INCIDENT RESPONSE REPORT: Malware Traffic Analysis

Incident Name: Operation BURNINCANDLE

Date of Report: December 2, 2025

Analyst: Joshua Blankenship

Tools Used: Wireshark (Packet Analysis), VirusTotal (Threat Intelligence)

Scenario Source: Malware-Traffic-Analysis.net (2022-03-21)

1. Executive Summary

Incident Overview

Field	Detail
Severity	High
Victim Hostname	BURNINCANDLE
Victim IP	10.0.9.14
Malware Family	IcedID (BokBot)
Status	Closed / Containment Required

Summary

A network forensic analysis was conducted on captured traffic (PCAP) originating from the internal host BURNINCANDLE (10.0.9.14). The investigation confirmed a malware infection initiated via an unencrypted HTTP GET request. The host downloaded a GZIP-compressed payload from a malicious domain. Initial hash analysis of the exported file yielded no results; however, a pivot to domain-based threat intelligence confirmed the infrastructure as part of an IcedID (BokBot) banking trojan campaign.

2. Investigation Details & Infection Vector

Infection Timeline

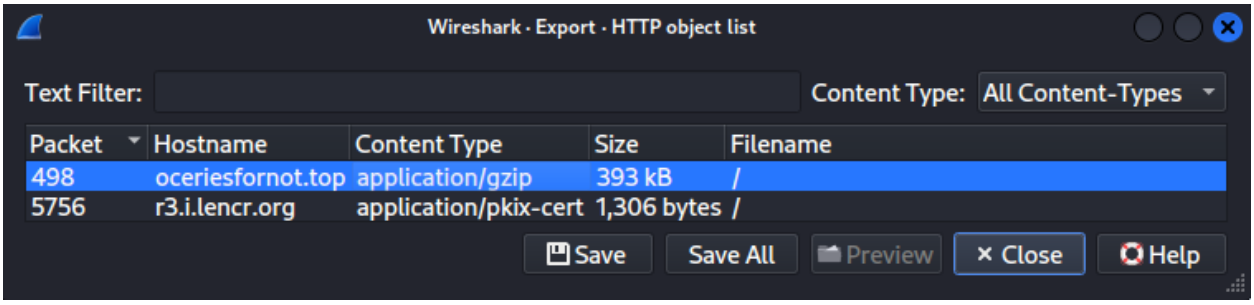
The compromise was initiated by a single outbound HTTP request from the victim to the external domain oceriesfornot.top. The server response contained a GZIP archive disguised as web content.

Description	Source / Artifact	Network Evidence
Initial Access	HTTP GET Request	Victim connected to 188.166.154.118 over Port 80.
Payload Delivery	Encrypted GZIP payload	Validated via Wireshark "Export Objects" list (application/gzip).
Persistence Activity	C2 Beaconing (Encrypted)	Observed immediate establishment of multiple HTTPS/TLS connections to external IP addresses following the download.

Investigation Workflow & Pivot

Step 1: File Identification & Extraction: The analyst identified a suspicious file transfer within the HTTP traffic. Using Wireshark's "Export HTTP Objects" feature, the GZIP payload was extracted for analysis.

Figure 1a: Wireshark "Export HTTP Objects" window showing the malicious GZIP payload.



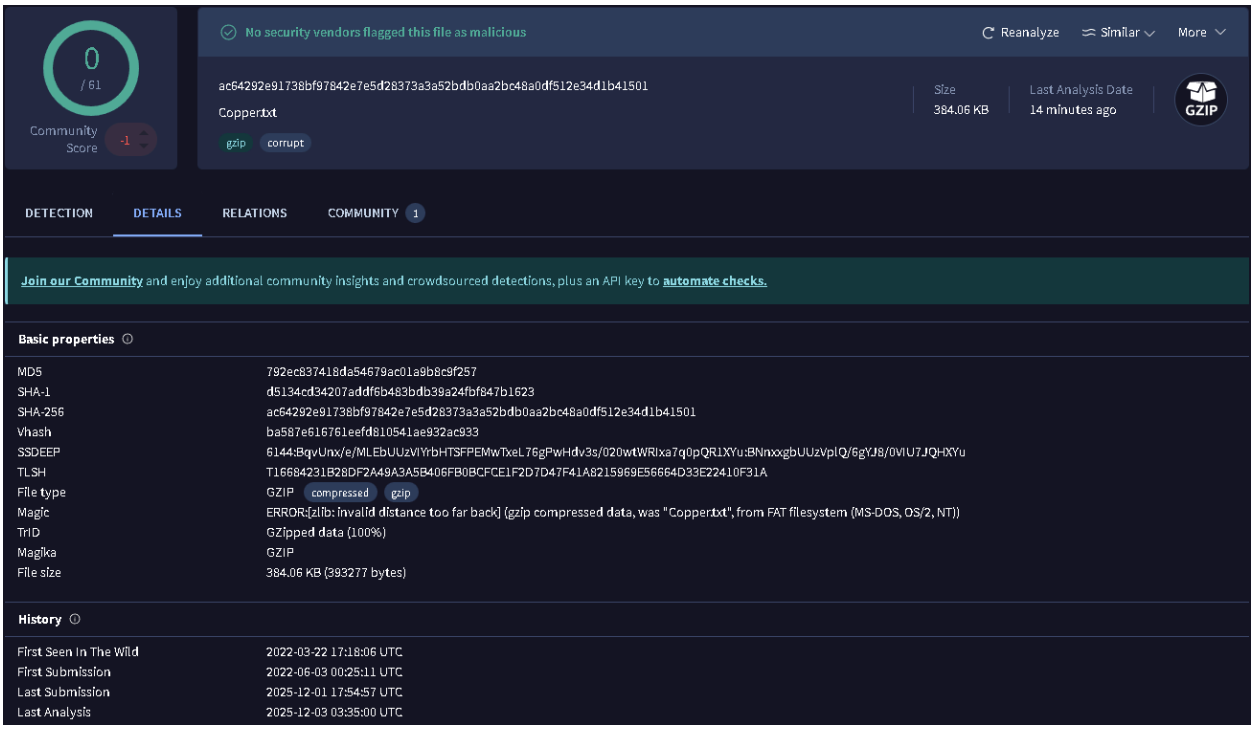
Step 2: Hash Verification: The extracted file (malware_payload.gz) was hashed using the SHA256 algorithm to generate a unique file signature.

Figure 1b: Command line hash generation of the extracted payload.

```
┌──(kali㉿kali)-[~/Documents]
└─$ sha256sum sample
ac64292e91738bf97842e7e5d28373a3a52bdb0aa2bc48a0df512e34d1b41501  sample
```

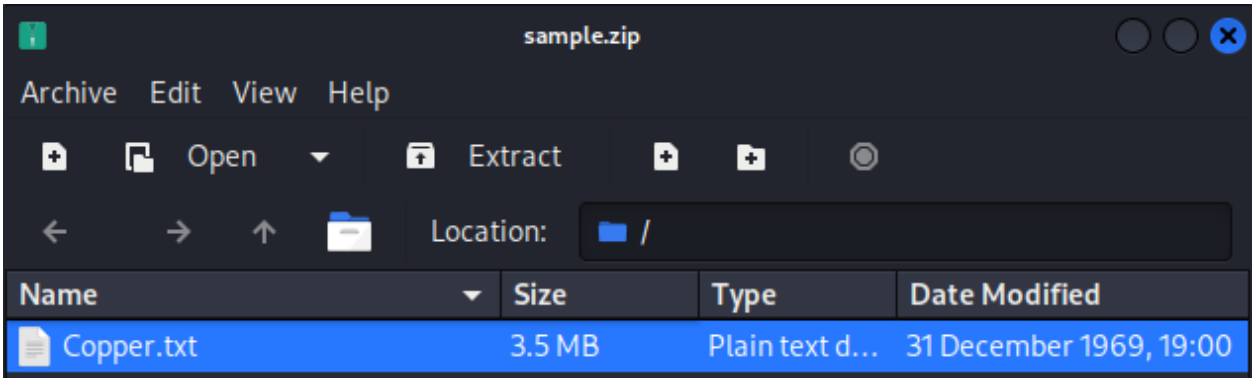
Step 3: Hash Lookup (Negative Result): A search of the file hash in VirusTotal returned 0 detections, likely due to the file being a unique, encrypted configuration artifact rather than a known executable.

Figure 1c: VirusTotal search result showing 0 detections for the file hash.



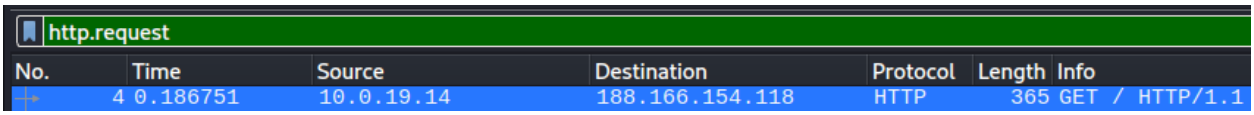
Step 4: Artifact Analysis: Further inspection of the payload revealed the file Copper.txt, a known artifact associated with IcedID encrypted configurations.

Figure 1d: Visual confirmation of the Copper.txt artifact within the payload.



Step 5: URL Analysis: Shifted investigation focus from the file to the network infrastructure. Searching the source domain oceriesfornot.top immediately confirmed it as a known malicious C2 (Command & Control) server.

Figure 1e: Wireshark filter (http.request) isolating the initial malware download request.



Step 6: OSINT Pivot (Positive Confirmation): A search for the domain oceriesfornot.top was conducted on the ThreatFox IOC Database. This confirmed the domain is a known Botnet C2 associated with the BokBot (IcedID) malware family.

Figure 2: ThreatFox IOC database confirming the malicious domain oceriesfornot.top is linked to

IOC ID:	394377
IOC:	oceriesfornot.top
IOC Type:	domain
Threat Type:	botnet_cc
Malware:	IcedID
Malware alias:	BokBot, IcelD
Confidence Level:	Confidence level is high (100%)

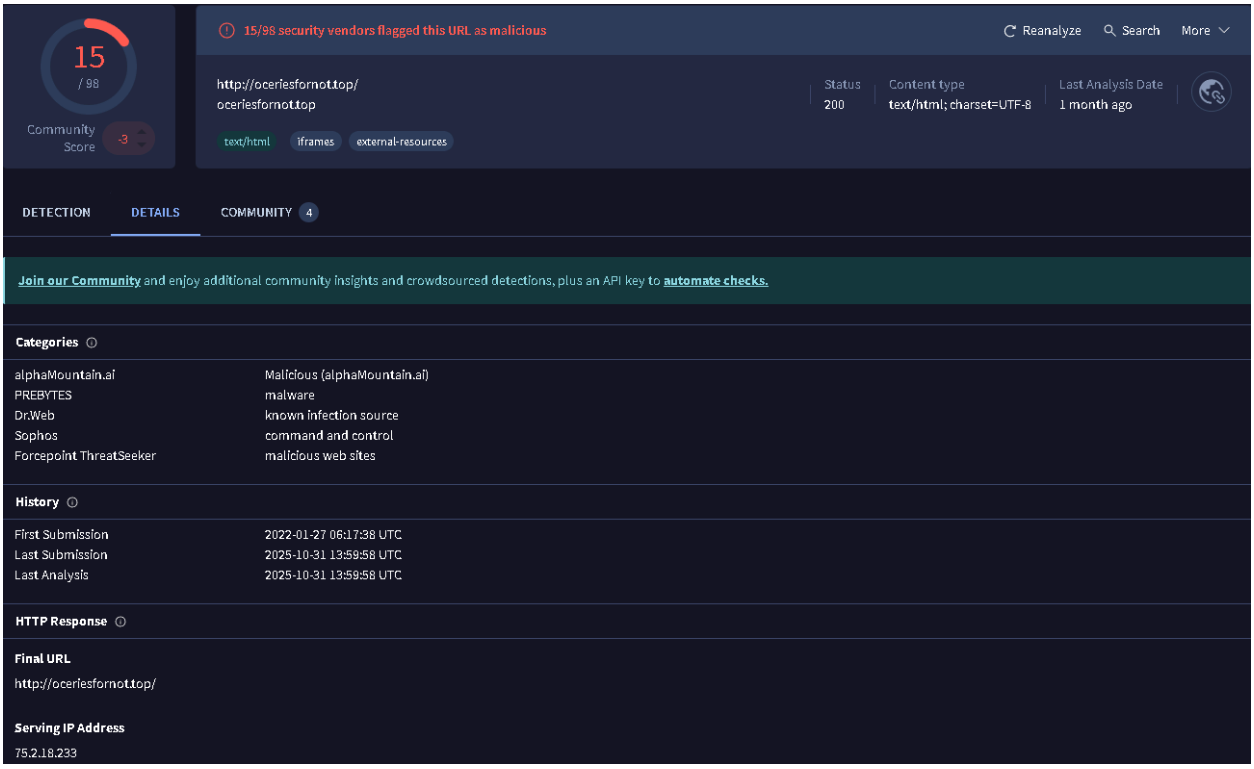
BokBot/IcedID.

3. Indicators of Compromise (IOCs)

The following Indicators of Compromise (IOCs) were extracted directly from the network traffic and verified against threat intelligence databases.

Threat Intelligence Validation

Figure 3: Threat intelligence validating the malicious C2 domain.



Network Indicators (For Blocking)

- **Malicious Domain: oceriesfornot.top**
- **Malicious IP (Initial C2): 188.166.154.118**

File Artifacts (For Endpoint Scans)

- **Artifact Filename: Copper.txt (Encrypted configuration file contained within the GZIP payload).**

Figure 4: Wireshark Endpoints Statistics identifying external malicious IP connections.

Wireshark · Endpoints · 2022-03-21-traffic-analysis-exercise.pcap

Ethernet · 3 | IPv4 · 12 | IPv6 | TCP · 26 | UDP · 3

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.0.19.14	29	8 kB	15,350	0.19%	29	8 kB	0	0 bytes
23.219.38.10	1	341 bytes	10	10.00%	0	0 bytes	1	341 bytes
68.142.107.1	2	672 bytes	14	14.29%	0	0 bytes	2	672 bytes
68.142.107.129	1	336 bytes	11	9.09%	0	0 bytes	1	336 bytes
69.28.162.0	1	336 bytes	11	9.09%	0	0 bytes	1	336 bytes
69.28.162.128	1	336 bytes	11	9.09%	0	0 bytes	1	336 bytes
72.21.81.240	3	1 kB	33	9.09%	0	0 bytes	3	1 kB
104.80.96.219	5	1 kB	53	9.43%	0	0 bytes	5	1 kB
169.254.179.89	9	2 kB	54	16.67%	9	2 kB	0	0 bytes
188.166.154.118	1	365 bytes	502	0.20%	0	0 bytes	1	365 bytes
209.197.3.8	3	1 kB	39	7.69%	0	0 bytes	3	1 kB
239.255.255.250	20	4 kB	33	60.61%	0	0 bytes	20	4 kB

4. Remediation Recommendations

Based on the confirmed presence of a banking trojan and C2 activity, the following actions are recommended:

1. **Containment: Isolate the host 10.0.9.14 (BURNINCANDLE) from the network to prevent lateral movement or data exfiltration.**
2. **Network Blockade: Configure firewall rules to deny all inbound and outbound traffic to the domains and IP addresses listed in the IOC section.**
3. **System Restoration: Wipe and re-image the compromised system from a known clean backup.**
4. **Credential Reset: Force a password reset for the user account associated with the compromised host.**