THREAT INTELLIGENCE REPORT

Generated: February 05, 2026

Healthcare & Retail Threat Intelligence Platform

Total IOCs	ATT&CK Coverage	Anomalies Detected	Active Feeds
505	25 techniques	46	6

Executive Summary

This report summarizes threat intelligence collected from 6 active sources, comprising 505 unique indicators of compromise (IOCs). Analysis identified 25 MITRE ATT&CK; techniques across 11 tactics, with 46 anomalous indicators flagged for priority investigation.

Key Findings:

• Primary threat category: **malware_download** (100 IOCs)

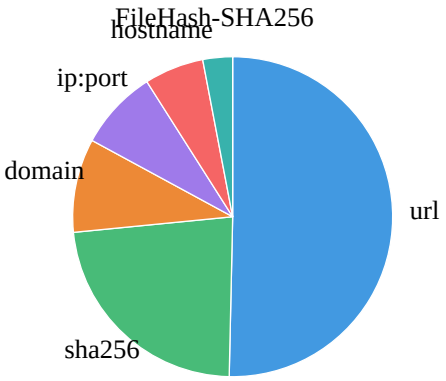
• Most prevalent malware family: **Mirai** (35 samples)

• Active threat campaigns detected: **14** (8 with malware attribution)

• Anomaly detection rate: **9.1%** of indicators flagged as unusual

IOC Distribution Analysis

IOC Types



Collection Sources

Source	IOC Count	Percentage
urlhaus	100	19.8%
malwarebazaar	100	19.8%
openphish	100	19.8%
threatfox	100	19.8%
alienvault_otx	100	19.8%
feodotracker	5	1.0%

MITRE ATT&CK; Coverage

Threat mapping identified **25** unique ATT&CK; techniques across **11** tactics, covering approximately **79%** of the kill chain.

Top ATT&CK; Techniques

Technique ID	IOC Count
T1105	113
T1566.001	111
T1059	103
T1204.002	100
T1598	100
T1566.002	100
T1571	46
T1499.002	41
T1059.004	41
T1110.001	41

Detected Threat Campaigns

ML clustering identified **14** potential threat campaigns based on shared infrastructure, malware, and behavioral patterns.

Campaign	Size	Malware	Threat Types
Unknown Campaign	100	-	malware_download
Phishing Campaign	100	-	phishing
Unknown Campaign	75	-	-
Mirai Botnet Activity	66	win.xworm, win.stealc	payload, botnet_cc
Mirai Botnet Activity	61	Stealc, GuLoader	malware
Unknown Campaign	39	-	malware
Unknown Campaign	22	-	-
Cobalt Strike Infrastructure	18	unknown, win.stealc	botnet_cc, payload_delivery
Unknown Campaign	5	win.santa_stealer, win.stealc	botnet_cc, payload_delivery
Unknown Campaign	4	win.xworm, win.remcos	botnet_cc

High-Confidence Indicators

The following indicators have the highest confidence scores based on source reliability, corroboration, and threat context.

Type	Value	Confidence	Threat Type
url	http://42.235.100.225:34496/i	73	malware_download
url	http://27.204.193.247:46392/i	73	malware_download
url	https://github.com/beratmelodi8-coder...	73	malware_download
url	https://github.com/listiyor/inattv/ra...	73	malware_download
url	https://github.com/cixx123/ssports/ra...	73	malware_download
url	http://42.225.231.157:43285/i	73	malware_download
url	http://27.215.50.61:47985/bin.sh	73	malware_download
url	http://27.204.193.247:46392/bin.sh	73	malware_download
url	http://42.235.100.225:34496/bin.sh	73	malware_download
url	http://42.6.138.15:45331/i	73	malware_download
url	http://196.251.107.12/public_files/mT...	73	malware_download
url	http://196.251.107.12/public_files/1J...	73	malware_download
url	http://42.225.231.157:43285/bin.sh	73	malware_download
url	http://123.12.198.34:49225/bin.sh	73	malware_download
url	http://183.30.204.228:2213/Video.lnk	73	malware_download