Operation Phantom Circuit: North Korea’s Global Data Exfiltration Campaign

securityscorecard.com/blog/operation-phantom-circuit-north-koreas-global-data-exfiltration-campaign/

In December 2024, a routine software update concealed a global threat. Attackers from the Lazarus Group, based in North Korea, infiltrated trusted development tools, compromising hundreds of victims worldwide. This sophisticated campaign, code-named “Phantom Circuit,” targeted cryptocurrency and technology developers, employing advanced obfuscation techniques through proxy servers in Hasan, Russia.

STRIKE’s investigation of ‘Phantom Circuit’ revealed a critical shift in Lazarus Group tactics: embedding malware directly into trusted applications. “This approach allows widespread impact and long-term access while evading detection,” explains Ryan Sherstobitoff, Senior Vice President of Research and Threat Intelligence at STRIKE.

Investigation

STRIKE’s investigation began with Operation 99, uncovering the Lazarus Group’s use of command-and-control (C2) servers. These servers, active since September 2024, formed the backbone of an elaborate infrastructure to manage and exfiltrate stolen data, which we discovered based on our analysis of netflow data provided by Team Cymru in combination with SecurityScorecard STRIKE team threat intelligence data feeds.

Campaign Start Date	September 2024
Primary Function	Communication with infected systems over **port 1224**
Hidden Layer	Administrative platform accessible via **port 1245**, featuring a hidden React web application and Node.js API.
Purpose	Remotely organize and manage stolen data globally.
Infrastructure Sophistication	Demonstrated advanced planning and technical expertise, surpassing typical expectations for cybercriminal operations.

“These servers included a complete administrative platform for managing compromised systems worldwide,” Sherstobitoff explains. “This infrastructure demonstrated a level of planning and sophistication that surpassed expectations.”

Read the full report here

Infrastructure and Operation

The Lazarus Group employed a network of servers and tools to conduct this operation. Their infrastructure featured command-and-control servers, spoofed domains, and persistent remote management sessions. By embedding malware into trusted development tools, the attackers ensured widespread compromise while maintaining stealth.

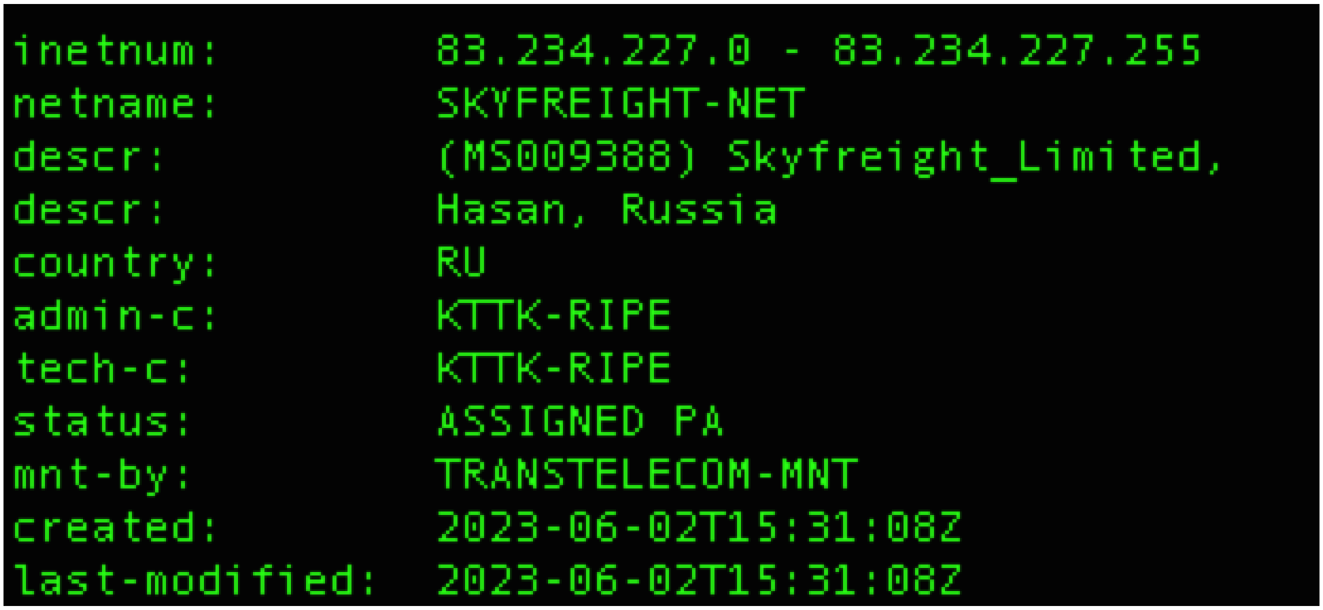
STRIKE documented several key C2 servers central to the operation. Their role was serving payloads and collecting data from victims

Server IP	Active Period	Role
94.131.9.32	**January 2025**	**Latest command-and-control (C2) server.**
185.153.182.241	**Dec 2024**	**December Campaigns**
86.104.74.51	**November 2024**	**Spoofed domain: sageskills-uk[.]com.**
5.253.43.122	**December 2024**	**December Campaigns**

The Evidence Chain

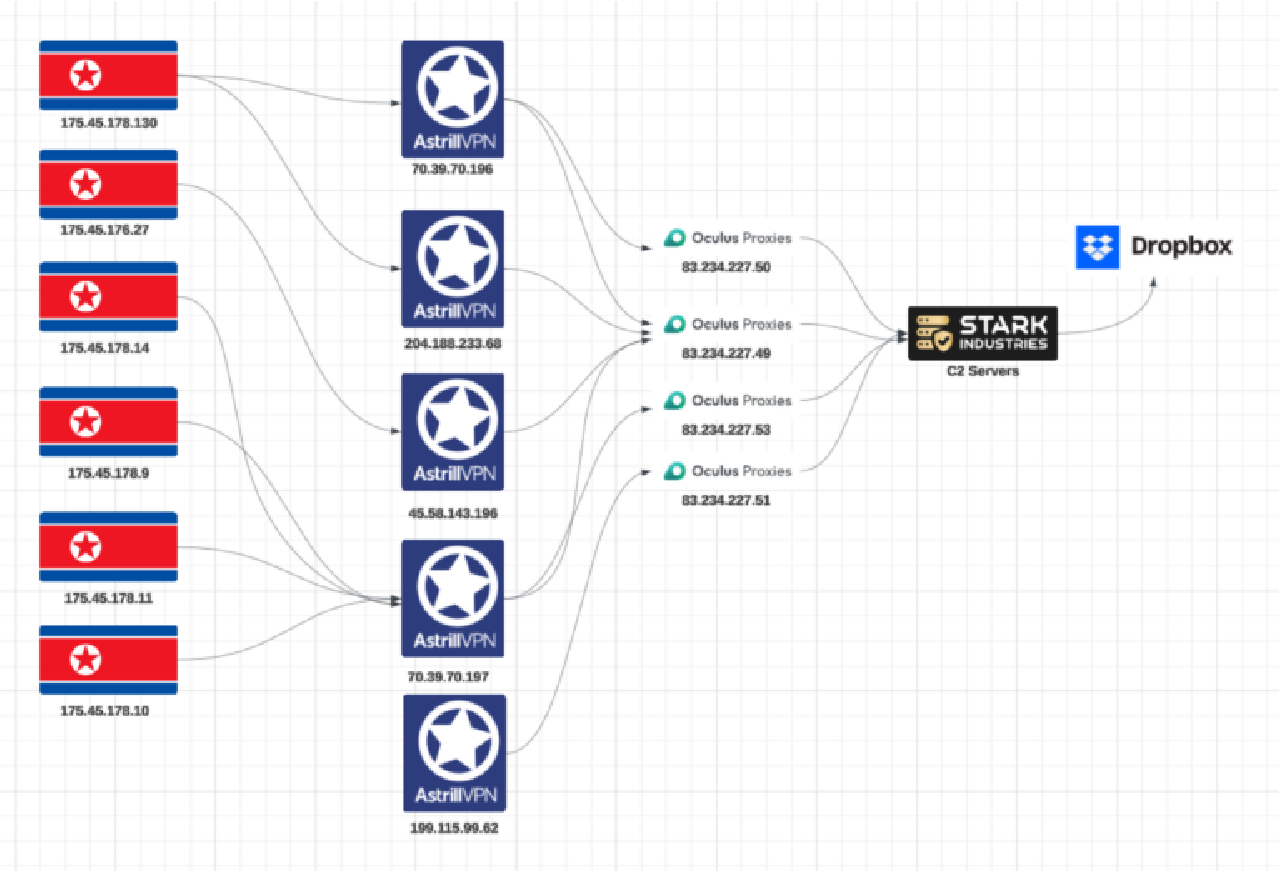
STRIKE observed a layered infrastructure in the operation, with traffic originating from North Korean IP addresses and passing through a network of VPNs and proxies. These connections routed traffic through Oculus Proxy nodes in Hasan, Russia, before reaching command-and-control servers. This deliberate design ensured anonymity and evasion at every step.

1. **Initial Connection**: North Korean IP addresses, including **175.45.178.130**, **175.45.176.27**, **175.45.178.14**, **175.45.178.9**, **175.45.178.11**, and **175.45.178.10**, were the starting points of the operation.
2. **VPN Obfuscation**: These IPs connected to **Astrill VPN endpoints**, including **70.39.70.196**, **204.188.233.68**, **45.58.143.196**, **70.39.70.197**, and **199.115.99.62**, to hide their true origin.
3. **Proxy Relay**: Traffic was routed through the **Oculus Proxy network**, specifically IPs **83.234.227.49**, **83.234.227.50**, **83.234.227.51**, and **83.234.227.53**, registered to Sky Freight Limited in Hasan, Russia. These proxies served as an additional layer of anonymity.
4. **Command and Control Servers**: The proxied connections ultimately reached the **C2 infrastructure** hosted on **Stark Industries** servers. These servers handled communications with compromised systems and managed exfiltrated data.
5. **Data Exfiltration to Dropbox**: From the C2 servers, stolen data was uploaded to **Dropbox**, where the attackers stored and organized the exfiltrated information for further use.

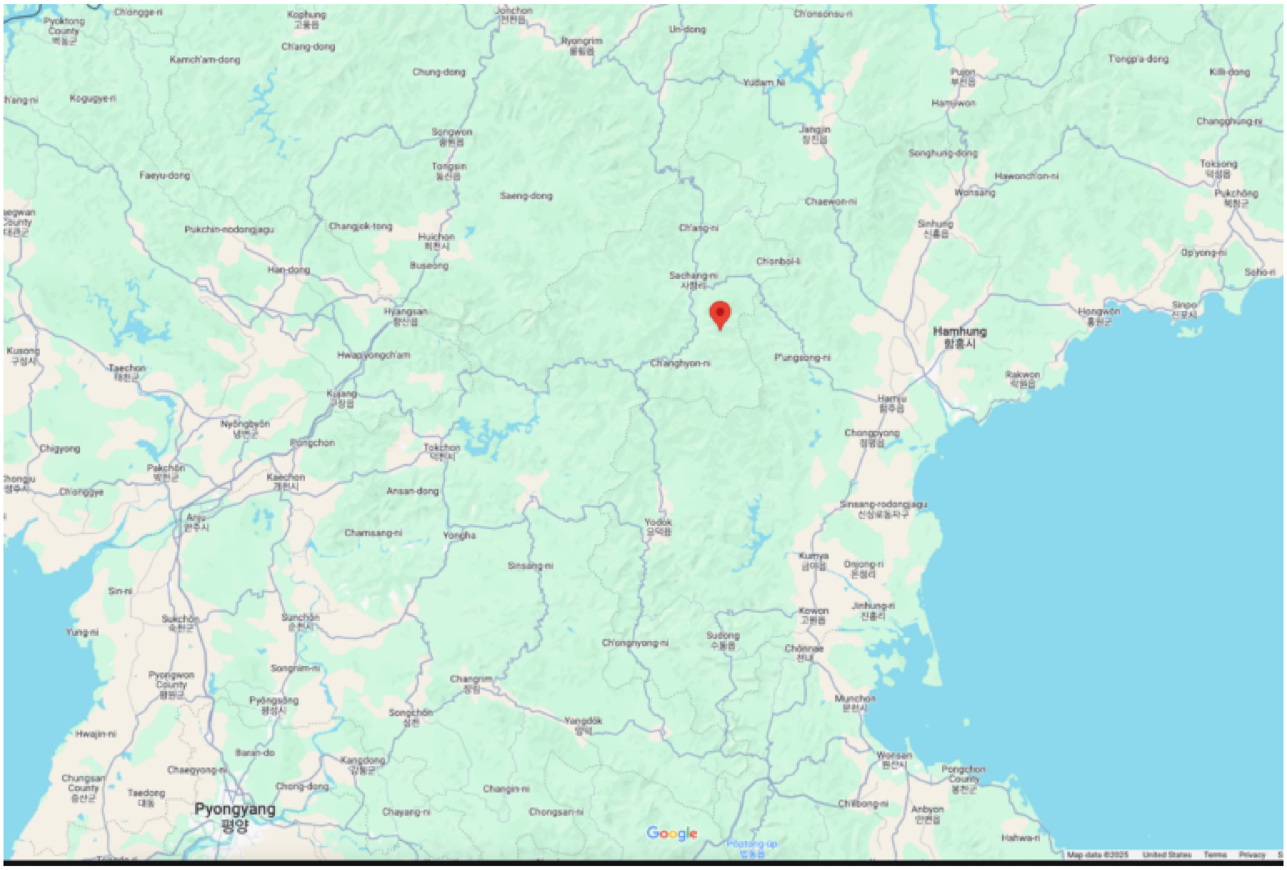


```
inetnum:          83.234.227.0 - 83.234.227.255
netname:          SKYFREIGHT-NET
descr:            (MS009388) Skyfreight_Limited,
descr:            Hasan, Russia
country:          RU
admin-c:          KTTK-RIPE
tech-c:           KTTK-RIPE
status:           ASSIGNED PA
mnt-by:           TRANSTELECOM-MNT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

This meticulously designed infrastructure allowed the Lazarus Group to maintain persistent access, evade detection, and securely exfiltrate sensitive information while concealing their operations at every step.



This pattern repeated consistently, demonstrating a deliberate and structured approach to obfuscating the attackers' true origin. Persistent RDP sessions, some lasting up to 10 days, allowed attackers to maintain direct access to compromised systems, posing significant risks to data integrity and system recovery.

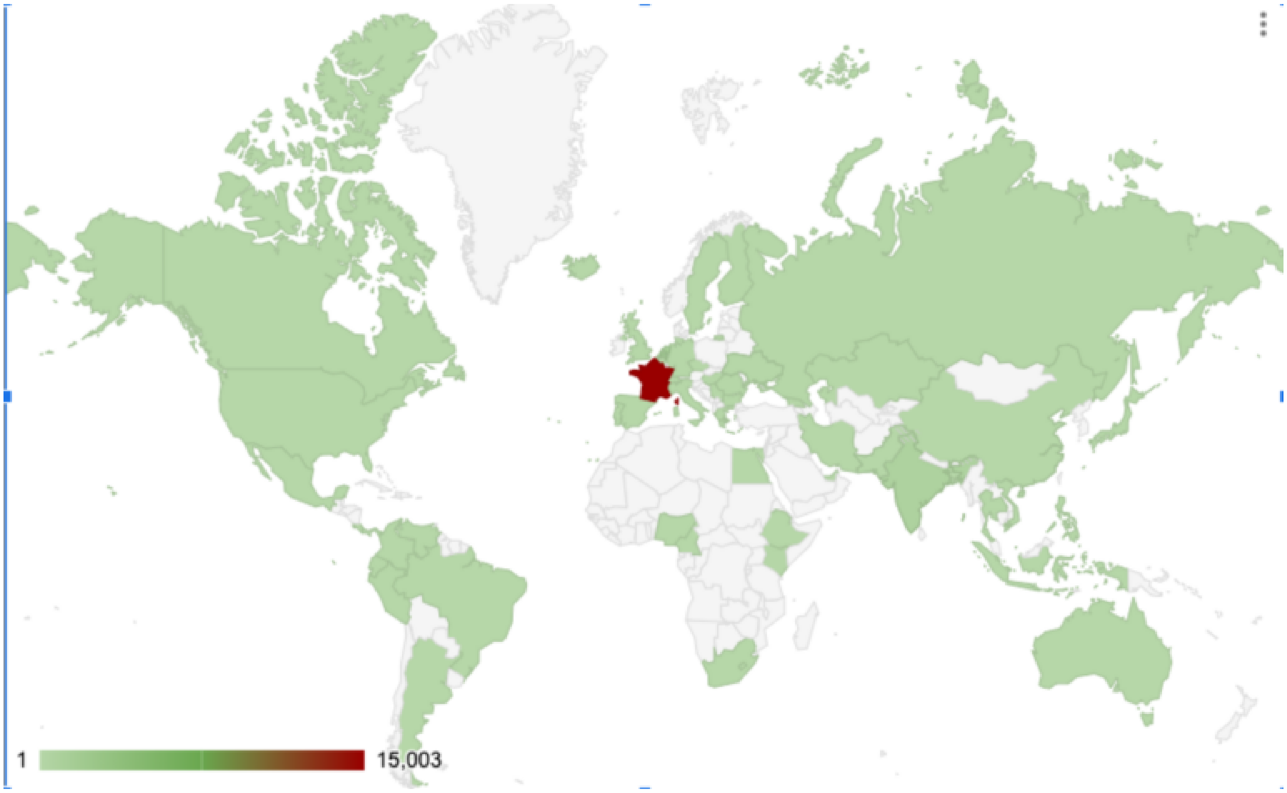


The Scale of Compromise

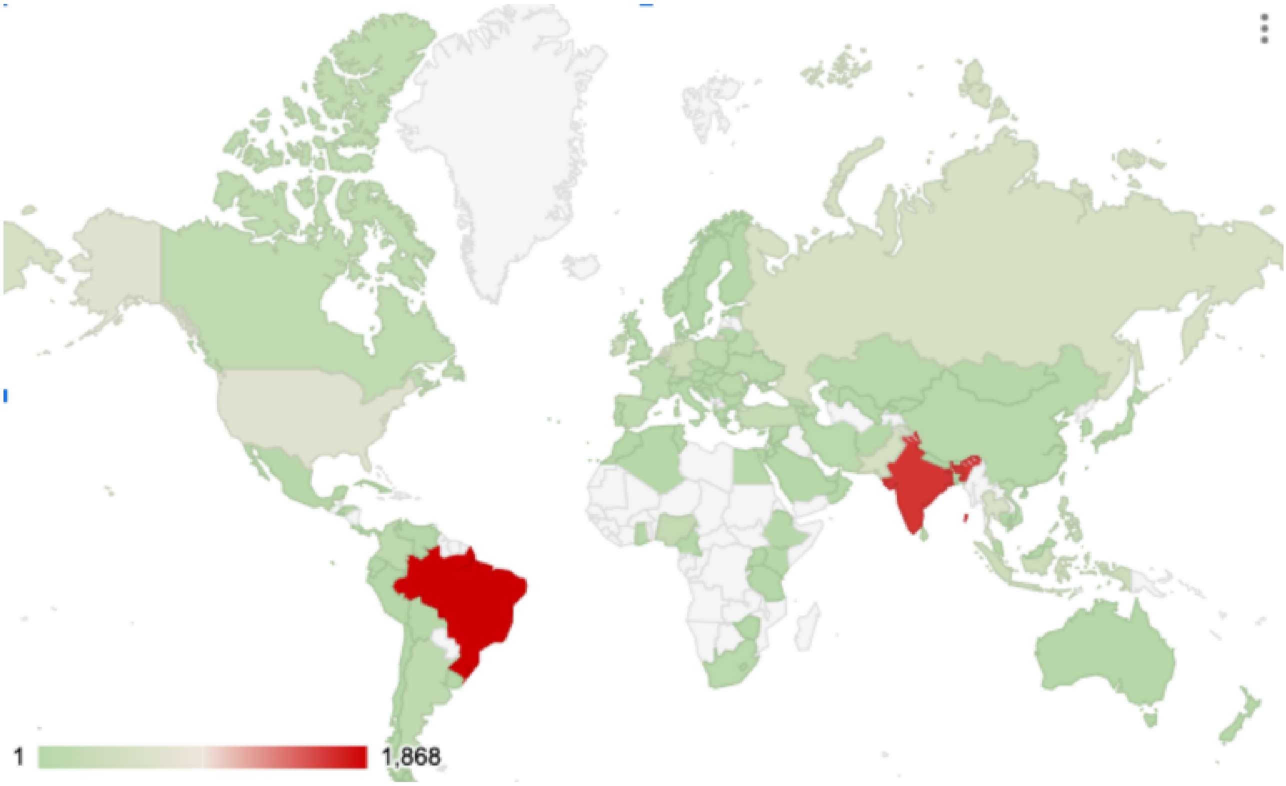
Operation Phantom Circuit unfolded in three waves, compromising over 1,500 systems worldwide:

- **November 2024**: Targeted 181 developers, primarily in European technology sectors.
- **December 2024**: Expanded to hundreds of developers globally, with major hotspots in India (284 victims) and Brazil (32 victims).
- **January 2025**: Added 233 more victims, including 110 systems in India’s technology sector alone.

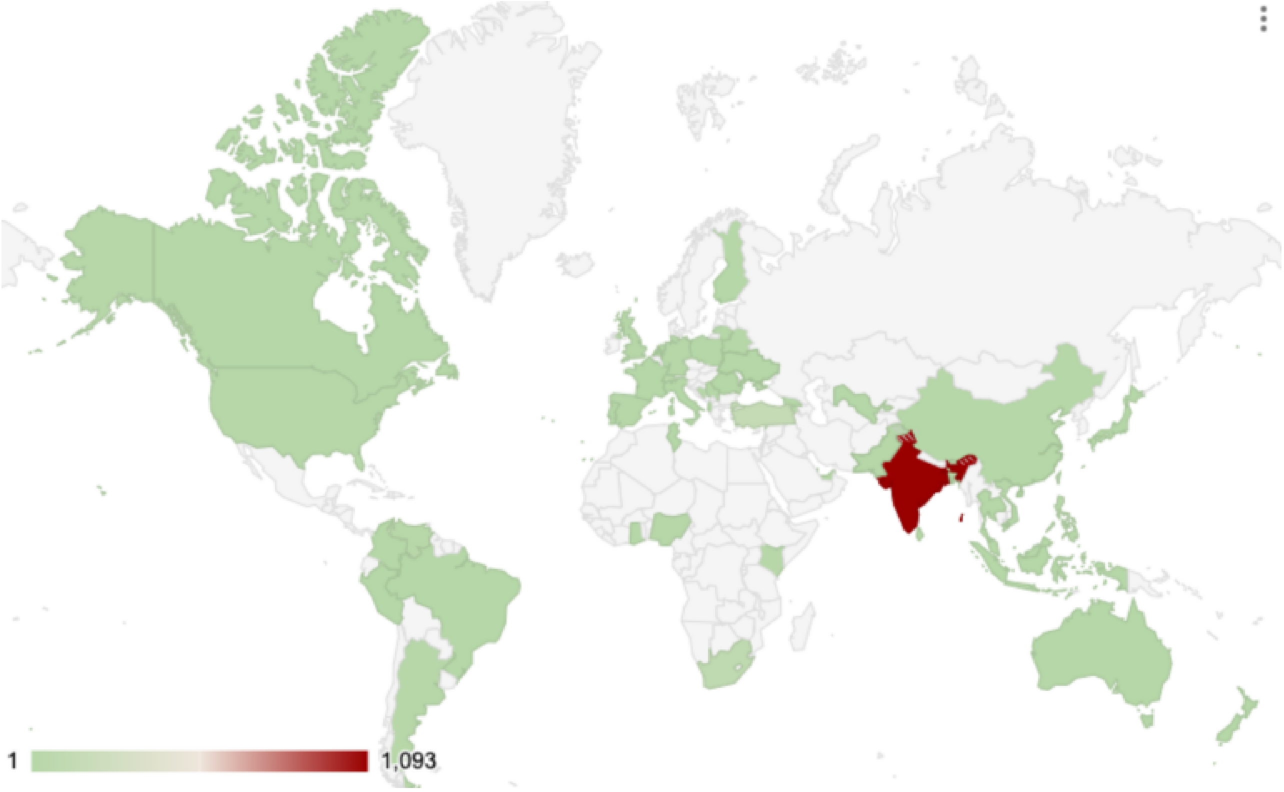
The attackers exfiltrated critical data, including development credentials, authentication tokens, browser-stored passwords, and system information. Once collected by the C2 servers, the data was transferred to Dropbox, where it was organized and stored. Persistent connections to Dropbox highlighted the attackers’ systematic approach, with some servers maintaining active sessions for over five hours.



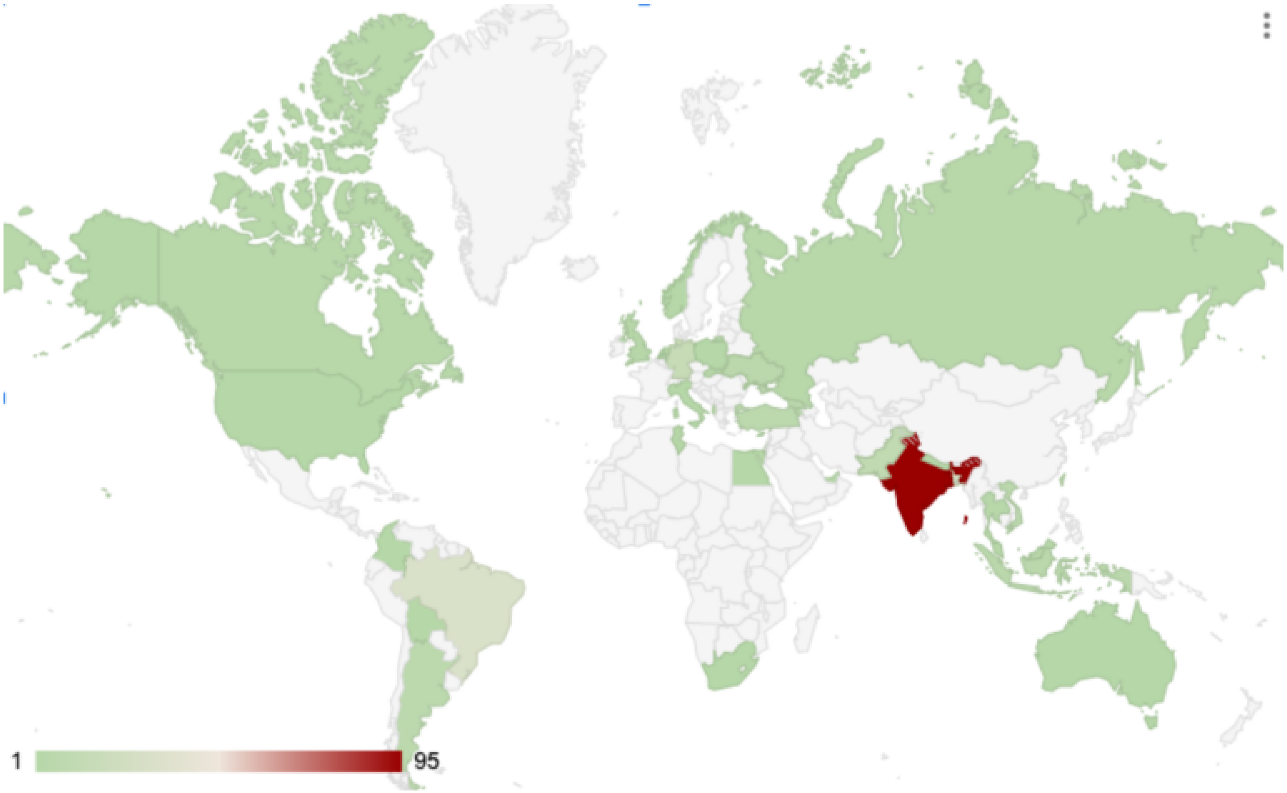
Victims from November 2024 campaign (connections made to c2)



Victims from December 2024 campaign (connections made to c02)



Victims from January 2025 campaign (connections made to co2)



Victims from January 2025 campaign (connections made to co2)

Inside the Attack Infrastructure

The Lazarus Group’s administrative platform showcased their advanced capabilities in managing stolen data. This custom-built panel was designed to search, filter, and organize exfiltrated information with precision, emphasizing efficiency and control.

Key Features of the Platform:

- System Tracking: Monitoring device details, including PC names, operating systems, and configurations.
- Credential Management: Collecting URLs, browser-stored credentials, and authentication tokens for exploitation.
- Activity Logs: Tracking timestamps for victim interactions to streamline operations.

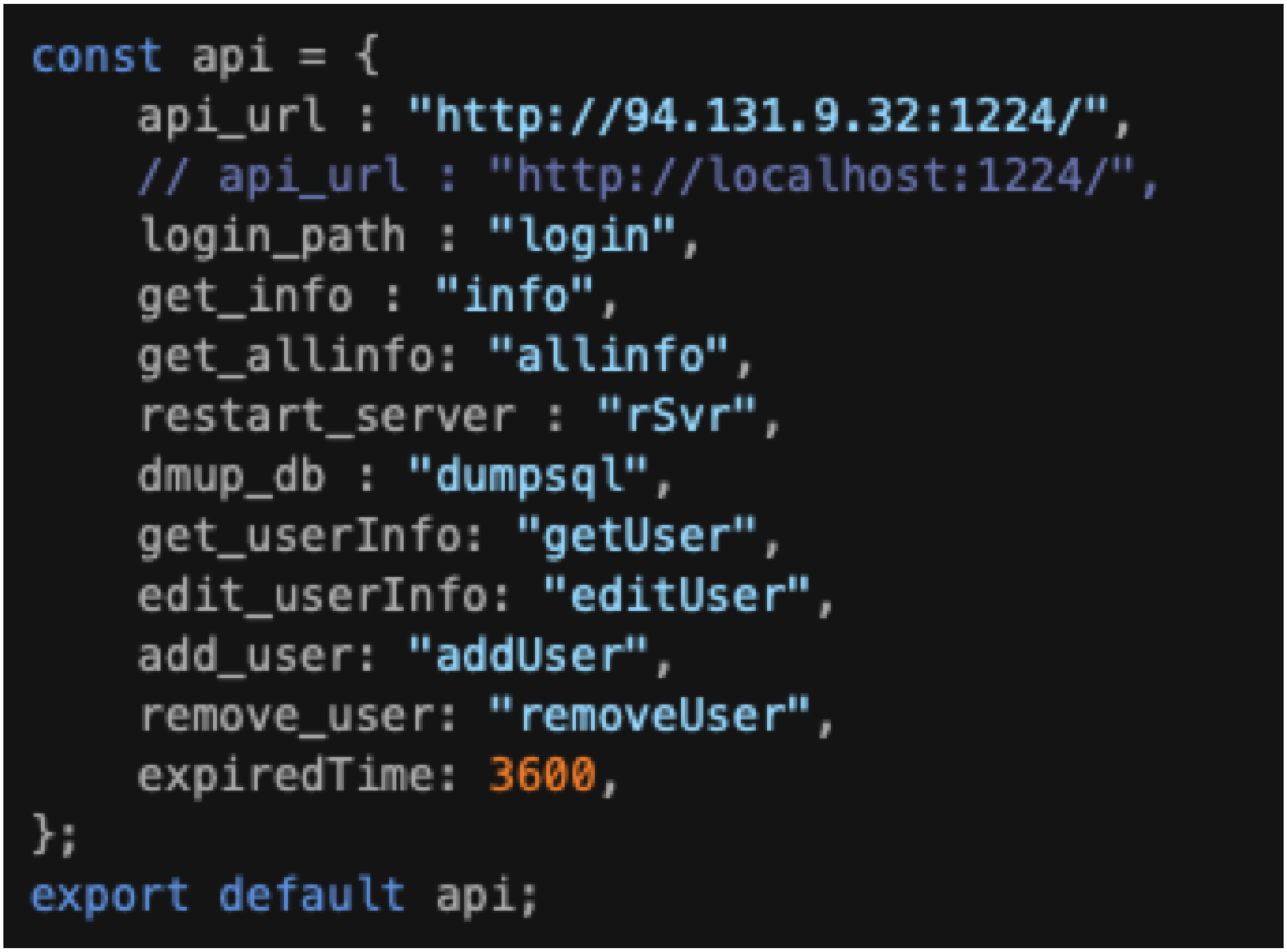
STRIKE’s analysis revealed that the administrative platform was a robust system powered by modern frameworks. The backend, built on Node.js, exposed multiple API endpoints that provided granular operational control. Static analysis of files such as Config.js and App.js revealed the attackers’ ability to interact with these endpoints and manage stolen data systematically.

Modern Infrastructure Design

The use of React and Node.js demonstrated the Lazarus Group’s shift toward scalable, modern attack infrastructures. This integration of advanced management tools into their command-and-control (C2) servers highlighted a high level of planning and technical expertise.

Application Structure

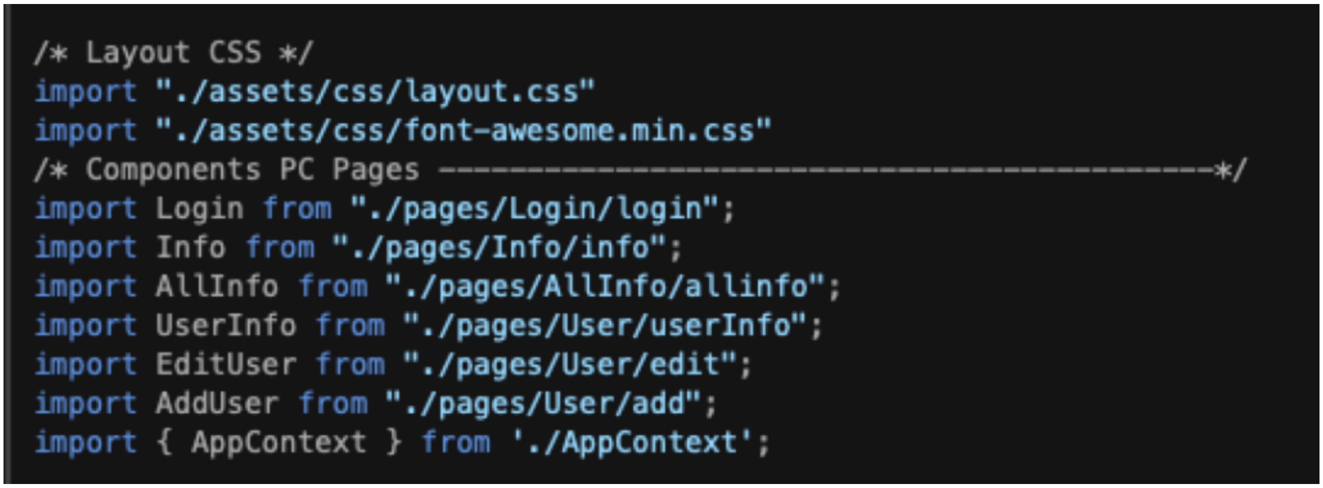
A closer examination of the platform’s structure uncovered several layers of functionality:



```
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;
```

Hidden Pages and Access Points:

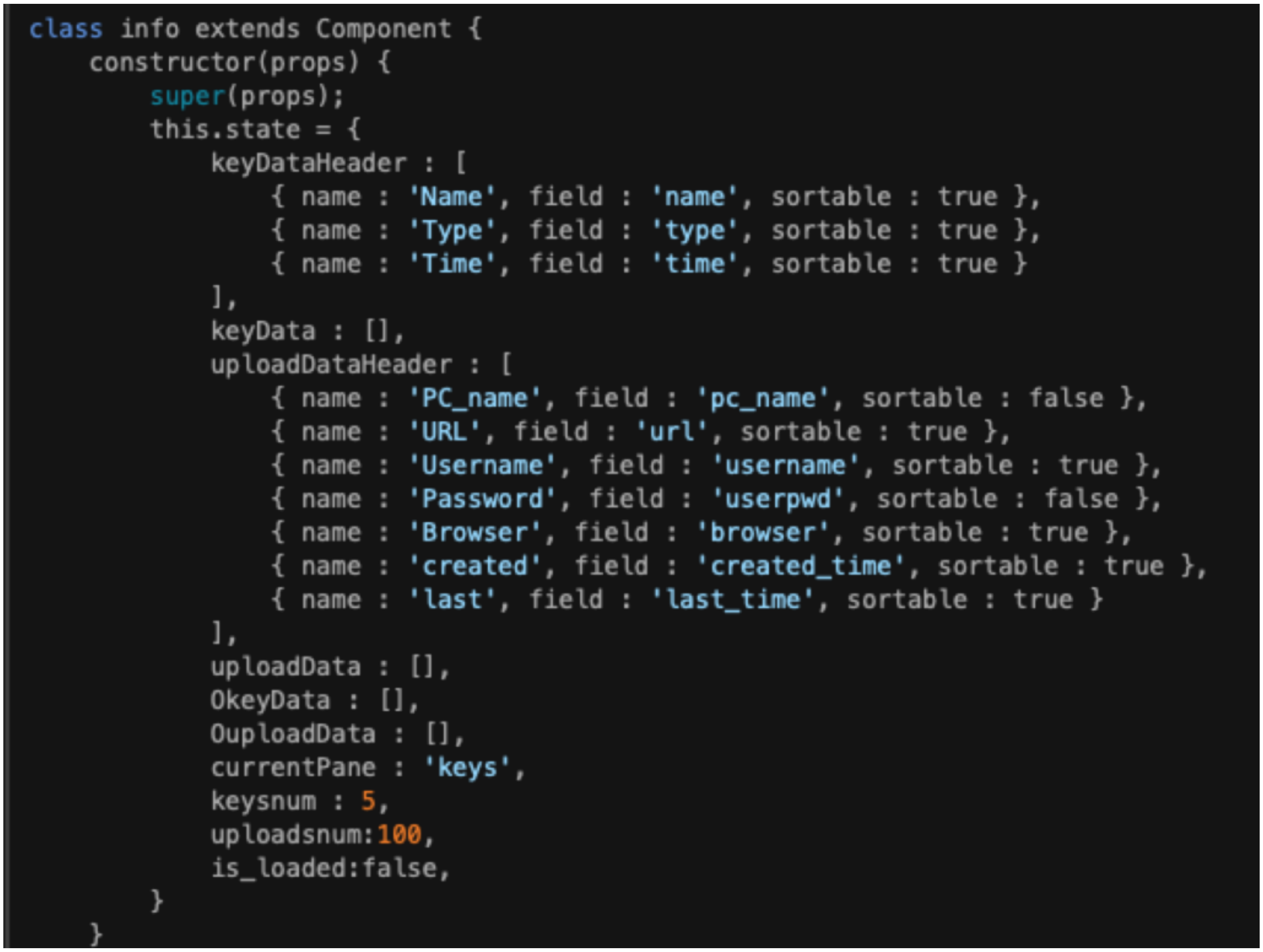
Analyzing **App.js** revealed detailed information about hidden page paths secured behind a login wall. These pages facilitated precise control over compromised systems, enabling operators to manage data efficiently.



```
/* 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';
```

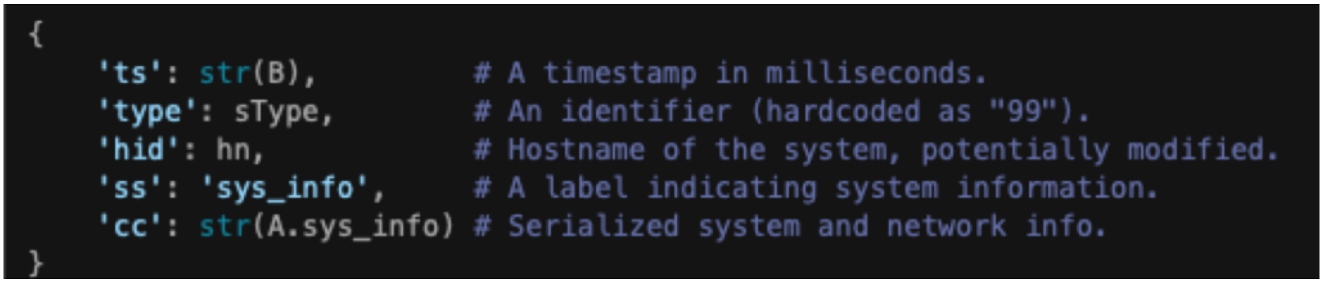
Victim Data Management:
The Info page, while inaccessible during the analysis, was determined to retrieve and display exfiltrated victim data. A closer examination of the server's JavaScript files revealed its functionality, including the ability to collect and manage:

- **PC Names and URLs**
- **Passwords and Credentials**
- **System Configuration Details**



```
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,
        }
    }
```

Data Flow:
The backend was designed to extract and filter data from implants via the **/keys API endpoint**, allowing operators to search for specific information and organize data for further use.



```
{
    '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.
}
```

“The level of precision and customization in this platform is troubling,” adds Sherstobitoff. “It shows a deliberate effort to manage stolen data at scale while evading detection.”

By embedding these advanced tools into their infrastructure, the Lazarus Group demonstrated a sophisticated approach to global cyber operations, maintaining control over compromised systems and stolen data with minimal risk of exposure.

Impact on Global Development

The Lazarus Group’s campaign targeted applications used in cryptocurrency and authentication systems, embedding malware into trusted software packages. Developers unknowingly included these compromised packages in their projects, introducing malicious code into production environments.

STRIKE observed the attackers exfiltrating sensitive development credentials, authentication tokens, and system configuration details. After collection by the C2 servers, the data was transferred to Dropbox as a final step, where it was stored and organized. Persistent connections to Dropbox highlight the methodical nature of their operations; for instance, one server maintained active sessions for over five hours.

This campaign is consistent with North Korea’s documented use of cyberattacks to fund state programs. Between 2017 and 2023, reports estimate that North Korea generated $1.7 billion from cryptocurrency thefts, underscoring the need for global organizations to verify software dependencies and monitor their development environments.

The Russian Proxy Connection

The use of Oculus proxies that are hosted on assets in Sky Freight’s proxy end-points in Russia played a critical role in Lazarus’s obfuscation strategy. Five IP addresses—83.234.227.49 through 83.234.227.53—routed traffic between VPN exits and the C2 servers.

OSINT information attributes this infrastructure to the Oculus Proxy service, a commercial service used by the attackers to route traffic through. By leveraging legitimate proxy networks, Lazarus added a layer of legitimacy to their operations, further complicating detection efforts.

Several endpoints within the same network range were linked to a case reported last year, where an individual had direct interactions with North Korean state actors. These actors were disguising themselves as recruiters or job sourcers. STRIKE managed to trace the proxy IPs back to some of the same Astrill VPNs associated with the Phantom Circuit operation.

Additionally, we observed that one Astrill VPN (present in Phantom Circuit), which connected to one of the proxies referenced in last year’s case, could also be traced back to Pyongyang, specifically to the IPs 175.45.176.68 and 175.45.178.10.

Analysis of Competing Hypotheses (ACH)

STRIKE applied the CIA's Analysis of Competing Hypotheses (ACH) methodology to assess the origins of the "Phantom Circuit" campaign. The evaluation considered multiple scenarios, with evidence strongly supporting Lazarus Group as the primary actor.

Hypotheses Evaluated:

1. **H1**: Lazarus Group (North Korea) is responsible.
2. **H2**: A non-state actor is impersonating Lazarus.
3. **H3**: Multiple actors collaborated, with Lazarus playing a partial role.
4. **H4**: Misattribution due to similar tactics and techniques.

Findings:

- STRIKE identified direct links to North Korean IPs and tactics consistent with Lazarus, including supply chain compromises and a focus on cryptocurrency theft.
- The campaign's scale and custom tools reflect capabilities aligned with state-sponsored groups rather than independent actors.
- No evidence suggested collaboration with or impersonation by other groups.

Based on this analysis, STRIKE attributes "Phantom Circuit" to the Lazarus Group with high confidence, aligning with their historical focus on cryptocurrency theft to fund state programs.

Defending Against Supply Chain Attacks

Operation Phantom Circuit highlights the critical need for organizations to secure their software supply chains. STRIKE recommends the following measures to mitigate risks:

- **Package Verification**: Validate the integrity of software updates using cryptographic checksums or signatures.
- **Network Monitoring**: Analyze connections to uncommon ports, such as 1224 and 1245, associated with malicious activity.
- **Proxy Detection**: Identify and block suspicious proxy usage, particularly from commercial services linked to malicious campaigns.
- **Development Tool Audits**: Regularly review and update development tools to identify and mitigate vulnerabilities.
- **Remote Access Scrutiny**: Monitor for persistent Remote Desktop Protocol (RDP) sessions that could indicate unauthorized access.

These practices emphasize the importance of proactive security measures in protecting critical development environments from evolving threats.

Contact STRIKE for Incident Response

If you suspect your organization has been impacted by Operation Phantom Circuit, Operation 99, or similar Lazarus activities, contact the STRIKE Incident Response team immediately. Our experts provide:

- **Rapid Containment**: Minimize damage and halt ongoing breaches.
- **Forensic Analysis**: Understand how attackers gained access and what data was affected.
- **Strategic Guidance**: Strengthen your security posture against evolving threats.

Proactively Mitigate Supply Chain Risks
To protect your organization from future supply chain attacks, SecurityScorecard's Supply Chain Detection and Response (SCDR) solution offers the tools to:

- Monitor and assess your software supply chain for vulnerabilities.
- Detect suspicious activity across your development pipelines.
- Receive actionable insights to prevent advanced threats like "Phantom Circuit."

Take control of your supply chain security today. **Contact us** for assistance or to learn more about SCDR and incident response services.

For STRIKE media inquiries, contact us here.