ADVISORY FOR ICM SECTORS

Threat Actor Uses LapDogs, Operational Relay Box (ORB) Infrastructure to Obfuscate Traffic

Original report published on: June 16, 2025[1]

Executive Summary

SecurityScorecard's STRIKE team identified a novel network of Operational Relay Boxes (ORB) called "LapDogs" began targeting primarily Linux-based Small Office/Home Office (SOHO) devices globally since September 2023. The LapDogs network has accumulated victims across the United States and Southeast Asia region, with its size growing steadily.

A custom backdoor called "ShortLeash", established foothold on compromised devices and connects them within the ORB network. ShortLeash generates unique, self-signed Transport Layer Security (TLS) certificates with spoofed metadata for each node. STRIKE team analysis traces these certificates to over 1,000 actively infected nodes globally, revealing the geographical patterns.

Victimology analysis reveals affected Internet Service Providers (ISPs), hardware vendors, and specific organisations operating in several sectors such as technology, real estate, telecommunications, media.

Background

The LapDogs campaign uses an Operational Relay Box (ORB) network – a relatively novel technique increasingly favoured by nation-state actors. Unlike traditional botnets, which are used for disruptive attacks such as Distributed Denial of Services (DDoS), ORB maintain controls over compromised devices without disrupting its normal functionality as designed. This allows the threat actors to utilise compromised devices that appears as legitimate traffic for long-term infrastructure espionage operations.

LapDogs has steadily grown into a global network of over 1,000 infected nodes, with a strong focus on specific regions and sectors. A custom backdoor called "ShortLeash" is designed to compromise and maintain access to devices. It issues self-signed TLS certificates spoofed with "LAPD" metadata – likely attempt to impersonate the Los Angeles Police Department for legitimacy and mislead analysts or automated detection solutions.

Analysis of these spoofed certificates revealed spikes in issuance that aligned with targeted intrusion attempts, such as focused campaigns against Japan and Taiwan on specific dates. Some compromised devices served not only as proxies but also as access points into internal networks, highlighting the campaign's strategic use of hybrid victims.

LapDogs reflects a broader shift in tradecraft, with threat actors using ORB networks to conduct persistent, covert intrusions that are harder to detect, attribute and remediate. As these techniques becoming common, traditional Indicators of Compromise (IOCs) and remediation strategies may prove insufficient, underscoring the urgent need to secure embedded and edge devices often overlooked in enterprise environment.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention of ShortLeash malware identified in this advisory:

- Scan for Indicators of Compromise to detect threat actor activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Ensure all internet-facing SOHO and edge devices (routers, access points, IP cameras, etc) are running the latest firmware available.
- Disable or limit remote management interfaces to private network.
- If compromise is suspected, factory-reset affected devices, reprovision securely and update to the latest firmware available. Backdoors like ShortLeash may persist through soft reboots or partial resets.
- Enforce strong password hygiene and reset password from default credentials on all network devices.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise [1]

SHA256 Hash	Description
75618401b64046d970df49fcfdfcc36174b0aae27ac4e1c178dc75219992080a	ShortLeash Bash startup script
9b954bfc2949d07eb41446225592eaa65ed3954cd2b93a13c574bb89147a4465	ShortLeash - Linux variant
33ff77940436498a50bbb05391324964063cd3c93f2e66b07d1cb31442bb1513	
073133298e5cca0833354be754f5d14358c0dbc24ba5f70e5b5eceec1d6726e6	
02ab315e4e3cf71c1632c91d4914c21b9f6e0b9aa0263f2400d6381aab759a61	ShortLeash - Windows variant
1a180186e6fbaf6fa88f934965290235e8418976d6f3546dbf100217d1752db4	

Network Fingerprints	Description
CN=ROOT, O=LAPD, ST=California, C=US, L=LA, OU=Police department	Certificate metadata – subject and issuer (TLS Certificate)
CN=ROOT, O=LAPD, ST=California, C=US, OU=Police department, L=LA	Certificate metadata – subject and issuer (TLS Certificate) (appears in different order)
3fd3fd16d3fd3fd22c3fd3fd3fd3fdf20014c17cd0943e6d9e2fb9cd59862b	JARM fingerprint for the malicious service

IP Address	Description
119[.]31[.]186[.]253	LapDogs Node IP
103[.]131[.]189[.]36	
103[.]131[.]189[.]2	
64[.]176[.]228[.]227	Suspected LapDogs Virtual Private Server (VPS) Node
103[.]117[.]100[.]77	
103[.]117[.]100[.]79	
103[.]117[.]100[.]117	
103[.]135[.]248[.]52	
141[.]164[.]44[.]183	
141[.]164[.]50[.]206	
141[.]164[.]51[.]99	
141[.]164[.]63[.]253	
158[.]247[.]203[.]36	
158[.]247[.]208[.]113	
158[.]247[.]216[.]244	
158[.]247[.]244[.]8	
158[.]247[.]250[.]190	
180[.]21[.]22[.]148	

Domain	Description
northumbra[.]com	LapDogs related domain
ns[.]northumbra[.]com	
www[.]northumbra[.]com	LapDogs C2 Domain
study[.]northumbra[.]com	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1133	External Remote Services
	T1190	Exploit Public-Facing Application
Execution	T1059	Command and Scripting Interpreter
Persistence	T1037.005	Boot or Logon Initialisation Scripts: Linux and Unit
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1070.004	Indicator Removal on Host: File Deletion
	T1140	Deobfuscate/Decode Files or Information
	T1578	Modify Cloud Compute Infrastructure
Credential Access	T1110	Brute Force
Discovery	T1046	Network Service Scanning
	T1083	File and Directory Discovery
Lateral Movement	T1021.001	Remote Services: SSH
	T1210	Exploitation of Remote Services
Command and Control	T1001	Data Obfuscation
	T1071.001	Application Layer Protocol: Web Protocols
	T1573.002	Encrypted Channel: Asymmetric Cryptography

References

1. ^ “LapDogs, The New Operational Relay Box (ORB)”