DRONA
CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

Phishy v2.0.0: Next-Gen Golang Phishing Panel

An advanced, real-time phishing-as-a-service architecture driving automated identity theft, WebSocket-driven live session manipulation, and multi-step credential harvesting workflows.

PREPARED BY
Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE
July 9, 2026

CLASSIFICATION MATRIX
HIGH: RED AMBER GREEN

THREAT AWARENESS ADVISORY

Advanced Phishing Panel 'Phishy v2.0.0' Released by Threat Actor 'phishyfam'

Issued By: Drona Cyber Solutions Pvt Ltd

Intelligence Source: Drona Threat Intel

Target Sector: Global Enterprise & Financial Infrastructure (Coinbase, Okta)

Severity Classification: HIGH

Executive Summary

On June 24, 2026, threat actor (TA) **phishyfam** advertised a sophisticated new version of their phishing kit, dubbed **Phishy v2.0.0**, on the English-language cybercrime forum DarkForums. Developed primarily using Golang and the React framework, the kit represents a major shift toward interactive, real-time phishing operations rather than static, passive credential harvesting. At the time of discovery, the threat actor offered prebuilt targeted templates for Coinbase and Okta—two globally prominent platforms utilized heavily across enterprise and consumer ecosystems.

Drona Threat Intel engaged directly with the threat actor to analyze the tool's core capabilities. The findings indicate that Phishy v2.0.0 poses a severe, immediate risk to organizations relying on traditional, single-factor or basic multi-factor authentication (MFA) protocols by giving malicious operators the power to intercept and manipulate live user sessions dynamically.

> `[CONSOLE_CRITICAL_WARNING_ALERT]`
>
> **CRITICAL CAPABILITY:** Phishy v2.0.0 utilizes a persistent WebSocket engine that allows cybercriminals to monitor a victim's exact interaction in real time, view live data forms, and forcefully swap active client-facing pages to collect secondary authentication codes, financial tokens, and session details instantly.

Attack Chain & Distribution Workflow

The operational workflow of an active phishing campaign utilizing the Phishy v2.0.0 kit proceeds through the following structured engineering phases:

- **Ingress & Lure Generation:** The threat actor deploys highly customized HTML/CSS phishing interfaces modeled exactly after legitimate corporate identity providers or digital currency exchanges.
- **Victim Interaction & Connection:** As soon as a target visits the fake infrastructure, a persistent connection is negotiated via WebSockets, alerting the centralized operator panel that a live session is active.
- **Real-Time Monitoring:** The operator tracks comprehensive metadata, including the victim's IP address, precise geographic location, device characteristics, and active browser tab status.
- **Dynamic Page Manipulation:** When the victim submits their primary credentials, the operator manually or automatically triggers the "Change Page" module, updating the victim's view to display localized sub-prompts such as SMS Code entry or Case Access Codes.
- **MFA Interception & Exfiltration:** Multi-factor authentication values and cryptographic wallet parameters are collected in near-real-time, allowing immediate session hijacking and account takeovers before the legitimate token expires.

Technical Analysis of Core Capabilities

According to direct intelligence gathered by Drona Threat Intel, the architecture of Phishy v2.0.0 exhibits specific high-performance design decisions aimed at maximizing efficiency and bypassing modern endpoint telemetry:

- **Golang Binary Architecture:** The phishing engine compiles down into a single, highly optimized Golang binary tailored specifically for the operator's target operating system, natively supporting both Unix and Windows distributions.
- **WebSocket-Driven Real-Time Engine:** Traditional kits rely on periodic HTTP asynchronous polling, which creates delays. Phishy v2.0.0 establishes direct WebSockets, providing instantaneous screen-state updates to the control dashboard.
- **Centralized Multi-Server Infrastructure:** Malicious operators can configure and deploy multiple distinct phishing servers and unique brand campaigns from a single centralized instance of the dashboard.
- **Multi-User Collaborative Access:** The platform supports the provision of unlimited operator sub-accounts, facilitating team-based cybercrime operations and Phishing-as-a-Service (PaaS) business models.

- **Defensive Automated Operations:** In Unix environments, the panel automatically handles reverse proxy generation via Nginx and automates secure HTTPS deployments utilizing Certbot for Let's Encrypt certificates, minimizing configuration errors.

Commercial Model & Actor Activity

The threat actor phishyfam has been observed across multiple forums, including PwnForums and DarkForums, since early 2026. Their historical focus includes selling targeted lead databases and leasing interactive utility kits. The commercial structure for Phishy v2.0.0 is distributed across modular tiers:

- **Prebuilt Focus Templates:** Individual brand templates for Coinbase and Okta are retailed at $100 each.
- **Compiled Binary Licensing:** A standalone compiled binary is licensed at $500 for a one-time purchase or $800 bundled with continuous development updates.
- **Core Source Code:** Unrestricted access to the core Golang and React source repository is commercialized at $1,000 for a one-time transaction or $1,600 with perpetual updates.

Strategic Recommendations & Mitigations

To protect corporate boundaries and consumer infrastructure against the automated real-time manipulation capabilities of Phishy v2.0.0, the following actions must be taken:

REQUIREMENT	ACTION-ORIENTED MITIGATION STRATEGY
ENFORCE FIDO2 MFA	Transition authentication flows completely away from SMS and voice-based OTP parameters. Enforce hardware security keys or FIDO2-compliant passkeys that natively bind to the origin domain, rendering intercepted tokens useless on phishing endpoints.
IMPLEMENT Session Anomalies	Deploy automated behavioral monitoring engines capable of identifying instantaneous changes in user IP geolocation routing or multiple concurrent server handshakes within identical session IDs.
RESTRICT WebSocket Traffic	Monitor internal networks for persistent outbound WebSocket channels directed toward unclassified external hosting environments or suspicious residential proxy networks.
AUDIT Directory Logs	Regularly inspect Okta and enterprise directory connection trees for high-frequency connection attempts originating from foreign bulletproof hosting infrastructure.
TRAIN Targeted Personnel	Conduct interactive simulation exercises focusing specifically on multi-step authorization requests and dynamic administrative case access code screens.

Indicators of Compromise (IoCs)

The following network artifacts were identified by Drona Threat Intel during behavioral observation of the active phishing infrastructure:

INDICATOR VALUE	INDICATOR TYPE	GEOGRAPHIC CONTEXT / HOSTING PROVIDER
`146.70.144.48`	IPv4 Address	Poland | Malicious Infrastructure
`149.88.20.213`	IPv4 Address	Portugal | Datacamp Limited
`146.70.193.95`	IPv4 Address	Serbia | M247 Ltd Belgrade
`93.115.0.7`	IPv4 Address	Serbia | HostRoyale Technologies Pvt Ltd