ADVISORY FOR ICM SECTORS

‘PurpleHaze’ and ‘ShadowPad’ Campaigns Target Media Sector

Original report published on: June 09, 2025[1]

Executive Summary

Between October 2024 to early of 2025, SentinelOne’s SentinelLABS tracked two campaigns named as ‘PurpleHaze’ and ‘ShadowPad’ – targeting entities across various sectors including Media. In October 2024, SentinelOne itself was targeted in a reconnaissance attempt (PurpleHaze), and in early of 2025, a ShadowPad-linked intrusion impacted a third-party logistics provider managing SentinelOne hardware.

These activities underscores the persistent threat posed by threat actors – particularly growing focus on cybersecurity vendors that target organisations from government, telecommunications, media, finance, and transport sectors. SentinelOne identified some of the malicious infrastructure used in these activity clusters as part of an Operational Relay Box (ORB) network, which includes compromised network edge devices.

Background

This report presents a detailed investigation into a series of coordinated cyberespionage campaigns targeting high-profile organisations across multiple sectors globally. The investigation stems directly from observations of attempted reconnaissance and intrusion activities against SentinelOne and a related third-party logistics provider.

For PurpleHaze activity campaign, it was first observed in October 2024, when SentinelOne’s internet-facing infrastructure was subjected to targeted reconnaissance attempts. The threat actor exploited vulnerabilities in widely used technologies such as Ivanti VPN appliances just before public disclosure and deployed a reverse-SSH backdoors named “GOREshell”. The tools and tradecraft reflect a high degree of technical maturity, with use of custom malware, advanced obfuscation, and zero-day vulnerabilities usages. SentinelOne detected and neutralised the activity in its early stage where no compromise of systems or data was identified.

In early 2025, a third-party logistics contracted to handle SentinelOne employee hardware was identified to be compromised where it is linked to ShadowPad – a backdoor often used in long-term cyberespionage operations. Further investigation revealed the usage of ScatterBrain loader, a custom obfuscating compiler that integrates multiple operational modes and protection components to complicate the analysis of binaries it generates. ScatterBrain disrupt both static and dynamic analyses against modern binary analysis frameworks and defender tools used in present day. SentinelOne’s own infrastructure was found not to be breached but the event highlighted supply chain risk.

SentinelOne found that both activity clusters were found to be partially related, sharing infrastructure, tools and targeting patterns. SentinelOne managed to conduct a full forensic review of internal systems, software, and hardware following discovery of both incidents.

A key insight from the report is the growing trend of cybersecurity vendors being directly targeted, not just as defenders but as valuable sources of insight, credentials, and operational footholds. These campaigns highlighted the importance of layered defence, robust supply chain oversight and control, and early detection capabilities.

Detection and Mitigation

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

- Scan for Indicators of Compromise to detect threat actor activities (Annex A).
- Prioritise patching for internet-facing edge devices infrastructure.
- Vendor Application Security Testing (VAST) program to attest and reduce risks associated with vendor-supplied software.
- Implement network segmentation and disable all internet-facing remotes services.
- Enhance visibility through script logging and endpoint telemetry.

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]

SHA-1 Hash	Description
106248206f1c995a76058999ccd6a6d0f420461e	Webshell
411180c89953ab5e0c59bd4b835eef740b550823	GOREshell (snapd)
4896cfff334f846079174d3ea2d541eec72690a0	Nimbo-C2 agent (PfSvc.exe)
5ee4be6f82a16ebb1cf8f35481c88c2559e5e41a	ShadowPad
7dabf87617d646a9ec3e135b5f0e5edae50cd3b9	GOREshell (update-notifier)
a31642046471ec138bb66271e365a01569ff8d7f	GOREshell
a88f34c0b3a6df683bb89058f8e7a7d534698069	ShadowPad
aa6a9c25aff0e773d4189480171afcf7d0f69ad9	ShadowPad
c43b0006b3f7cd88d31aded8579830168a44ba79	ShadowPad
cb2d18fb91f0cd88e82cb36b614cfedf3e4ae49b	GOREshell (glib-2.0.dll)
cbe82e23f8920512b1cf56f3b5b0bca61ec137b9	Legitimate VMWare executable (VGAuthService.exe)
ebe6068e2161fe359a63007f9febea00399d7ef3	GOREshell
f52e18b7c8417c7573125c0047adb32d8d813529	ShadowPad (AppSov.exe)

IP Address	Description
103[.]248[.]61[.]36	Malware hosting location
107[.]173[.]111[.]26	GOREshell C2 server
128[.]199[.]124[.]136	C2 server
142[.]93[.]212[.]42	Suspected PurpleHaze infrastructure
142[.]93[.]214[.]219	GOREshell C2 server
143[.]244[.]137[.]54	Suspect PurpleHaze infrastructure
45[.]13[.]199[.]209	Exfiltration IP address
65[.]38[.]120[.]110	ShadowPad C2 server

Domain	Description
cloud[.]trendav[.]co	Suspected PurpleHaze infrastructure
downloads[.]trendav[.]vip	GOREshell C2 server
dscriy[.]chtq[.]net	ShadowPad C2 server
epp[.]navy[.]ddns[.]info	GOREshell C2 server
mail[.]ccna[.]organiccrap[.]com	GOREshell C2 server
mail[.]secmailbox[.]us	Suspected PurpleHaze infrastructure
network[.]oossafe[.]com	Suspected ShadowPad C2 server
news[.]imaginerjp[.]com	ShadowPad C2 server
notes[.]oossafe[.]com	Suspected ShadowPad C2 server

secmailbox[.]us	Suspected PurpleHaze infrastructure
sentinelxdr[.]us	Suspected PurpleHaze infrastructure
tatacom[.]duckdns[.]org	C2 server
trendav[.]vip	Suspected PurpleHaze infrastructure
updata[.]dsqurey[.]com	ShadowPad C2 server

References

1. ^ “Follow the Smoke – Activity Clusters ‘PurpleHaze’ and ‘ShadowPad'"