

THREAT ADVISORY

DarkSword C2 Infrastructure

October 2, 2026

Executive Summary

Researchers from Team Cymru identified active **DarkSword C2 controller infrastructure** within their detection pipeline, observing **43 hosts across 26 networks** located in Hong Kong, the United States, Singapore, China, Japan, Brazil, and South Korea. According to the researchers, hosting activity is heavily concentrated within the APAC region.

Additional industry reporting indicates that **DarkSword** has evolved from a highly sophisticated mobile exploitation framework into a broader threat ecosystem supported by extensive command-and-control infrastructure. Independent researchers have identified more than 100 DarkSword-related management panels and operational infrastructure nodes actively supporting threat actor operations.

The threat presents particular concern because DarkSword has been associated with advanced mobile exploitation, credential theft, surveillance activities, data exfiltration, and operator-controlled post-compromise actions. Multiple threat intelligence organizations have documented DarkSword infrastructure being used by both commercial surveillance operators and other threat actors.

Known Indicators of Compromise (IOCs)

Suspected DarkSword C2 Infrastructure

IP Address
8.210.67.79
35.203.134.133
38.60.125.123
38.181.56.130

Detection Recommendations

Organizations should:

- Review firewall, proxy, DNS, EDR, and NDR telemetry for communications involving the identified IPs.
- Hunt for outbound HTTPS sessions to unknown infrastructure located in APAC hosting regions.
- Monitor for anomalous mobile-device traffic communicating with previously unseen cloud infrastructure.
- Investigate suspicious browser-based activity associated with mobile devices.

Threat Overview

DarkSword has been described as a sophisticated exploitation and surveillance framework capable of:

- Device fingerprinting
- Command-and-control communications
- Credential theft

Our People Make the Difference

THREAT ADVISORY

DarkSword C2 Infrastructure

October 2, 2026

- Data collection and exfiltration
- Remote device management
- Surveillance operations
- Post-exploitation tasking from operator-controlled infrastructure

Researchers have observed the ecosystem leveraging dedicated administration panels, cloud-hosted infrastructure, and geographically distributed servers. Infrastructure analysis has identified significant concentrations of hosting assets in Hong Kong while also finding activity in the United States, Japan, Singapore, and Europe.

Tactics, Techniques, and Procedures (TTPs)

Initial Access

T1189 – Drive-by Compromise

DarkSword has been observed using malicious or compromised websites to initiate exploitation activity against victim devices.

T1566 – Phishing and Social Engineering Lures

Researchers documented infrastructure masquerading as legitimate sign-in portals and trusted web content.

Execution

T1059 – Command and Scripting Interpreter

Browser-delivered code and scripted payload execution are used during compromise operations.

T1203 – Exploitation for Client Execution

DarkSword has been associated with exploitation of multiple vulnerabilities to achieve code execution on targeted devices.

Persistence / Command & Control

T1071 – Application Layer Protocol

Operator infrastructure utilizes web-based communications for command-and-control activities.

T1105 – Ingress Tool Transfer

Observed infrastructure supports payload delivery and operator tasking functions.

Credential Access

T1555 – Credentials from Password Stores

T1003 – Credential Access Activities

Our People Make the Difference

THREAT ADVISORY

DarkSword C2 Infrastructure

October 2, 2026

Researchers report collection of credentials, session information, saved account data, and other sensitive identity artifacts.

Collection

T1005 – Data from Local System

T1119 – Automated Collection

T1213 – Data from Information Repositories

DarkSword activity has been associated with collection of files, contacts, messages, browser data, and other sensitive information stored on compromised devices.

Exfiltration

T1041 – Exfiltration Over C2 Channel

Collected information is transmitted to operator-controlled command-and-control infrastructure.

Potential Detection Opportunities

Network Monitoring

Alert on:

- Communications to identified IOC IP addresses
- Low-volume encrypted traffic to unfamiliar international cloud-hosted infrastructure
- Repeated outbound HTTPS connections to newly-observed domains
- Mobile-device communications occurring outside normal enterprise patterns

Endpoint Monitoring

Monitor for:

- Unusual browser activity
- New network connections initiated by mobile management software
- Credential access indicators
- Unauthorized collection of device data

Threat Hunting Queries

Search for:

- Connections to known DarkSword infrastructure
- Newly registered domains mimicking authentication services
- Unexpected outbound communications originating from executive or high-value user devices
- Mobile endpoints exhibiting persistent beaconing behavior

THREAT ADVISORY

DarkSword C2 Infrastructure

October 2, 2026

Remediation Recommendations

Immediate Actions

1. Block known IOC IP addresses at firewalls, web proxies, DNS filtering platforms, and secure web gateways.
2. Review all outbound communications involving the identified IPs over the previous 90 days.
3. Investigate devices that communicated with the identified infrastructure.
4. Validate endpoint protection telemetry for potential command-and-control activity.
5. Ensure operating systems, browsers, and mobile devices are fully patched.

Strategic Actions

1. Implement Network Detection and Response (NDR) monitoring.
2. Deploy DNS logging and threat intelligence enrichment.
3. Enhance mobile device management (MDM) visibility and controls.
4. Enforce phishing-resistant MFA.
5. Implement continuous threat hunting for emerging C2 infrastructure.
6. Conduct threat exposure assessments focused on externally facing systems and mobile access paths.

How Blackswan Cybersecurity Can Help

Blackswan Cybersecurity can assist organizations in identifying, containing, and mitigating DarkSword-related threats through:

Threat Hunting & IOC Validation

- Enterprise-wide IOC sweeps
- Historical log analysis
- Network and endpoint correlation
- Detection engineering and rule creation

Managed Detection & Response (MDR)

- 24x7 monitoring for C2 communications
- Threat intelligence enrichment
- Rapid incident triage and escalation
- Continuous threat hunting

Incident Response

- Compromise assessment
- Remote and onsite incident response
- Forensic collection and analysis
- Containment and eradication support

Security Architecture Review

- Mobile security posture assessments
- Internet-facing asset reviews
- Zero Trust maturity assessments

Our People Make the Difference

13717 Neutron Rd, Dallas, TX 75244 | www.Blackswan-Cybersecurity.com

THREAT ADVISORY

DarkSword C2 Infrastructure

October 2, 2026

- Identity and access management validation

Executive Risk Briefings

- Threat impact analysis
- Regulatory and compliance implications
- Board and executive reporting
- Strategic security roadmap development

Organizations concerned about potential exposure should immediately review telemetry for the identified indicators and conduct targeted threat hunting activities against known DarkSword infrastructure. Current reporting suggests a distributed and evolving threat ecosystem with active command-and-control infrastructure spanning multiple geographic regions.