2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

THE PHANTOM CIRCUIT: THE LAZARUS GROUP'S EVOLUTION IN SUPPLY CHAIN COMPROMISE

A sophisticated global effort by North Korea, leveraging advanced techniques to infiltrate networks and exfiltrate sensitive data from developers worldwide.

Ryan Sherstobitoff

SecurityScorecard, USA

rsherstobitoff@securityscorecard.io

ABSTRACT

In December 2024, a routine software update concealed a global cyber threat. The North Korean state-sponsored Lazarus Group infiltrated trusted development tools, launching a sophisticated supply chain attack code-named Phantom Circuit. This campaign compromised hundreds of victims across cryptocurrency and technology sectors, leveraging advanced obfuscation techniques via proxy servers in Hasan, Russia.

Our investigation uncovered a critical shift in Lazarus Group's tactics – embedding malware directly into widely used development applications. The attackers utilized an extensive command-and-control (C2) infrastructure, operational since September 2024, to manage exfiltrated data. Their administrative platform, secured behind proxy relays, facilitated persistent remote access and data organization through a hidden React-based interface with Node.js APIs. Further analysis indicated overlap between Phantom Circuit and North Korean IT worker schemes, where state-sponsored actors disguised as freelance developers contributed to compromised software projects.

This study presents a detailed analysis of Phantom Circuit, including its layered infrastructure, anonymization techniques, and global scale of compromise. Our findings indicate:

- Infrastructure sophistication: Lazarus employed VPNs and commercial proxy services to obscure North Korean IP addresses before routing traffic to C2 servers.
- Targeted sectors: Over 1,500 developers worldwide, primarily in technology and cryptocurrency, were compromised.
- Data exfiltration: Stolen credentials, authentication tokens, and system configurations were systematically organized and stored in *Dropbox* for further exploitation.
- Operational adaptations: The use of modern frameworks like React and Node.js for managing stolen data underscores Lazarus Group's evolution in cyber operations.

Our investigation leveraged a combination of OSINT analysis and netflow and *STRIKE* threat intelligence feeds. We identified key North Korean IP addresses originating traffic to *Astrill* VPN endpoints. These endpoints then relayed through the *Oculus Proxy* network, registered to Sky Freight Limited in Hasan, Russia, before reaching the command-and-control infrastructure. Further analysis showed connections between these IPs and previous cyber operations linked to North Korean state-sponsored activities, confirming the involvement of Lazarus Group actors operating from Pyongyang. Additionally, overlaps were identified between Phantom Circuit and North Korea's IT worker schemes, where operatives, masquerading as freelance developers, injected malicious code into software repositories used in global development projects.

BACKGROUND

During *STRIKE*'s investigation of Operation 99, our team identified multiple command-and-control (C2) servers active since September 2024. These servers, despite variations in payload structure and obfuscation techniques, shared a consistent implementation across the campaign. While their primary purpose appeared to be delivering payloads and maintaining communication with infected systems over port 1224, deeper analysis revealed an additional operational layer.

Critical questions – such as how exfiltrated data was handled and what infrastructure was used to manage these servers – remained unanswered until now. Our findings uncovered a concealed administrative system within the C2 infrastructure that provided Lazarus with centralized control over their campaign.

The discovery of this hidden layer provided key insights into the mechanics of Lazarus's campaign. Each C2 server hosted a web-based administrative platform, built with a React application and a Node.js API. This platform was not just an interface but a comprehensive system that allowed the attackers to:

- Organize and manage exfiltrated data with precision.
- Maintain direct oversight of compromised systems.
- Control payload delivery and other operations from a centralized hub.

This administrative layer was consistent across all the C2 servers analysed, even as the attackers varied their payloads and obfuscation techniques to evade detection.

Supply chain attack

Lazarus has been observed altering legitimate software packages by embedding obfuscated backdoors, deceiving developers into executing these compromised packages. To the untrained eye it goes unnoticed and successfully executes. These packages may involve anything from cryptocurrency applications to authentication solutions.

Global reach

This analysis makes it evident that Lazarus was orchestrating a global operation targeting the cryptocurrency industry and developers worldwide. The campaigns resulted in hundreds of victims downloading and executing the payloads, while in the background, the exfiltrated data was being siphoned back to Pyongyang.

Attributing back to Pyongyang

Using NetFlow analysis and temporal traffic patterns, we traced the operation to Pyongyang with high confidence. The Lazarus Group employed a multi-layered obfuscation strategy to conceal their origin and manage their campaign. The flow of operations was as follows:

1. Initial connection: six distinct North Korean IP addresses were observed initiating connections that marked the starting point of the operation.
2. VPN obfuscation: the attackers routed traffic through *Astrill* VPN endpoints, leveraging the commercial service to mask their true geographic origin.
3. Proxy relay: from the VPNs, traffic moved through an intermediate proxy layer registered to Sky Freight Limited in Hasan, Russia. This additional layer blended malicious traffic with legitimate network activity.
4. Command-and-control servers: the obfuscated traffic ultimately reached the C2 infrastructure, hosted on Stark Industries servers. These servers facilitated payload delivery, victim management and data exfiltration.

This layered infrastructure tied the six North Korean IP addresses directly to the C2 servers, confirming Lazarus Group's role in managing the operation from within North Korea.

Key findings

- We successfully identified the operational infrastructure used to coordinate targeted operations. We assess with high confidence that this network served to route traffic from *Astrill* VPNs to the destination C2s through proxies.
- Lazarus uses a sophisticated network of *Astrill* VPN exit points and proxies to obscure traffic while managing C2 servers. We successfully traced the connections through the VPNs to six distinct IP addresses in Pyongyang, North Korea.
- This operation is a clear indication of a software supply chain attack, where Lazarus is implanting malicious code into legitimate software. We observed targeted operations from September 2024 to January 2025. The latest campaign claimed 233 victims across the world.
- Lazarus developed a sophisticated React application and API to manage exfiltrated data and the delivery of payloads. This application was deployed on every C2 server and managed over port 1245.

ATTACKER'S OPERATIONAL INFRASTRUCTURE

Lazarus operators maintained an operational infrastructure to manage C2s and associated assets. We began our investigation by looking into connections to the C2 server, hoping to be able to identify from where the adversary was controlling the infrastructure. We identified an intermediate network of proxies that were found connecting to the C2s over management ports such as 1245 and 3389 (Remote Desktop).

According to WHOIS and other public records, this intermediate proxy network is registered to Sky Freight Limited, located in Hasan, Russia. These IPs are actually assigned to the *Oculus Proxy* network, as we describe later.

```
inetnum:        83.234.227.0 - 83.234.227.255
netname:        SKYFREIGHT-NET
descr:          (MS009388) Skyfreight_Limited,
descr:          Hasan, Russia
country:        RU
admin-c:        KTTK-RIPE
tech-c:         KTTK-RIPE
status:         ASSIGNED PA
mnt-by:         TRANSTELECOM-MNT
created:        2023-06-02T15:31:08Z
last-modified:  2023-06-02T15:31:08Z
```

Figure 1: The intermediate proxy network is assigned to Sky Freight Limited, in Hasan, Russia.

We observed the adversary managing multiple C2 servers from the IP address 83[.]234[.]227[.]50. This IP connected to the latest C2 server, 94[.]131[.]9[.]32, between 17 January and 18 January via port 1245 and remains active at the time of writing this paper. Additionally, it has historically connected to 185[.]153[.]182[.]241 on ports 1224, 1245, 2248, 2252 (C2-specific ports) and 3389 (RDP) between 26 December and 16 January. It also established connections with 5[.]253[.]43[.]122 during the period of 26 December to 17 January over ports 1224, 1245 and 3389. Both servers were used in targeted campaigns linked to this operation.

The adversary accessed 185[.]153[.]182[.]241 via Remote Desktop Protocol (RDP) on several occasions, specifically on 30 December, 6 January and 10 January, maintaining an RDP session for 10 days. In the context of Operation 99, which

involved the C2 server 5[.]253[.]43[.]122, the adversary logged in via RDP more than a dozen times between 26 December and 15 January.

Based on this activity, we assess with high confidence that IP address 83[.]234[.]227[.]50 serves as an intermediate proxy controlled by the Lazarus group, given its connection to multiple distinct C2 servers.

Further analysis identified another IP, 83[.]234[.]227[.]49, from the same net-range connecting to a different Lazarus-controlled server (45[.]128[.]52[.]14) over ports 3389, 1224 and 1245 between 2 and 10 December. This C2 was hosted on Stark Industries infrastructure and exhibited activity similar to Operation 99, which was linked to attacks publicly reported in November 2024 involving Lazarus' presence on the *Codementor* platform.

Going deeper, we uncovered another Lazarus C2 server, 86[.]104[.]74[.]51, which was active throughout most of November 2024. This server, also hosted on Stark Industries infrastructure, resolved to the domain sageskills-uk[.]com in late September 2024, spoofing the legitimate entity skillsage.uk. The C2 server was accessed by the same intermediate proxy exit points hosted in Russia.

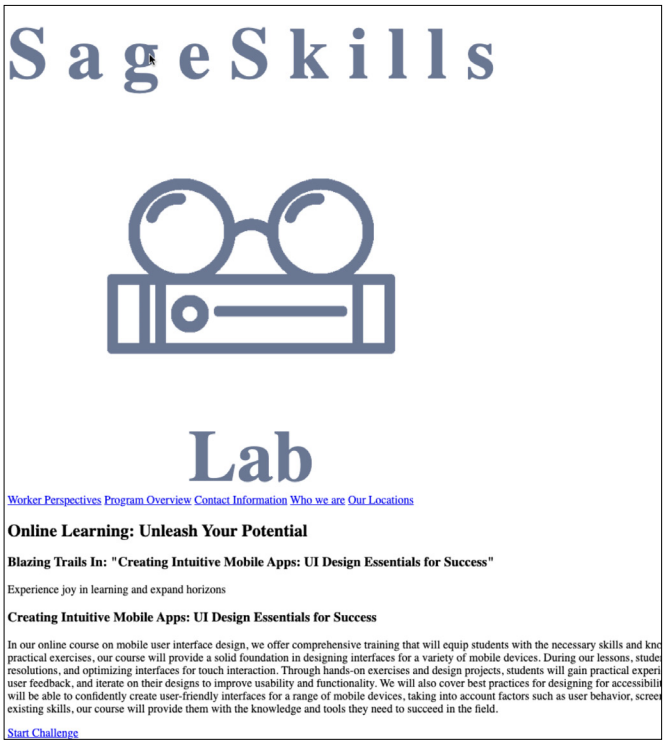

Figure 2: Archived landing page for adversary-controlled coding learning site.

The IP address 83[.]234[.]227[.]53 was observed connecting to the Sageskills website (a known Lazarus C2) on ports 1224, 1245 and 3389 on 8 and 29 November 2024. Additionally, the IP address 83[.]234[.]227[.]49 was seen connecting to the same server over the same ports between 7 and 11 November 2024.

INTERMEDIATE PROXIES

The source IPs observed connecting to the various C2s form a network of intermediate proxies designed to mask traffic. This layer leverages ISP proxies to obscure the true origin of the connections.

The IP address 83[.]234[.]227[.]50, observed connecting to the command-and-control server, appears to be linked to an *Oculus Proxy* endpoint. Similarly, 83[.]234[.]227[.]49 is also associated with *Oculus Proxy* infrastructure. The adversary is using 83.234.227.49 through 83.234.227.53 for this infrastructure, exclusively.

These findings suggest that the adversary is deliberately leveraging specific proxy endpoints within the *Oculus Proxy* network to further obscure their traffic. This tactic adds an additional layer of anonymity, complicating attribution and detection efforts, and demonstrates the adversary's strategic use of commercial proxy services to evade monitoring and ensure operational security.

ASTRILL VPN CONNECTIONS

We assess with high confidence that the IPs used to connect to the C2s were merely a relay/proxy and used to obfuscate the true origin. The adversary was establishing a secondary session after connecting to the VPN with the proxy, thus obscuring the true identity of where they actually connected from.

During the Sageskills attack, we observed a connection from an *Astrill* VPN IP address (70.39.70.196) to 83[.]234[.]227[.]53 between 1 and 6 November 1 2024. According to *VirusTotal*, the *Astrill* IP address is linked to the DPRK IT worker scheme, which at first seemed low confidence, but after analysis we can assess with high confidence that it is an exit point used by Lazarus.

In December, the same *Astrill* IP was observed connecting to 83[.]234[.]227[.]50, which had been seen communicating to the C2 servers. On 23 January 2025, another *Astrill* VPN IP address was seen connecting to the proxy 83[.]234[.]227[.]53, which, in turn, connected to the C2 94[.]131[.]9[.]32 on the same day. North Korea has used *Astrill* VPNs in the past, which have been identified in targeted IT worker schemes.

Tracing connections back to North Korea

North Korea appears to be using *Astrill* VPNs significantly from the net-range 175.45.176.0/22, which represents their only assigned address space. The following is the analysis of specific IPs involved in routing traffic through proxies in Russia to manage C2 infrastructure.

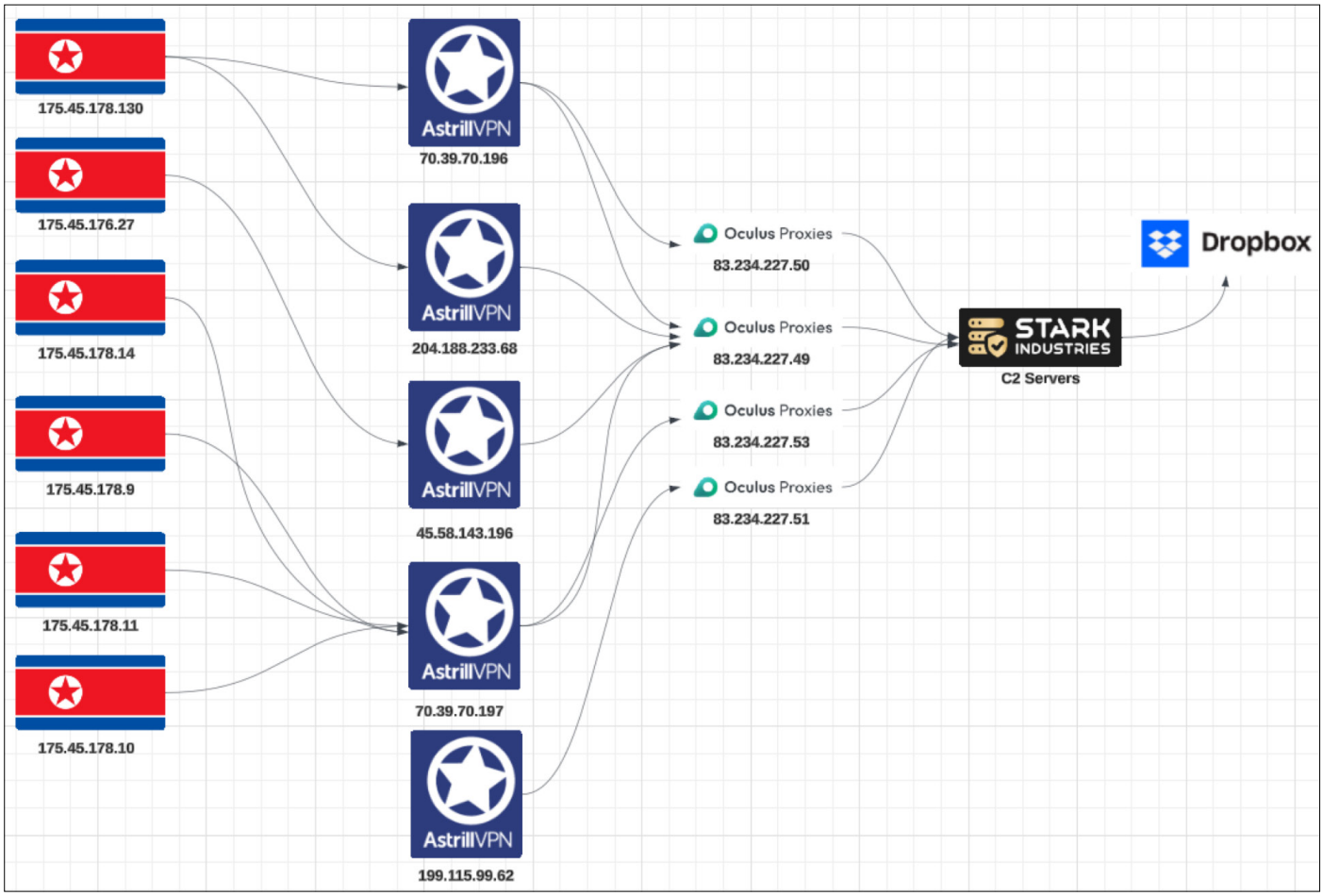

Figure 3: Operational infrastructure.

In December 2024, a North Korean IP address (175.45.178.130) was observed connecting to the *Astrill* VPN (70.39.70.196), aligning with the timeframe of the campaign's attacks and connections to the C2 servers. Notably, on 2 December 2024, the *Astrill* VPN established a connection to the proxy server at 83[.]234[.]227[.]49, immediately after the North Korean IP connected to the VPN. On the same day, the VPN then connected to the C2 server (5[.]253[.]43[.]122), establishing a clear chain of activity that ties the North Korean IP, VPN, proxy, and C2 server together, identifying the North Korean IP as the true source of the traffic.

These findings underscore the coordination of the campaign's infrastructure and provide direct evidence of the North Korean IP's involvement in initiating the activity. The temporal alignment of connections – from the North Korean IP to the VPN, through the proxy, and finally to the C2 server – highlights the deliberate use of obfuscation layers to conceal the origin of the traffic while maintaining operational efficiency. This connectivity pattern strengthens attribution to North Korean state actors and demonstrates the sophistication of their tactics.

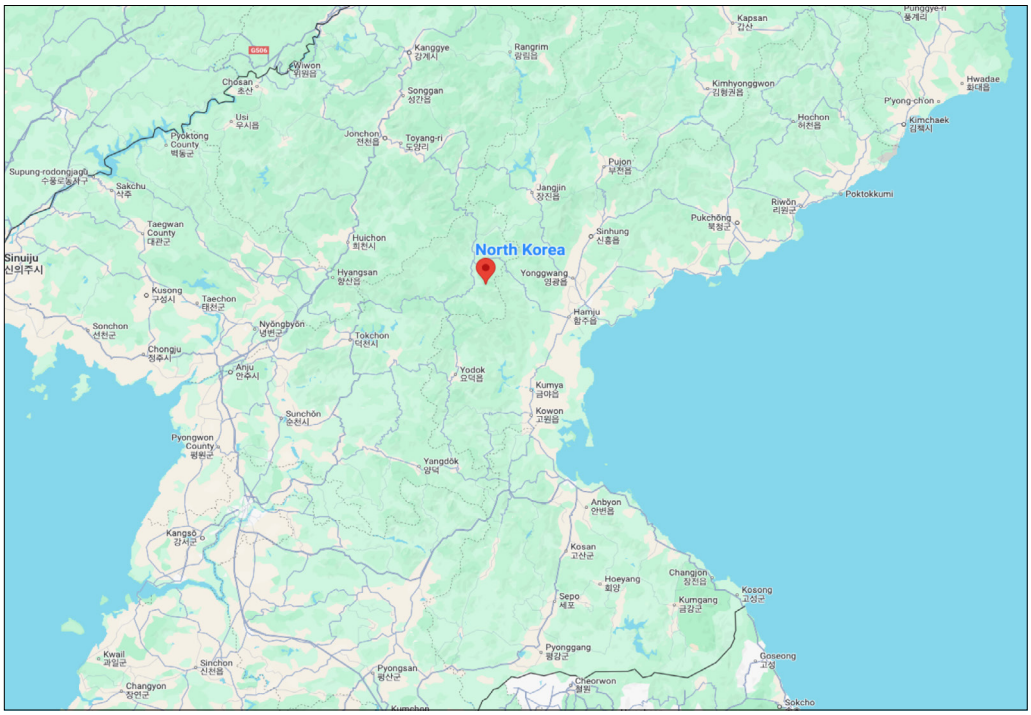

Figure 4: Approximate source origin in North Korea.

OPERATIONAL INFRASTRUCTURE TEMPORAL ANALYSIS

The observed campaign, attributed to North Korean actors, reveals the use of proxies as key facilitators for managing command-and-control servers from November 2024 to January 2025. Attackers employed proxies such as 83.234.227.49, 83.234.227.53 and 83.234.227.51 to route and manage connections to multiple C2 servers, ensuring obfuscation of attacker-originated traffic. These proxies served as intermediaries, shielding the attackers' infrastructure and providing an additional layer of anonymity. The campaign involved direct ties to North Korean IPs, including 175.45.178.130, 175.45.178.14 and 175.45.178.10, suggesting either that the operations were routed through North Korean assets (unlikely, as it's a closed country and closed network) or that they were coordinated directly from within the country. The simultaneous use of multiple proxies for managing distinct C2 servers reflects an advanced understanding of operational security and network management.

The activity peaked in December 2024, with a heightened level of proxy usage to facilitate communication with C2 infrastructure, including servers at 185.153.182.241, 86.104.74.51 and 5.253.43.122. The usage of *Astrill* VPN IPs, such as 70.39.70.196 and 45.58.143.196, further complicated attribution and detection by masking the origin of the connections.

The attackers' strategy of overlapping timelines, managing C2s through geographically distributed proxies, and leveraging secure VPN channels showcases a sophisticated campaign aimed at ensuring resilience and minimizing detection. The deliberate routing of communications through managed proxies highlights the attackers' focus on maintaining control over their infrastructure while evading defensive measures.

DROPBOX DATA EXFILTRATION

Throughout the December campaign, we observed the C2 server at 185.153.182.241 repeatedly connecting to multiple *Dropbox* IPs. We assess with high confidence that this activity likely indicates the adversary transferring stolen data to a *Dropbox* location. These connections occurred with the C2 acting as the client between 4 and 30 December 2024, with a total connection time of 5 hours and 14 minutes. A similar pattern was observed with the C2 server 5.253.43.122, which established connections between 16 and 26 December 2024. This behaviour also appeared during the November campaign, involving the C2 server at 86.104.74.51, which connected to *Dropbox* IPs from 8 to 30 November 2024. Additionally, the same pattern re-emerged during the January campaign, with connections to *Dropbox* IPs occurring between 17 and 24 January 2025.

November campaign

The campaign in November 2024 had 181 unique victims connecting to the C2 (86.104.74.51), spread around the world. Based on the above analysis and the role of intermediate proxies, the adversary was managing the server through the proxies 83.234.227.53 and 83.234.227.49 via ports 1245 and 3389.

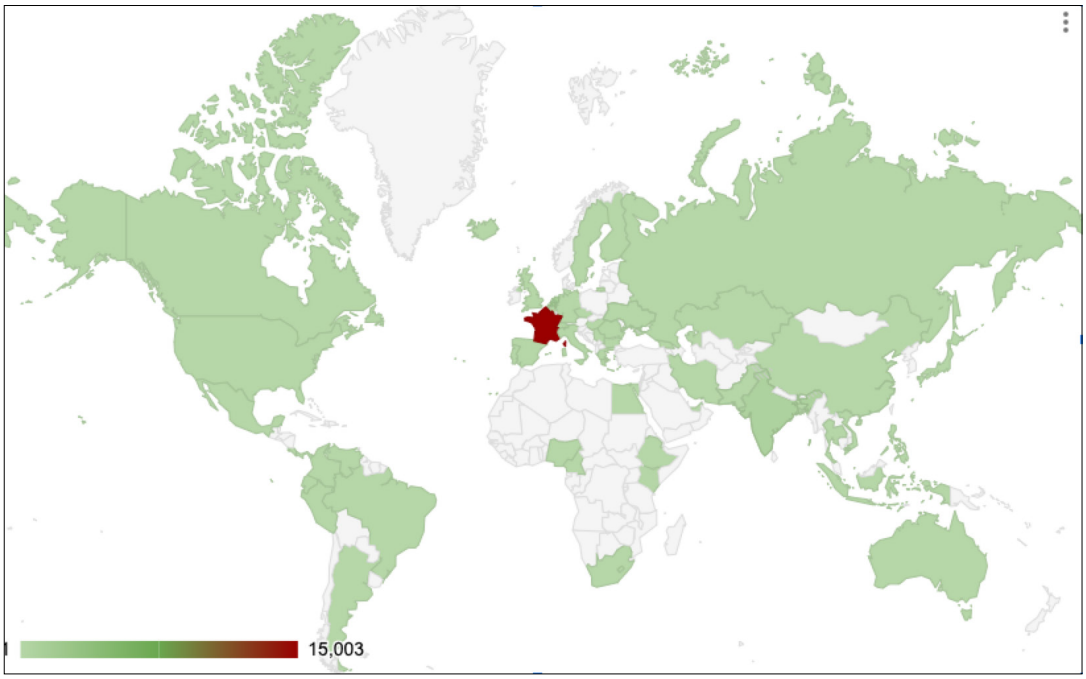

Figure 5: Victims from November 2024 campaign (connections made to C2).

December campaigns

Campaigns in December 2024 indicated 1,225 unique victims across three C2 servers (185.153.182.241, 45.128.52.14 and 86.104.74.51). Brazil (32 unique IPs) and India (284 unique IPs) were the countries with the most traffic to the C2s.

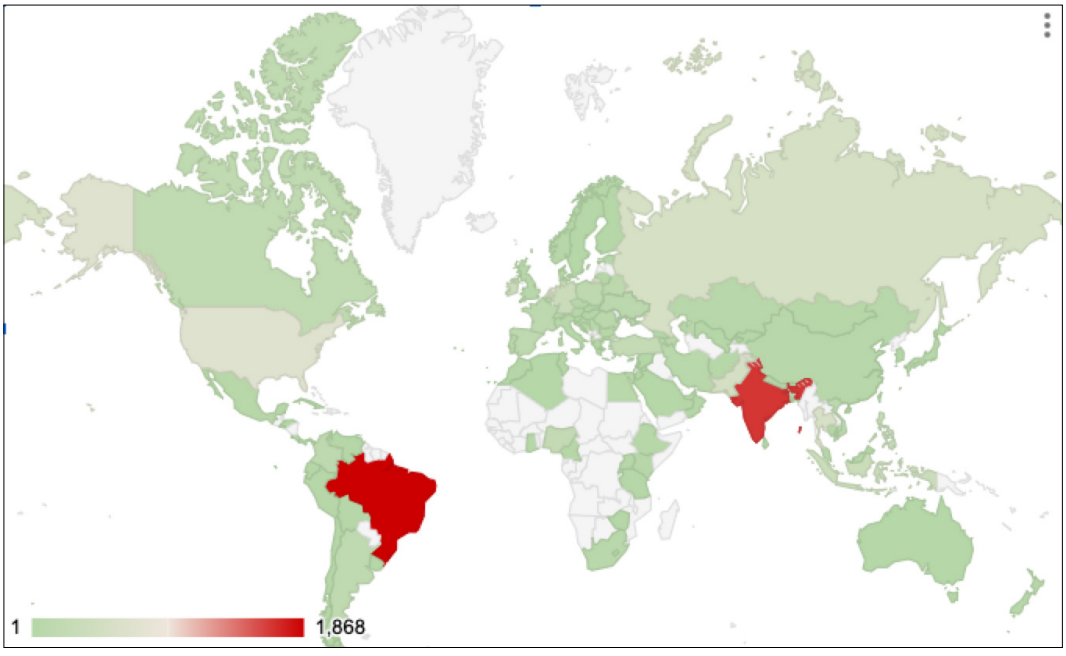

Figure 6: Victims from December 2024 campaign (connections made to C2).

January campaign analysis

The recently established C2 server (94.131.9.32) received traffic originating from 175.45.178.11 and 175.45.178.10, routed through multiple layers of obfuscation. Notably, traffic from 175.45.178.11 was consistently routed throughout January 2025, flowing through the *Astrill* VPN exit points (70.39.70.196, 70.39.70.197) and the proxy (83.234.227.53) before reaching its destination. Activity involving 94.131.9.32 peaked between 21 and 23 January 2025, as significant traffic flowed to the server via these proxies. There were 233 unique victims as part of this recent campaign, communicating over port 1224. India was the most heavily impacted country, with 110 unique victims during the course of the campaign.

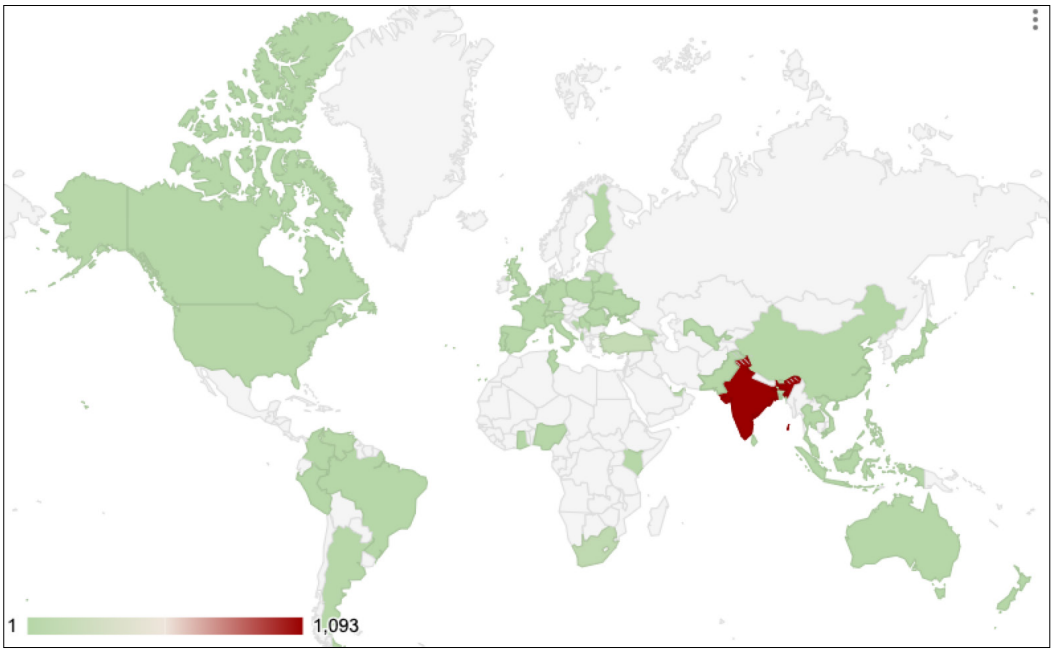

Figure 7: Victims from January 2025 campaign (connections made to C2).

The adversary set up an additional server (94.232.247.192), also hosted at Stark Industries, which the proxy 83.234.227.53 connected to on 23 January 2025. At the time of writing this paper, this server is no longer online. Another proxy, 83.234.227.52, established connections on ports 1224 and 3389 between 21 and 22 January 2025. This campaign was short-lived, with 87 total unique victims communicating to this server and India being the hardest hit area.

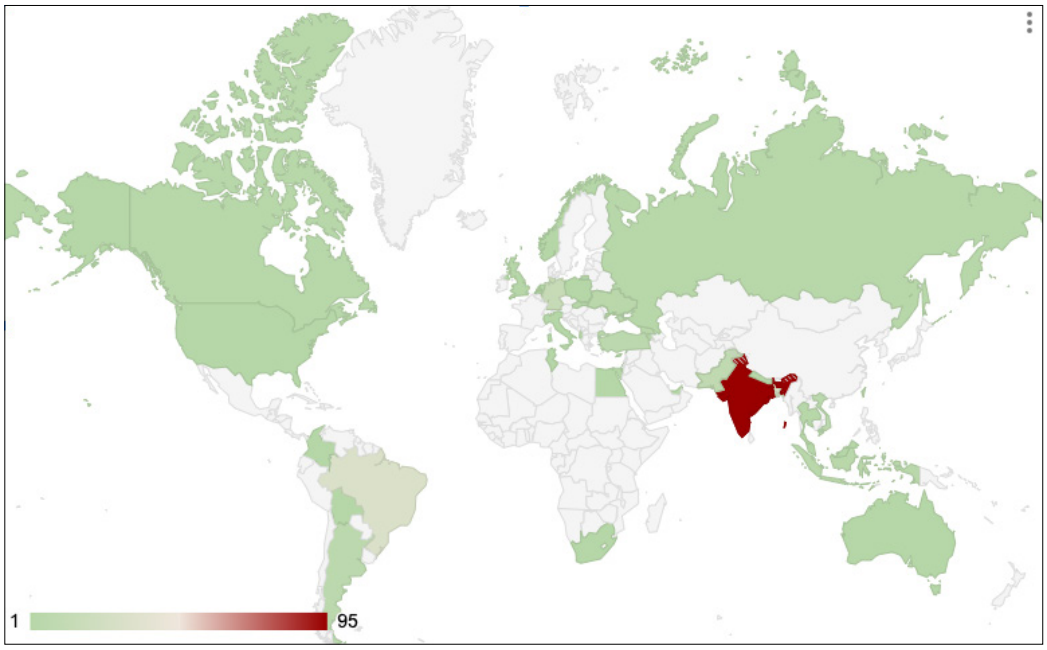

Figure 8: Victims from January 2025 campaign (connections made to C2).

C2 OPERATIONAL INFRASTRUCTURE

Much of the analysis so far has focused on the attackers' operational infrastructure and attribution to Pyongyang. However, one aspect that remains unexplored is the role of port 1245 in these campaigns. It is evident that the proxy servers connect over port 1245, suggesting they may be managing certain operations. Our investigation uncovered that, beyond payloads and downloaders, the C2 servers also hosted a 'hidden' web-admin panel. Upon examination, this web-admin portal was found to operate on port 1245 and displayed a login page requiring authentication to access the backend. This panel, hosted on the C2 servers, appears to facilitate the display of exfiltrated data from victims and provides attackers with the ability to search and filter the information.

The panel seems to be custom-built and specifically deployed on the C2 servers. Analysis of traffic patterns suggests that the adversary accesses the information using *Astrill* VPNs and through proxy connections.

Figure 9: React web-admin login.

Further investigation of the server revealed valuable insights into its functionality and the operator's interface. Our findings showed that the application is built on Node.js and exposes multiple API endpoints, potentially offering additional critical information. Analysing the Config.js file provided details about the available API endpoints and the specific pages accessible to the operator.

```
const api = {
    api_url : "http://94.131.9.32:1224/",
    // api_url : "http://localhost:1224/",
    login_path : "login",
    get_info : "info",
    get_allinfo: "allinfo",
    restart_server : "rSvr",
    dmup_db : "dumpsql",
    get_userInfo: "getUser",
    edit_userInfo: "editUser",
    add_user: "addUser",
    remove_user: "removeUser",
    expiredTime: 3600,
};
export default api;
```

Figure 10: Config.js.

Another file, App.js, revealed more detailed information about specific pages that would be accessible to the operator. An extraction from this file shows specific page paths that are hidden behind a login wall.

```
/* Layout CSS */
import "./assets/css/layout.css"
import "./assets/css/font-awesome.min.css"
/* Components PC Pages ------------------------------------------*/
import Login from "./pages/Login/login";
import Info from "./pages/Info/info";
import AllInfo from "./pages/AllInfo/allinfo";
import UserInfo from "./pages/User/userInfo";
import EditUser from "./pages/User/edit";
import AddUser from "./pages/User/add";
import { AppContext } from './AppContext';
```

Figure 11: App.js.

Info

The info page offers details about victims, although the actual backend data could not be displayed. By examining the files, we can determine its true functionality. A static analysis of the JavaScript files reveals that the server retrieves victim-uploaded data from the backend. This includes exfiltrated information such as PC names, URLs, passwords, and more. Furthermore, it displays data extracted from implants interacting with the /keys API endpoint.

```
class info extends Component {
    constructor(props) {
        super(props);
        this.state = {
            keyDataHeader : [
                { name : 'Name', field : 'name', sortable : true },
                { name : 'Type', field : 'type', sortable : true },
                { name : 'Time', field : 'time', sortable : true }
            ],
            keyData : [],
            uploadDataHeader : [
                { name : 'PC_name', field : 'pc_name', sortable : false },
                { name : 'URL', field : 'url', sortable : true },
                { name : 'Username', field : 'username', sortable : true },
                { name : 'Password', field : 'userpwd', sortable : false },
                { name : 'Browser', field : 'browser', sortable : true },
                { name : 'created', field : 'created_time', sortable : true },
                { name : 'last', field : 'last_time', sortable : true }
            ],
            uploadData : [],
            OkeyData : [],
            OuploadData : [],
            currentPane : 'keys',
            keysnum : 5,
            uploadsnum:100,
            is_loaded:false,
        }
    }
```

Figure 12: Info.js.

The data sent from the payload will be displayed in the backend within the keys table.

```
{
    'ts': str(B),          # A timestamp in milliseconds.
    'type': sType,         # An identifier (hardcoded as "99").
    'hid': hn,             # Hostname of the system, potentially modified.
    'ss': 'sys_info',      # A label indicating system information.
    'cc': str(A.sys_info) # Serialized system and network info.
}
```

Figure 13: Data sent from the payload.

ANALYSIS OF COMPETING HYPOTHESES (ACH)

The Analysis of Competing Hypotheses (ACH) is a systematic methodology designed to evaluate multiple possible explanations for a given issue or situation. Originally developed by the CIA, ACH aids analysts in organizing evidence, identifying biases, and methodically comparing competing hypotheses to determine the most likely conclusion.

Hypotheses

- **H1**: The campaign is led by the Lazarus Group (North Korean APT) and directly involves North Korea.
- **H2**: The campaign is executed by a non-state actor or criminal group attempting to impersonate Lazarus to obscure attribution.
- **H3**: The operation involves collaboration among multiple state or non-state actors, with Lazarus playing a partial or indirect role.
- **H4**: The campaign is entirely unrelated to Lazarus and is being misattributed due to similar TTPs.

Analysis

- **H1 (Lazarus Group involvement)**: Most of the evidence strongly supports this hypothesis, including direct links to North Korean IPs, Lazarus's known TTPs, infrastructure usage, and targeting patterns. Our investigation aligns closely with this attribution.
- **H2 (non-state actor impersonation)**: While possible, the campaign's sophistication, scale, and alignment with Lazarus's historical operations make this scenario less credible. Evidence such as ties to Pyongyang IPs and *Astrill* VPN activity further undermines this hypothesis.
- **H3 (collaborative effort)**: Although this hypothesis accounts for the operation's complexity, there is no compelling evidence to suggest collaboration beyond Lazarus. The observed infrastructure and techniques indicate a centralized effort consistent with the group's capabilities.
- **H4 (misattribution)**: The majority of the evidence directly implicates Lazarus, making misattribution highly unlikely. While some techniques (e.g. supply chain attacks) could theoretically be replicated, the clear link to Pyongyang IPs and *Astrill* VPN usage strongly counters this hypothesis.

Conclusions

- **Most likely hypothesis**: H1 – The campaign is orchestrated by the Lazarus Group (North Korean APT).
- **Confidence Level**: High.

CONCLUSION

Operation Phantom Circuit has exposed a highly sophisticated global campaign by Lazarus, targeting the cryptocurrency industry and software developers through supply chain attacks. By embedding obfuscated backdoors into legitimate software packages, Lazarus deceived users into executing compromised applications, enabling them to exfiltrate sensitive data and manage victims through command-and-control servers over port 1224. The campaign's infrastructure leveraged hidden React-based web-admin panels and Node.js APIs for centralized management of stolen data, affecting over 233 victims worldwide. This exfiltrated data was traced back to Pyongyang, North Korea, through a layered network of *Astrill* VPNs and intermediate proxies.

This operation underscores an urgent call to action for organizations and developers to strengthen their supply chain security by implementing rigorous code verification processes and network traffic monitoring. Security teams must collaborate globally to share threat intelligence and stay ahead of Lazarus's evolving tactics, which leverage modern web technologies and advanced obfuscation techniques. Industries, particularly those at high risk like cryptocurrency, must prioritize adopting robust monitoring tools, enforcing patch management, and deploying proactive defences to mitigate future attacks from advanced threat actors. The time to act is now – failing to address these vulnerabilities leaves critical systems and data exposed to similar campaigns.