Malware Analysis Report

Executive Summary

Risk Level	**HIGH (70/100)**
Summary	As a result of a comprehensive analysis, it is suspected to be a malicious file. | Malicious URL detected by ML model.

Analysis Metadata

Source URL	https://bazaar.abuse.ch/download/bb7d6d07467f8439d048/
Original Filename	downloaded_file
Analysis Date	2025-08-21 15:28:45

Static Properties (Archive Container)

File Size	10,123 bytes
File Type	HTML document
MIME Type	text/html

File Hashes

MD5	46a23432a689d25b64a1145715543066
SHA1	261b9c3ddee525378559ff56e4d5d9b92f8f6d9c
SHA256	188e6782b0b31e5be207d439fb703b21628bb03413d4c9c808ee09beef38df74

Heuristic Risk Factors

Extension Risk	LOW (.bin)
Size Anomaly	None detected.
Packers Detected	None detected.
Obfuscation Detected	No

Malware Analysis Report

Indicators of Compromise (IOCs)

Potential URLs	https://www.googletagmanager.com/gtag/js?id=G-5GQV3CJ17N"></script> https://js.hcaptcha.com/1/api.js' https://bazaar.abuse.ch/api/#auth_key" https://x.com/abuse_ch" https://www.linkedin.com/company/abuse-ch/" https://ioc.exchange/@abuse_ch" https://bsky.app/profile/abuse-ch.bsky.social" https://abuse.ch/terms-and-conditions/" https://abuse.ch/terms-of-use/" https://abuse.ch/privacy-policy/" https://abuse.ch/cookie-policy/"
Potential IPs	None found.
Suspicious API Calls	None found.

YARA Detection Results

Rule Name	Severity	Matched String (first)
DOCX_Suspicious_XML_Strings	MEDIUM	$url:
Media_Metadata_With_URL_or_IP	LOW	$url1:
Media_Metadata_With_Script_Extensions	LOW	$js: