access to infrastructure intelligence information.

The threat actors used Google Gmail addresses that we had already been tracking as Contagious Interview artifacts at the time of registration. Although Validin blocked the accounts shortly after registration, we observed the threat actors persisting in their efforts to use Validin by creating accounts at later dates. At that point, we intentionally kept one account active over the long term to monitor and gather intelligence on their activities.

We observed that the Contagious Interview threat actors engaged in coordinated activity and likely operated in teams to investigate threat intelligence related to their infrastructure and to monitor for signs of detection. Indicators suggest they used multiple indicators of compromise (IOC) repositories and CTI platforms, including Validin, VirusTotal, and Maltrail. We also identified indicators of real-time teamwork, including possible use of the Slack platform to coordinate their investigations.

Despite thoroughly examining threat intelligence and identifying artifacts that can be used to discover their infrastructure, the threat actors did not implement systematic, large-scale changes to make it harder to detect, thereby reducing its exposure to discovery and disruption. Instead, we observed only sporadic, limited-scale changes targeting specific artifacts used to identify Contagious Interview infrastructure, while the threat actors rapidly deployed new infrastructure in response to service provider takedowns.

This may reflect a focus on investing resources to maintain operational readiness and sustain the campaign's high volume of victim engagement by deploying new infrastructure rather than undertaking broad modifications to protect existing infrastructure. Based on log files unintentionally exposed on several Contagious Interview servers, we identified over 230 individuals affected during the period from January to March 2025, though the actual number is likely much higher.

Given the continuous success of their campaigns in engaging targets, it may be more pragmatic and efficient for the threat actors to deploy new infrastructure rather than maintain existing assets. Potential internal factors, such as decentralized command structures or operational resource constraints, may restrict their capacity to rapidly implement coordinated changes. Moreover, competitive pressures stemming from North Korea's annual revenue quotas for cyber teams likely incentivize operatives to make isolated adjustments to the infrastructure under their control in order to protect their own assets and outperform colleagues, rather than participate in centrally coordinated, large-scale updates.

The threat actors also used Validin to scout and evaluate new infrastructure before acquisition, likely aiming to avoid assets previously flagged as malicious, which would increase detection risk and reduce operational effectiveness once deployed. Following acquisition, they continued to monitor their assets for signs of detection throughout their lifecycle. We were closely monitoring Contagious Interview infrastructure during its acquisition and deployment, which revealed repeated OPSEC failures, suggesting a lack of consistent operational security controls during the infrastructure setup phase.

Background | Contagious Interview and ClickFix

First used in 2023 to label a campaign targeting job seekers, the term Contagious Interview has since been used interchangeably in other contexts, including to refer to an APT group assessed to be a subset of the North Korean umbrella group Lazarus.

In this post, we use Contagious Interview to refer to a cluster of campaigns, variants of the 2023 campaign, that target job applicants using diverse social engineering tactics to trick targets into executing malware.

Contagious Interview activities predominantly target individuals active in the cryptocurrency industry, aiming to gain access to their systems for various purposes, including intelligence collection and the theft of cryptocurrency assets. This supports North Korea's efforts in evading sanctions and generating illicit revenue for financing its projects, including missile programmes.

Contagious Interview campaigns have been typically associated with the umbrella threat cluster Lazarus. DTEX Systems has attributed these campaigns to a group referred to as Gwisin Gang, which likely emerged from an IT organization whose subordination within the North Korean state apparatus is still subject to assessment.

Recent Contagious Interview campaigns, also referred to as ClickFake Interview, involve a social engineering technique known as ClickFix. We assess that the threat actors whose activities are discussed in this post are involved in these campaigns.

ClickFix typically proceeds as follows. A targeted job seeker receives an invitation to participate in a job application process, directing them to a lure website where they are prompted to complete a skill assessment. During the assessment, the applicant encounters a fabricated error message, such as a camera access issue. They are then instructed to copy and paste command lines, often involving utilities like `curl`, to download and execute a supposed update from a separate malware distribution server, unknowingly deploying malware in the process. This technique is discussed in more detail in previous research.

Account Registrations | Initial Activities

The threat actors started creating Validin community accounts on 12 March 2025 at 22:44:11 UTC, an activity which spanned a relatively short interval of approximately 15 minutes, suggesting a concentrated and coordinated approach. We present below the email addresses used for account registrations as well as the IP addresses from which the registrations were conducted. We attribute this activity to Contagious Interview threat actors based on multiple indicators.

Email Address	IP Address
jimmr6587[@]gmail.com	38.170.181[.]10
excellentreporter321[@]gmail.com	194.33.45[.]162
rockstar96054[@]gmail.com	96.62.127[.]126
richardkdavis45[@]gmail.com	45.86.208[.]162
fairdev610[@]gmail.com	70.39.70[.]194
marvel714jm[@]gmail.com	77.247.126[.]189
montessantiago9712[@]gmail.com	38.170.181[.]10

hundredup2023[@]gmail.com	70.32.3[.]15
huzqur023[@]gmail.com	89.19.58[.]51

A significant portion of the IP addresses used for registration, such as `194.33.45[.]162`, `70.39.70[.]194`, `70.32.3[.]15`, `38.170.181[.]10`, and `45.86.208[.]162`, have been associated with Astrill VPN, a VPN service popular among North Korean threat clusters.

Additionally, even before the account registrations, SentinelLABS and Validin were already tracking the email addresses `fairdev610[@]gmail.com`, `richardkdavis45[@]gmail.com`, `rockstar96054[@]gmail.com`, `excellentreporter321[@]gmail.com`, and `hundredup2023[@]gmail.com` as Contagious Interview artifacts. We found these addresses in unintentionally exposed JavaScript scripts (Node.js applications) on Contagious Interview ClickFix malware distribution servers.

We have been tracking these Node.js applications under the ContagiousDrop moniker since their initial exposure. Typically implemented as `app.js` files, the applications distribute malware to targeted individuals and notify the threat actors via email about victim engagement. This engagement includes information submission to Contagious Interview lure websites and the execution of commands, such as `curl`, as directed by the threat actors as part of the ClickFix social engineering tactic. A ContagiousDrop sample is highlighted in previous research on Contagious Interview activity published in April 2025. These applications will be discussed in greater detail later in this blog post.

Moreover, some email addresses have been used for registering Contagious Interview domains pointing to lure websites. For example, `marvel714jm[@]gmail.com` and `jimmr6587[@]gmail.com` have been used to register the `paxos-video-interview[.]com` and `skill-share[.]org` domains, respectively.

Finally, some email addresses were used to register Validin accounts from IP addresses that were also used to register or log in to accounts with other email addresses we attribute with high confidence to Contagious Interview. For example, the account `montessantiago9712[@]gmail.com` was registered from the IP address `38.170.181[.]10`, the same as `jimmr6587[@]gmail.com`.

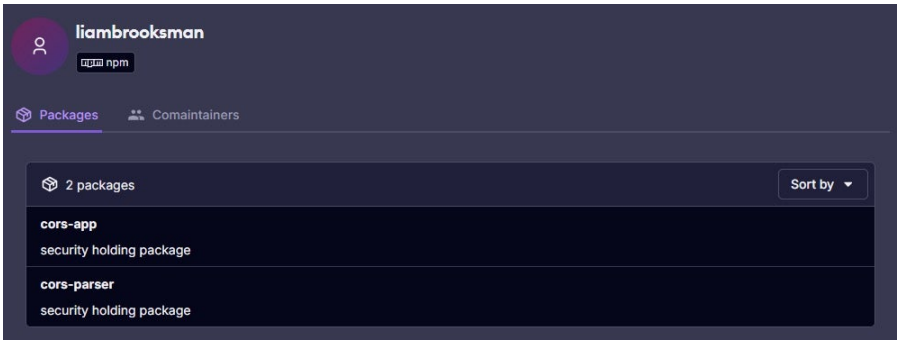
Approximately 15 minutes after the first observed account registration, Validin blocked the Contagious Interview accounts and subsequently prevented further community registrations originating from known Astrill VPN IP addresses or using Gmail accounts.

Account Registrations | Further Activities

After likely realizing that their access to Validin had been blocked, Contagious Interview threat actors attempted to register community accounts again on 25 March 2025 (13 days after the initial registration activity) and 26 April 2025. This time, they also used non-Gmail email addresses, most likely in response to Validin blocking Gmail-based registrations: `info[@]versusx[.]us` and `invite[@]quiz-nest[.]com`. We present below the email addresses used for Validin account registrations, along with the date, time, and originating IP addresses of these registrations.

Email Address	Date (UTC)	Time (UTC)	IP Address
info[@]versusx[.]us	2025-03-25	13:33:01	181.59.180[.]84
mvsolution9[@]gmail.com	2025-04-26	16:48:54	181.215.9[.]29
invite[@]quiz-nest[.]com	2025-04-26	16:51:29	181.215.9[.]29

The domain registration records for `versusx[.]us` include the email address `brooksliam534[@]gmail.com`, which has also been used to register several Contagious Interview domains discussed in previous research, such as `willotalent[.]us` and `nvidia-release[.]us`. Additionally, indicators suggest that the `brooksliam534[@]gmail.com` account has been involved in publishing malicious npm (Node Package Manager) packages (`cors-app` and `cors-parser`) as part of a software supply chain campaign attributed to Contagious Interview threat actors.



The *liambrooksman* persona (*brooksliam534[@]gmail.com*) tracked as maintainer of *cors-app* and *cors-parser*

We observed the registration of `invite[@]quiz-nest[.]com` approximately two minutes after the threat actors attempted to register `mvsolution9[@]gmail.com`. The registration of `mvsolution9[@]gmail.com` failed due to measures Validin implemented following the March 2025 account registration activities. Both actions originated from the same IP address, `181.215.9[.]29`, suggesting the involvement of a single operator.

`mvsolution9[@]gmail.com` has been used to register two Contagious Interview domains: `evalassesso[.]com`, which Sekoia has also attributed to Contagious Interview, and `speakure[.]com`. The `quiz-nest[.]com` website, at least up to 24 May 2025, was implemented in a manner typical of Contagious Interview lure websites.

We also observed login attempts on 9 May 2025 using the `excellentreporter321[@]gmail.com` and `marvel714jm[@]gmail.com` accounts, which had been blocked by Validin in March 2025.

The threat actors' shift to using non-Gmail addresses, along with their continuous attempts to bypass Validin's access controls, highlights their adaptability and persistent interest in Validin data. Recognizing their persistence in obtaining community access, we intentionally kept only the `info[@]versusx[.]us` account active to monitor subsequent activity, determine their objectives, and gather further intelligence. Since then, the Contagious Interview threat actors have continued attempting to register new Validin accounts through the time of writing this post.

Account Registrations | Personas

In accordance with Validin's policy for community accounts, the Contagious Interview actors completed registration forms requesting information such as full name, affiliation, and reason for registration.

Account	Full Name	Affiliation	Reason
excellentreporter321[@]gmail.com	Andress Victor Pabon Carrascal	DAG	Find My Platform.
fairdev610[@]gmail.com	Fair Dev	Talents Vision	Reference
hundredup2023[@]gmail.com	Thomas Mitchell	Baymax	to find domain
huzqur023[@]gmail.com	Hamza	Starlink	I will use this for phishing check
info[@]versusx[.]us	Noraida	Versusx	Research
invite[@]quiz-nest[.]com	Anika Larkin	Quiz Nest	Google
jimmr6587[@]gmail.com	jimmr	Individual	Github
marvel714jm[@]gmail.com	Mar Vel	Paxos	Valisin
montessantiago9712[@]gmail.com	Santiago Montes	Personal	Virus Checker
mvsolution9[@]gmail.com	Anika Larkin	Test	Ggle
richardkdavis45[@]gmail.com	Richard Davis	CreatDao	/
rockstar96054[@]gmail.com	Rock Lee	FWW	Googling

The threat actors used a diverse range of names, from generic handles like `jimmr` to pop-culture references such as `Rock Lee` (a character from the Japanese anime series Naruto), `Mar Vel` (likely referring to Mar-Vell, a Captain Marvel character from Marvel Comics), and `Santiago Montes` (the main protagonist of the animated television series Santiago of the Seas), as well as more elaborate, seemingly legitimate full names like `Andress Victor Pabon Carrascal`. The reuse of the name `Anika Larkin` for two different accounts, `invite[@]quiz-nest[.]com` and `mvsolution9[@]gmail.com`, combined with both accounts being registered from the same IP address (`181.215.9[.]29`) within approximately two minutes, suggests the involvement of a single individual.

Some affiliations correspond to fake hiring platforms operated by Contagious Interview. For example, `Quiz Nest` aligns with the domain `quiz-nest[.]com`, while `Paxos` corresponds to domains such as `paxos-video-interview[.]com` and `paxosassessments[.]com`. The account `marvel714jm[@]gmail.com`, which used the `Paxos` affiliation, was also used to register the domain `paxos-video-interview[.]com`. This suggests the actors leveraged their own infrastructure and fabricated brands to create a more convincing facade of legitimacy.

In addition to these fake platforms, the threat actors also used names of legitimate, well-known companies such as `Starlink`, as well as vague descriptors like `Individual` or `Personal`.

Some of the stated reasons for registration provide direct insight into the threat actors' primary objective: investigating threat intelligence information related to their infrastructure. For example, pretexts such as `Research`, `To find domain`, and `Find My Platform` indicate their interest in exploring Validin's data.

Validin Use | Activity Across Multiple Platforms

The majority of accounts began using the Validin platform immediately after registration. In total, we observed 57 unique search terms across all categories supported by the platform, including domain names, hashes, URLs, web metadata, keywords, and IP addresses.

The threat actors did not search for any IOCs reported in Validin's blog post, which we suspect triggered their initial interest in the platform. Therefore, we assess the post only brought Validin to their attention, after which they integrated Validin into a broader workflow for investigating threat intelligence related to their operations by leveraging multiple sources.

We observed indicators suggesting that the threat actors used additional IOC repositories and platforms alongside Validin to conduct comprehensive investigations. These included VirusTotal and the `apt_lazarus.txt` file, which is part of the Maltrail project and publicly available on GitHub. This file is regularly updated with domain names, IP addresses, and URLs attributed to the Lazarus umbrella APT cluster, as well as sources providing attribution information or context, such as social media, blog posts, and other threat intelligence platforms (including VirusTotal and Validin). VirusTotal is a malware analysis service and threat intelligence platform that aggregates detection results, reputation assessments, and contextual information for files, URLs, domains, and IP addresses from a wide range of detection engines, third-party tools, and its user community.

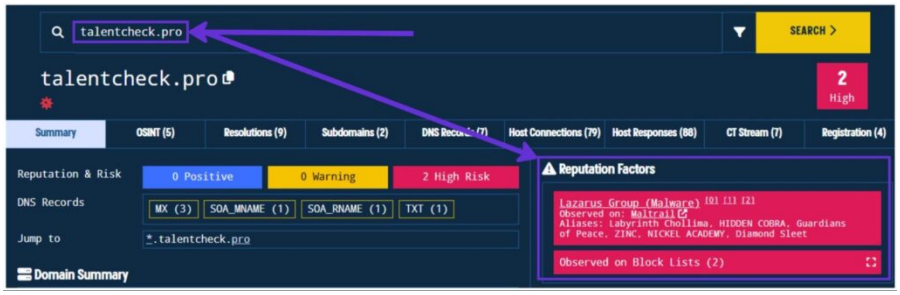
The very first search term used by the threat actors was the keyword `TalentCheck`, entered on 12 March 2025 at 22:44:40 UTC. `TalentCheck` is the title of multiple Contagious Interview websites, including `skillcheck[.]pro`, `talentcheck[.]pro`, and `vidassesspro[.]com`. The keyword was first published as an artifact identifying Contagious Interview websites approximately one day earlier by Maltrail in `apt_lazarus.txt`, on 11 March 2025 at 11:18:22 UTC. This suggests that the threat actors likely used Validin to investigate what additional information the platform could provide based on the `TalentCheck` keyword they first observed in `apt_lazarus.txt`.

TalentCheck in *apt_lazarus.txt*

Most of the search terms the threat actors used in Validin had been published exclusively in `apt_lazarus.txt` at the time of the search and were queried shortly after their appearance in the file, sometimes within less than an hour. This supports our assessment that the Contagious Interview actors closely monitored `apt_lazarus.txt` and used Validin to gather further details and contextual information.

In addition to Maltrail, we suspect that the Contagious Interview threat actors also use VirusTotal, or monitor what information about their infrastructure and malware is available on the platform, in conjunction with Validin. For example, the account `richardkdavis45[@]gmail.com` queried Validin for the URL `https[://]robinhood[.]evalvidz[.]com/invite/fZ6j8A2k` on 12 March 2025 at 22:59:20 UTC, just a few minutes after the exact same URL was first submitted to VirusTotal at 22:54:24 UTC.

Based on log files, we were able to reconstruct the exact navigation paths of the Contagious Interview threat actors within Validin. We observed a strong interest in external references that provide attribution information for specific search terms, which Validin displays in the `Reputation Factors` panel on the search results page. For most of the domains they searched, the threat actors visited every available external reference, demonstrating a determined effort to conduct thorough CTI investigations by gathering information from multiple sources.



Reconstructed navigation path of the *jimmr6587[@]gmail.com* account

Validin Use | Team Collaboration

We observed multiple accounts searching for the same terms within a very short time frame, indicating a coordinated and collaborative effort involving multiple individuals. In addition, we identified strong indicators that the threat actors were using Slack, a messaging platform commonly used for team communication and collaboration, to coordinate their activities.

When investigating patterns of account activity and search behavior using Validin log data, we observed that the `jimmr6587[@]gmail.com` account was the first to search for the domain `webcamfixer[.]online` on 12 March 2025 at 22:54:19 UTC, followed by `excellentreporter321[@]gmail.com` (22:55:17 UTC), `rockstar96054[@]gmail.com` (22:55:25 UTC), `richardkdavis45[@]gmail.com` (22:55:43 UTC), and `fairdev610[@]gmail.com` (22:55:55 UTC).

Our cross-examination of web server log data revealed that the search by `jimmr6587[@]gmail.com` was followed by requests to Validin from Slack Robots for the same URL generated by the search (`/detail?type=dom&find=webcamfixer[.]online`). Slack Robots retrieve web content when a user posts a URL in a channel or direct message, displaying summary information such as the page title, meta description, and a preview image.

These Slack Bot requests were followed by requests to the same URL from the IP addresses from which the accounts `excellentreporter321[@]gmail.com`, `rockstar96054[@]gmail.com`, `richardkdavis45[@]gmail.com`, and `fairdev610[@]gmail.com` had logged in. The timing of these requests aligns with each account's respective search for `webcamfixer[.]online` as recorded in Validin logs.

```
[redacted] - "-" [2025-03-12 22:55:10 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...] "Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)"

[redacted] - "-" [2025-03-12 22:55:12 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...]"Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)"

194.33.45.162 - "-" [2025-03-12 22:55:17 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...]
96.62.127.126 - "-" [2025-03-12 22:55:25 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...]
45.86.208.162 - "-" [2025-03-12 22:55:43 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...]
70.39.70.194 - "-" [2025-03-12 22:55:55 UTC] "GET /detail?type=dom&find=webcamfixer.online
HTTP/1.1" [...]
```

Web server log data

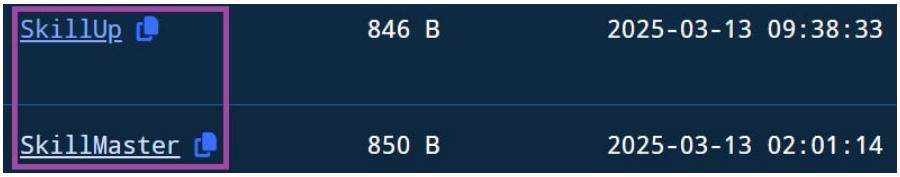
This suggests that the individual operating the `jimmr6587[@]gmail.com` account searched for `webcamfixer[.]online` in Validin, pasted the resulting URL into Slack, and that the individuals behind the other accounts subsequently clicked on the shared link in quick succession.

Validin Use | Limited Infrastructure Changes

Despite thoroughly investigating CTI information and identifying artifacts that could be used to discover their infrastructure, we did not observe any systematic or widespread actions by the Contagious Interview threat actors to make their infrastructure more difficult to discover and to protect it against detection and disruption. We observed only sporadic changes of limited scale that did not significantly reduce the infrastructure's visibility to defenders and threat researchers.

For example, after searching in Validin for the keyword `SkillMaster`, which is the title of multiple Contagious Interview websites, the threat actors changed the title of only one site, `skillmasteryhub[.]us`, from

SkillMaster to SkillUp a few hours after the search. This change was not applied to other websites with the same title, such as VidHireHub[.]com.



Website title change on 13 March 2025, as seen in Validin

Many of the Contagious Interview domains that the threat actors searched for in Validin were taken down by their respective registrars shortly after the search activity. Some may have been voluntarily deactivated by the threat actors themselves, likely to avoid seizure or further investigation, particularly if the domains were linked to their operational security. For example, the A DNS record for the domain careerquestion[.]com was removed just a few hours after the threat actors searched for it in Validin and confirmed its association with their operation.

The lack of systematic changes to their infrastructure, despite the threat actors' thorough examination of CTI information, suggests several possible explanations.

Given the continuous success of the campaign in engaging job applicants, the threat actors may be prioritizing maintaining operational readiness and meeting their objectives by rapidly deploying new assets to replace disrupted infrastructure, rather than undertaking large-scale targeted changes. We observed a high rate of new infrastructure deployment by the Contagious Interview threat actors alongside losses of existing infrastructure due to actions by service providers, which supports this assessment.

There may be internal limitations, such as a lack of a central authoritative command structure or resource constraints affecting their ability to modify infrastructure rapidly and at scale. Additionally, the North Korean regime sets annual earnings quotas for cyber teams, requiring them to self-fund while meeting revenue targets. These quotas likely incentivize operatives to continually seek new income sources, fostering intense competition within teams. As a result, individuals managing only portions of the Contagious Interview infrastructure may make limited changes aimed at evading detection of the infrastructure they oversee, thereby gaining advantages over colleagues, rather than engaging in coordinated, large-scale modifications.

Validin Use | New Infrastructure And OPSEC Failures

The activity patterns of the info@versusx[.]us account on Validin, which we intentionally kept active over the long term, suggest that the threat actors used the platform not only to monitor for signs of detection related to their existing infrastructure, but also:

- To scout and evaluate new infrastructure prior to purchase, highly likely to determine whether it had been previously reported as malicious. This helps the threat actors avoid acquiring assets already labeled as malicious, which would increase the risk of detection and reduce the effectiveness of their operations once deployed.
- To monitor newly acquired infrastructure throughout its lifecycle for any indicators of detection.

For instance, on March 25, 2025, we observed the info@versusx[.]us account searching for the domain names hiringassessment[.]net, hiringassessment[.]com, hireassessment[.]com, easyjobinterview[.]org, and screenquestion[.]org. All of these domains were available for purchase at the time. These names align with the recruitment-related themes typically used in Contagious Interview activities.

The info@versusx[.]us account also searched for multiple domains shortly after they were purchased and continued monitoring them for signs of detection after deploying web content. One example is skillquestions[.]com, which was first queried on March 25, 2025, at 17:33:34 UTC, just minutes before it was registered at 17:41:14 UTC. Additional searches occurred shortly before content was deployed on April 23, 2025, and continued periodically until May 6, 2025. According to Validin data, the skillquestions[.]com website remained operational until at least May 13, 2025, at 20:44:27 UTC.

Our continuous monitoring of the planning, acquisition, and deployment of new Contagious Interview infrastructure allowed us to identify OPSEC mistakes made by the threat actors throughout the process. We observed multiple instances of such errors, including the unintended exposure of files and directory contents, which indicate poor OPSEC practices during infrastructure deployment and provide further insight into their operations.

For example, api.release-drivers[.]online was exposing its web root directory, the files it contained, and their associated modification timestamps. This included error logs from a Node.js application stored in

`/home/relefmwz/api.release-drivers[.]online/`, indicating that the threat actors used the username `relefmwz`. The exposed timestamps provide insight into when the Contagious Interview operators deployed content to the server, allowing us to reconstruct their activity timeline.

Name	Last Modified	Size
__MACOSX	2025-04-28 10:52	-
cgi-bin	2025-04-28 10:50	-
node_modules	2025-03-19 02:08	-
public	2025-01-16 20:49	-
tmp	2025-04-28 11:05	-
package-lock.json	2025-03-19 02:08	49k
package.json	2025-03-19 02:08	1k
schema.js	2025-02-20 02:52	1k
stderr.log	2025-05-09 12:11	1187k

Exposed web root directory of *api.release-drivers[.]online*

Further, several newly deployed ClickFix malware distribution servers, such as `api.camdriverhelp[.]club` and `api.drive-release[.]cloud`, were exposing ContagiousDrop applications along with the log files they had generated. These files contain information on affected individuals, allowing us to gain valuable insights into the victimology of the campaigns.

ContagiousDrop Applications

The ContagiousDrop applications, typically implemented in `app.js files`, are deployed on ClickFix malware distribution servers such as `api.drive-release[.]cloud`. These applications run servers that listen on configured ports to handle incoming HTTP GET and POST requests, executing different functions based on the specific request path.

The ContagiousDrop applications deliver malware disguised as software updates or essential utilities. They distribute a tailored payload based on the victim's operating system (Windows, macOS, or Linux), system architecture, and method of interaction with the server, such as the use of the `curl` command.

```
//////////////////////////WINDOWS/////////////////////////////////////
app.get('/nvidia-:id.update', async (req, res) => {
  const { id } = req.params;
  const userAgent = req.headers['user-agent'] || '';
  const clientIp = req.headers['x-forwarded-for'] ||
  req.connection.remoteAddress || req.socket.remoteAddress;
  const isCurl = userAgent.includes('curl');
  const filePath = isCurl
    ? path.join(__dirname, 'result', 'nodejs.zip')
    : path.join(__dirname, 'result', 'nvidia-real.zip');
```

Operating system-specific malware delivery

In addition to delivering malware, the ContagiousDrop applications feature an integrated email notification system. These notifications, sent from a configured email address such as `designedcuratedamy58[@]gmail.com`, provide the Contagious Interview threat actors with insights into victim engagement and interaction patterns and are delivered to their configured recipient addresses. For example, an email is triggered when an affected individual starts a fake skill assessment or executes a `curl` command to download a file from the ClickFix malware distribution server.

```
const RECIPIENT = "daisukeokitsugu@gmail.com"
// Route to send the file

const emails ={
    "AM77": "eliteengineer0523@gmail.com",        // Ames
    // "RC1S": "rockstar96054@gmail.com",            // Rock
    "THOM": "hundredup2023@gmail.com",            // Thomas
    // "MA6C": "phoenixfire471@gmail.com",           // MAXWELL
    // "AW9S": "awesomium430@gmail.com",             // Awesome
    // "AL7J": "betosoto2819@gmail.com",             // Aladdin
    // "IS3K": "rodriguezjamesdaniel0807@gmail.com", // Isofu
    // "KT1P": "johnkane84830@gmail.com",           // Kane
    "RICH": "richardkdavis45@gmail.com",          // Richard
    // "CT3R": "thedrgn1011@gmail.com",              // Cat
    "ARTE": "fairdev610@gmail.com",               // Artemis
    "JALE": "trevorgreer9312@gmail.com",          // Jalen
    // "MV2R": "marvel714jm@gmail.com"               // Marvel
}
```

Email notification recipients

Furthermore, these applications record victim information across multiple files and interaction points, effectively building a victimology database and logging victim activities. For example, initial and later engagements are captured in `client_ips_start_test.json` and `client_ips_submit.json`, including details such as full name, email address, IP address, phone number, and the date of interaction. Malware download initiations are logged in files such as `client_ips_start.json` and `client_ips_mac_start.json`, which capture operating system–specific payload delivery.

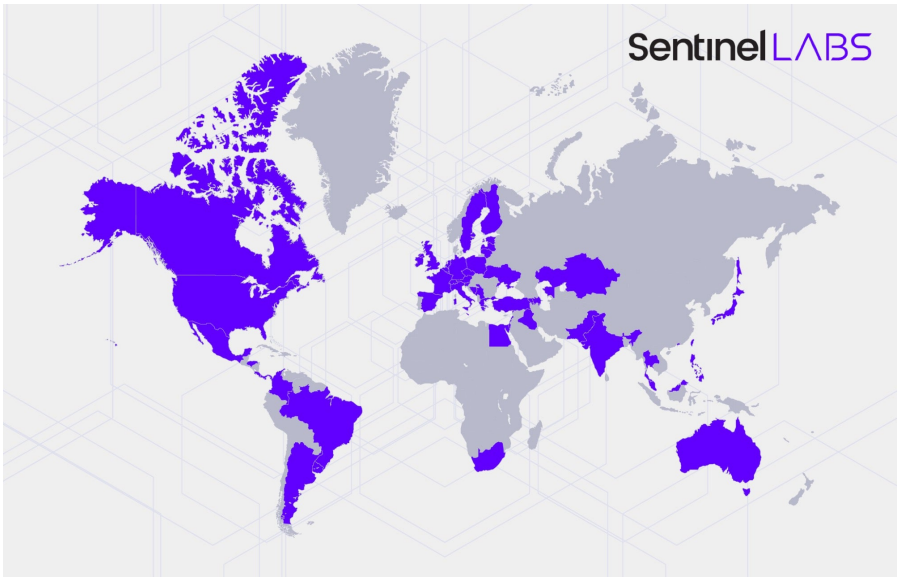
```
app.post('/start-test', async (req, res) => {
  const { data, name, email, company, unique } = req.body;
  const clientIp = req.headers['x-forwarded-for'] || req.connection.remoteAddress
  || req.socket.remoteAddress;

  const logEntry = {
    data,
    name,
    email,
    company,
    ip: clientIp,
    ID: unique,
    date: new Date().toISOString()
  };

  const filePath = path.join(__dirname, 'client_ips_start_test.json');

  // Log client data
  await logToFile(filePath, logEntry);
```

Logging to *client_ips_start_test.json*

ContagiousDrop | Victimology

Based on ContagiousDrop log files we retrieved, we identified over 230 individuals who engaged with Contagious Interview lures between mid-January and the end of March 2025. This figure is based on log files from only a few Contagious Interview servers; therefore, the actual number of affected individuals is likely significantly higher. Their engagement spanned multiple stages of the attack, including completing fake assessment tests and progressing to the infection phase via the ClickFix technique.

Most of the affected individuals work in roles related to cryptocurrency and blockchain technologies, primarily within the marketing and finance sectors, and are geographically distributed worldwide. They engaged with lures involving various job positions, such as Portfolio Manager, Investment Manager, and Senior Product Manager, across a range of impersonated companies including Archblock, Robinhood, and eToro.



Contagious Interview victimology

In addition to entries related to victim activity, the ContagiousDrop logs also contain records likely generated during testing of lure deployment and campaign infrastructure by the Contagious Interview threat actors themselves. They used email addresses and persona names we have associated with them, such as `awesomium430[@]gmail.com` (found in ContagiousDrop code) and Richard Davis. Other names, such as `test`, `test user`, and `Lazaro`, indicate internal testing activity, with `Lazaro` likely being derived from the name of the North Korean umbrella threat cluster associated with Contagious Interview activities: Lazarus.


```
{
  "data": "vpbR859W",
  "userName": "test user",
  "companyName": "Robinhood",
  "roleName": "Operations Manager",
  "IP": "45.86.208.162,198.54.116.89",
  "ID": "RICH",
  "date": "2025-03-24T09:49:59.345Z"
}
```

```
{
  "name": "Lazaro",
  "email": "awesomium430@gmail.com",
  "company": "https://www.gauntlet.xyz/",
  "ip": "200.10.34.127,199.188.200.35",
  "ID": "AW",
  "date": "2025-01-16T20:44:59.694Z"
}
```


Log entries

Conclusions

North Korean threat groups actively examine CTI information to identify threats to their operations and improve the resilience and effectiveness of their campaigns, depending on their operational priorities. In addition to the actors behind the Contagious Interview campaign cluster, SentinelLABS has also observed other North Korean groups demonstrating interest in threat intelligence prior to the activities discussed in this post. In 2024, we retrieved malware associated with ScarCruft, likely designed to target consumers of threat intelligence reporting, such as threat

researchers and other cybersecurity professionals. We suspect the actors aimed to gain insights into non-public CTI and defensive strategies.

In this post, we disclose indicators and TTPs that enable the sustained tracking of the Contagious Interview threat actors. While we expect them to alter their methods as a result, the expanding scale and broad targeting of these operations suggests greater benefit in empowering the wider public to effectively defend than there is in hoarding actionable intelligence indefinitely. SentinelLABS maintains other methods of tracking these evolving campaigns.

Based on our observations, the Contagious Interview threat actors do not implement systematic changes to their infrastructure based on the CTI information they consume from multiple sources, which could make their operations harder to detect or disrupt. Despite this, they continue to achieve a relatively high success rate in attracting job seekers through fraudulent employment offers and skill assessment tests. Their operational strategy appears to prioritize promptly replacing infrastructure lost due to takedown efforts by service providers, using newly provisioned infrastructure to sustain their activity.

Therefore, a critical element in mitigating this threat is the human factor. It is important that job seekers, particularly those within the cryptocurrency sector, exercise heightened vigilance when engaging with employment offers and associated assessments.

In addition, infrastructure service providers play an important role in disrupting Contagious Interview operations. Continuous and effective actions against the threat actors' infrastructure can significantly reduce their capacity to carry out attacks. Close collaboration and coordination between service providers and the threat intelligence community are crucial to mitigating the impact of these activities. SentinelLABS and Validin remain committed to sharing timely and actionable threat intelligence to support these collaborative efforts.

Indicators of Compromise

Email Addresses (Contagious Interview Operators)

admin[@]quickproassess[.]com
awesomium430[@]gmail.com
betosoto2819[@]gmail.com
brooksliam534[@]gmail.com
chris[@]wegrowup[.]us
daisukeokitsugu[@]gmail.com
denys[@]gmail.com
designedcuratedamy58[@]gmail.com
dzsignzdcuatzdamy[@]gmail.com
eliteengineer0523[@]gmail.com
excellentreporter321[@]gmail.com
fairdev610[@]gmail.com
ghostmaxim777[@]outlook.com
hundredup2023[@]gmail.com
huzqur023[@]gmail.com
info[@]versusx[.]us
invite[@]quiz-nest[.]com
jimmr6587[@]gmail.com
johnkane84830[@]gmail.com
legendaryaladdin[@]motionassess[.]com
marvel714jm[@]gmail.com
maxwell[@]gmail.com
montessantiago9712[@]gmail.com
mvsolution9[@]gmail.com
phoenixfire471[@]gmail.com
richardkdavis45[@]gmail.com
rockstar96054[@]gmail.com
rodriguezjamesdaniel0807[@]gmail.com
rv882866.hstgr.cloud[@]glitchmedic[.]com
sinbad[@]hirelytics360[.]com
thedrgn1011[@]gmail.com
trevorgreer9312[@]gmail.com
yudaiaoyama14[@]gmail.com

IP Addresses

Value	Note
181.215.9[.]29	Used for account registration and logging into Validin
181.53.13[.]189	Used for logging into Validin
181.59.180[.]84	Used for account registration and logging into Validin
194.33.45[.]162	Used for account registration and logging into Validin
216.24.215[.]231	Used for logging into Validin
38.170.181[.]10	Used for account registration and logging into Validin
45.86.208[.]162	Used for account registration and logging into Validin
70.32.3[.]15	Used for account registration and logging into Validin
70.39.70[.]194	Used for account registration and logging into Validin
77.247.126[.]189	Used for Validin account registration
89.19.58[.]51	Used for account registration and logging into Validin
96.62.127[.]126	Used for account registration and logging into Validin

Contagious Interview Domains

careerquestion[.]com
evaluateiq[.]com
hirelytics360[.]com
motionassess[.]com
nvidia-release[.]us
paxos-video-interview[.]com
paxosassessments[.]com
quickproassess[.]com
quiz-nest[.]com
robinhood[.]evalvidz[.]com
skill-share[.]org
skillcheck[.]pro
skillmasteryhub[.]us
skillquestions[.]com
talentcheck[.]pro
versusx[.]us
vidassesspro[.]com
VidHireHub[.]com
webcamfixer[.]online
willotalent[.]us

ClickFix Malware Distribution Servers

api.camdriverhelp[.]club
api.drive-release[.]cloud
api.release-drivers[.]online
glitchmedic[.]com

Domains Scouted by Contagious Interview Operators

easyjobinterview[.]org
hireassessment[.]com
hiringassessment[.]com
hiringassessment[.]net
screenquestion[.]org

SHA-1 Hashes

Value	Note
24042a8eea9b9c20af1f7bae00296b44968a068f	ContagiousDrop application (app.js)
44ddabf5b5d601077936a130a2863a96d2af1c8e	ContagiousDrop application (app.js)
4a8bfa28d46ae14e45a50e105e2d34f850ffa96c	ContagiousDrop application (app.js)