DRONA
CYBER SOLUTIONS

CYBERCRIME THREAT ADVISORY

DPRK-Aligned Threat Group 'Contagious Interview' (REF9403) Targets Software Developers Using Malicious SVG Steganography & 'OTTERCOOKIE' Malware

Document ID:	DTI-ADV-2026-0722
Date of Issue:	July 23, 2026
Classification:	TLP: GREEN
Prepared By:	Drona Threat Intel

1. Executive Summary

Drona Threat Intel has analyzed a new cyber espionage campaign designated **REF9403**, attributed to the North Korean (DPRK)-aligned threat group known as **Contagious Interview**. The campaign specifically targets software engineers and IT developers across global organizations via social engineering lures disguised as lucrative employment opportunities on communication platforms like Slack.

A primary innovation in this campaign is the use of **SVG steganography**. The threat actors embed Base64-encoded, fragmented malware payloads inside HTML comment blocks of SVG flag images within trojanized coding challenge repositories (e.g., Next.js e-commerce templates). When developers run standard initialization commands like `npm run dev` or `npm start`, a malicious script extracts and reassembles the payload to deploy a four-stage malware family identified as **OTTERCOOKIE**.

OTTERCOOKIE operates as a cross-platform information stealer and backdoor, harvesting browser credentials, cryptocurrency wallets, system keychains, SSH/AWS configuration files, and clipboard data, while establishing a persistent **Socket.IO-based Remote Access Trojan (RAT)**.

2. Threat Summary & Key Risk Metrics

Risk Score	HIGH	**TLP Rating**	TLP: GREEN
Threat Actor	**Contagious Interview (DPRK-Aligned)**	**Campaign ID**	REF9403
Primary Malware	**OTTERCOOKIE (Stealer / Backdoor)**	**Target Domain**	Software Developers, IT & ITES
Impacted Regions	Global (Worldwide)	**Infection Vector**	Trojanized NPM Repositories & SVG Steganography

> **Key Operational Threat:** Because software developers possess elevated access privileges, SSH keys, AWS credentials, and source code access, a compromise via OTTERCOOKIE poses a severe risk of secondary supply chain attacks against enterprise environments.

3. Technical Analysis & Infection Chain

3.1 Initial Access & Execution

The attack chain commences when adversaries contact developers via Direct Messages (DMs) on Slack or developer channels, sharing a link to a coding assessment project. The project appears as a legitimate Next.js or React web application template. Upon executing `npm run dev`, Node.js invokes `server/index.js`, which quietly triggers a malicious validation script (`serverValidation.js`) in the background while the front-end application functions normally to avoid suspicion.

3.2 Steganographic Payload Reassembly

To bypass static code analysis and EDR detection, the payload is split into Base64-encoded chunks hidden inside HTML comment tags across multiple SVG image files (e.g., flag vectors in an `/assets` folder). `serverValidation.js` reads the SVG files in alphabetical order, strips the comments, concatenates the Base64 strings, and executes the reconstructed JavaScript using a custom decoder and `eval()`.

3.3 Multi-Stage OTTERCOOKIE Execution

Once reassembled, the **OTTERCOOKIE** payload deploys across four distinct functional modules:

- **Module 1: Browser & Wallet Stealer (`npm-cache`)** — Cross-platform module targeting Chrome, Edge, and Brave. It extracts login databases, autofill records, and cryptocurrency wallet extension data. On macOS, it also exfiltrates the system Keychain. Data is posted to `ldb.rightwidth[.]dev/upload` and `/cldbs`.
- **Module 2: Sensitive File & Credential Sweeper** — Enumerates logical drives (via `wmic` on Windows) or home directories (macOS/Linux). It recursively searches for sensitive files matching patterns like `.env`, `.pem`, `.aws`, `.ssh`, and configuration files, exfiltrating them to `upload.rightwidth[.]dev/upload`.
- **Module 3: Socket.IO Backdoor (Persistent C2)** — Establishes a persistent HTTPS WebSocket connection to `controller.rightwidth[.]dev` using Socket.IO. It gathers OS host details, checks for virtual machine/sandbox environments, and grants operators interactive shell access via `child_process.exec()`.
- **Module 4: Dropper & Clipboard Stealer** — Polling the clipboard every 500ms using `pbpaste` (macOS) or `Get-Clipboard` (PowerShell/Windows), exfiltrating contents to `rightwidth[.]dev/api/service/makelog`. On Windows, it uses `curl` to download second-stage executables disguised as `.txt` files from `file.rightwidth[.]dev`.

4. MITRE ATT&CK® Mapping

Tactic	Technique ID	Technique Name
Command & Control (TA0011)	T1001.002	Data Obfuscation: Steganography
Collection (TA0009)	T1005	Data from Local System
Exfiltration (TA0010)	T1041	Exfiltration Over C2 Channel
Command & Control (TA0011)	T1071.001	Application Layer Protocol: Web Protocols
Discovery (TA0007)	T1082	System Information Discovery
Discovery (TA0007)	T1083	File and Directory Discovery
Collection (TA0009)	T1115	Clipboard Data
Credential Access (TA0006)	T1555	Credentials from Password Stores

5. Indicators of Compromise (IoCs)

Indicator Value	Type	Context / Description
rightwidth[.]dev	Domain	Primary C2 Infrastructure
ldb.rightwidth[.]dev	Domain	Credential & Wallet Exfiltration C2
upload.rightwidth[.]dev	Domain	File Stealer Exfiltration C2
controller.rightwidth[.]dev	Domain	Socket.IO Backdoor C2
file.rightwidth[.]dev	Domain	Payload Dropper Host
195.26.248[.]212	IPv4	Associated C2 Server IP
188.40.64[.]61	IPv4	Associated C2 Server IP
8e571d58794b9b44ae53c2c67bedef72c500e8adbb80aab7a5c26adcba55b1e3	SHA-256	Malicious JS / OTTERCOOKIE Sample
e6360f83a95540aa2176d279ca4694513afb1e5116a7ffe591c6b5bcf3b9c3c4	SHA-256	OTTERCOOKIE Payload Variant

6. Strategic Mitigation Recommendations

1. **Developer Security Awareness:** Train engineering teams regarding social engineering tactics involving unsolicited job offers, Slack DMs, and untrusted code execution.
2. **Code Review & Repository Isolation:** Require mandatory security reviews for third-party test projects and execute candidate coding challenges exclusively within isolated, non-production virtual environments or sandboxes.
3. **EDR Behavioral Rules:** Configure Endpoint Detection & Response (EDR) agents to detect anomalous process trees, such as Node.js or `npm` spawning shell commands (`cmd.exe` , `powershell.exe`) or making outbound connections to unverified domains.
4. **Network Egress Filtering:** Block outbound communication to all listed `rightwidth[.]dev` domain indicators at perimeter firewalls and DNS resolvers.
5. **FIDO2 / Hardware MFA Enforcement:** Enforce phishing-resistant MFA (e.g., YubiKeys) for developer access to cloud infrastructure, AWS console, and code repositories to limit the impact of stolen session tokens and browser credentials.