PyDetective Analysis Result
Package: sample_malicious_package
Version: 0.0.1
Timestamp: 2025-06-06 15:57:17
Final Verdict: **MALICIOUS**

Package Metadata

Key	Value
package_name	sample_malicious_package
version	0.0.1
author	Matej Skultety
author_email	xskultety@stuba.sk
home_page	
package_url	

Evaluation Summary

Evaluation	Evaluation Verdict	Low Priority Issues	High Priority
Network	SUSPICIOUS	4	0
Syscalls	MALICIOUS	8	15
Static	MALICIOUS	2	9
Post_install	SAFE	0	0

Network: Issues Found

Priority	Rule	Indicator
LOW	IP without OTX details accessed	2a02:ec80:300:ed1a::3
LOW	IP without OTX details accessed	185.15.59.226
LOW	Unexpected domain accessed	wikipedia.com
LOW	Unexpected domain accessed	www.package.test

Syscalls: Triggered Falco Rules

Priority	Rule	Indicator
HIGH	Modify authentication process	
HIGH	Crontab Modification via Subprocess	crontab -l
HIGH	Suspicious Network Utility Execution	curl -s https://wikipe
HIGH	Crontab Modification via Subprocess	crontab -
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
HIGH	Modify authentication process	
HIGH	Crontab Modification via Subprocess	crontab -l
HIGH	Suspicious Network Utility Execution	curl -s https://wikipe
HIGH	Crontab Modification via Subprocess	crontab -
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe

LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
HIGH	Modify authentication process	
HIGH	Crontab Modification via Subprocess	crontab -l
HIGH	Suspicious Network Utility Execution	curl -s https://wikipe
HIGH	Crontab Modification via Subprocess	crontab -
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
HIGH	Crontab Modification via Subprocess	crontab -l
HIGH	Suspicious Network Utility Execution	curl -s https://wikipe
HIGH	Crontab Modification via Subprocess	crontab -
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe
LOW	Outbound HTTP/HTTPS Connection	curl -s https://wikipe

Static Analysis: Triggered YARA Rules

Priority	Rule	Indicator
HIGH	Suspicious_HTTPS_Env_Exfiltration	sandbox/downloaded_pack
HIGH	Suspicious_SSH_Key_Access	sandbox/downloaded_pack
LOW	Suspicious_Persistence_Simulation	sandbox/downloaded_pack
HIGH	Suspicious_Obfuscated_Code_During_…	sandbox/downloaded_pack
HIGH	Suspicious_System_Info_Collection	sandbox/downloaded_pack
HIGH	Suspicious_Process_Execution	sandbox/downloaded_pack
HIGH	Suspicious_HTTPS_Env_Exfiltration	sandbox/downloaded_pack
HIGH	Suspicious_SSH_Key_Access	sandbox/downloaded_pack
LOW	Suspicious_Persistence_Simulation	sandbox/downloaded_pack
HIGH	Suspicious_System_Info_Collection	sandbox/downloaded_pack
HIGH	Suspicious_Process_Execution	sandbox/downloaded_pack