PyDetective Analysis Result
Package: sample_malicious_package
Version: 0.0.1
Timestamp: 2025-06-06 15:57:50
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	Output
LOW	IP without OTX details accessed	{'ip': '2a02:ec80:300:ed1a: '14907', 'asn_description': US', 'country': 'NL', 'netw 'US-WMF-20121130'}
LOW	IP without OTX details accessed	{'ip': '185.15.59.226', 'as 'asn_description': 'WIKIMED 'country': 'NL', 'network_n 'Wikimedia-esams-infra'}
LOW	Unexpected domain accessed	{'domain': 'wikipedia.com', 'MarkMonitor, Inc.', 'creat '', 'expiration_date': '', 'name_servers': ['NS0.WIKIM 'NS1.WIKIMEDIA.ORG', 'NS2.WIKIMEDIA.ORG']}
LOW	Unexpected domain accessed	{'domain': 'www.package.tes 'registrar': None, 'creatio 'None', 'expiration_date':

		'name_servers': None}

Syscalls: Triggered Falco Rules

Priority	Rule	Output
HIGH	Modify authentication process	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263410539540, ' None, 'k8s.pod.name':
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263411239684, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
HIGH	Suspicious Network Utility Execution	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263412751659, ' None, 'k8s.pod.name': 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263414910531, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c

		'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263434283862, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263435585423, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Modify authentication process	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263746589429, ' None, 'k8s.pod.name':
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263747458595, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
HIGH	Suspicious Network Utility Execution	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263749068958, '

		None, 'k8s.pod.name': 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263752723239, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263768315392, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218263768773873, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Modify authentication process	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264086331014, ' None, 'k8s.pod.name':

HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264087316185, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
HIGH	Suspicious Network Utility Execution	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264087996552, ' None, 'k8s.pod.name': 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264091170246, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264109919356, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c

		'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264110536528, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264471074438, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
HIGH	Suspicious Network Utility Execution	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264471927261, ' None, 'k8s.pod.name': 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
HIGH	Crontab Modification via Subprocess	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264473943704, ' None, 'k8s.pod.name': 'proc.cmdline': 'cront 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264490711553, '

		'185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}
LOW	Outbound HTTP/HTTPS Connection	{'container.id': '9d95 'container.image.repos 'pydetective_sandbox_c 'container.image.tag': 'container.name': 'infallible_spence', ' 1749218264491716581, ' '185.15.59.226', 'fd.s 'k8s.ns.name': None, 'k8s.pod.name': None, 'proc.cmdline': 'curl https://wikipedia.com' 'user.name': 'root'}

Static Analysis: Triggered YARA Rules

Priority	**Rule**	**Output**
HIGH	Suspicious_HTTPS_Env_Exfiltration	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description code that exfiltrates e variables via HTTPS POS similar network exfiltr 'author': 'Matej Skulte 'category': 'network_ex 'strings': [{'identifie 'offset': 4616, 'matche '6f732e656e7669726f6e'} {'identifier': '$https' 1014, 'matched_data': '4854545053436f6e6e6563 {'identifier': '$post', 483, 'matched_data': '7 {'identifier': '$post', 839, 'matched_data': '7 {'identifier': '$post', 912, 'matched_data': '5 {'identifier': '$post', 1212, 'matched_data': ' {'identifier': '$post', 1221, 'matched_data': ' {'identifier': '$json', 1167, 'matched_data':

		'6a736f6e2e64756d7073'} {'identifier': '$header 1267, 'matched_data': '436f6e74656e742d547970 {'identifier': '$url', 1884, 'matched_data': '68747470733a2f2f'}]}
HIGH	Suspicious_SSH_Key_Access	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description code that accesses or m keys in ~/.ssh director credential files.', 'au Skultety', 'category': 'credential_access'}, ' [{'identifier': '$ssh_d 'offset': 2163, 'matche '2e737368'}, {'identifi '$open_r', 'offset': 19 'matched_data': '6f7065 {'identifier': '$open_r 2377, 'matched_data': ' {'identifier': '$open_r 2533, 'matched_data': ' {'identifier': '$open_r 2911, 'matched_data': ' {'identifier': '$open_r 3086, 'matched_data': ' {'identifier': '$open_r 3486, 'matched_data': ' {'identifier': '$open_r 3761, 'matched_data': ' {'identifier': '$open_r 4975, 'matched_data': ' {'identifier': '$open_r 6251, 'matched_data': ' {'identifier': '$id_rsa 2215, 'matched_data': '69645f727361'}, {'iden '$id_rsa', 'offset': 22 'matched_data': '69645f
LOW	Suspicious_Persistence_Simulation	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description code that creates persi mechanisms and also upd writes files.', 'author Skultety', 'category':

		'persistence', 'priorit 'strings': [{'identifie 'offset': 3297, 'matche '63726f6e746162'}, {'id '$cron', 'offset': 3331 'matched_data': '63726f {'identifier': '$cron', 3360, 'matched_data': '63726f6e746162'}, {'id '$cron', 'offset': 3381 'matched_data': '63726f {'identifier': '$cron', 3492, 'matched_data': '63726f6e746162'}, {'id '$cron', 'offset': 3767 'matched_data': '63726f {'identifier': '$open', 1964, 'matched_data': ' {'identifier': '$open', 2377, 'matched_data': ' {'identifier': '$open', 2533, 'matched_data': ' {'identifier': '$open', 2911, 'matched_data': ' {'identifier': '$open', 3086, 'matched_data': ' {'identifier': '$open', 3486, 'matched_data': ' {'identifier': '$open', 3761, 'matched_data': ' {'identifier': '$open', 4975, 'matched_data': ' {'identifier': '$open', 6251, 'matched_data': ' {'identifier': '$write' 4994, 'matched_data': '2e7772697465'}, {'iden '$write', 'offset': 632 'matched_data': '2e7772
HIGH	Suspicious_Obfuscated_Code_During_…	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description base64, hex, or binary- that is decoded and exe dynamically.', 'author' Skultety', 'category': 'obfuscation'}, 'string [{'identifier': '$base6 5280, 'matched_data': '6261736536342e6236346

		{'identifier': '$exec', 5320, 'matched_data': ' {'identifier': '$exec', 5742, 'matched_data': ' {'identifier': '$setup' 5959, 'matched_data': '736574757028'}, {'iden '$binary', 'offset': 50 'matched_data': '6227'} {'identifier': '$binary 5583, 'matched_data': '
HIGH	Suspicious_System_Info_Collection	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description code that collects syst information such as use hostname, OS details, P version, and environmen variables.', 'author': Skultety', 'category': 'reconnaissance'}, 'str [{'identifier': '$uname 4421, 'matched_data': '706c6174666f726d2e756e {'identifier': '$getuse 4453, 'matched_data': '676574706173732e676574 {'identifier': '$hostna 'offset': 4541, 'matche '706c6174666f726d2e6e6f {'identifier': '$hostna 'offset': 4641, 'matche '736f636b65742e676574686 5'}, {'identifier': '$s 'offset': 4574, 'matche '706c6174666f726d2e7379
HIGH	Suspicious_Process_Execution	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack , 'meta': {'description code that opens or spaw processes using subproc modules, or executes su commands.', 'author': ' Skultety', 'category': 'strings': [{'identifie '$subprocess_popen', 'o 'matched_data': '737562270726f636573732e

		{'identifier': '$subpro 'offset': 3749, 'matche '73756270726f636573732e {'identifier': '$os_pop 'offset': 1960, 'matche '6f732e706f70656e'}, {' '$cmd1', 'offset': 1833 'matched_data': '637572 {'identifier': '$cmd1', 1932, 'matched_data': '6375726c20'}]}
HIGH	Suspicious_HTTPS_Env_Exfiltration	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack e_malicious_package/__i 'meta': {'description': code that exfiltrates e variables via HTTPS POS similar network exfiltr 'author': 'Matej Skulte 'category': 'network_ex 'strings': [{'identifie 'offset': 4597, 'matche '6f732e656e7669726f6e'} {'identifier': '$https' 995, 'matched_data': '4854545053436f6e6e6563 {'identifier': '$post', 464, 'matched_data': '7 {'identifier': '$post', 820, 'matched_data': '7 {'identifier': '$post', 893, 'matched_data': '5 {'identifier': '$post', 1193, 'matched_data': ' {'identifier': '$post', 1202, 'matched_data': ' {'identifier': '$json', 1148, 'matched_data': '6a736f6e2e64756d7073'} {'identifier': '$header 1248, 'matched_data': '436f6e74656e742d547970 {'identifier': '$url', 1865, 'matched_data': '68747470733a2f2f'}]}
HIGH	Suspicious_SSH_Key_Access	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack e_malicious_package/__i

		'meta': {'description': code that accesses or m keys in ~/.ssh director credential files.', 'au Skultety', 'category': 'credential_access'}, ' [{'identifier': '$ssh_d 'offset': 2144, 'matche '2e737368'}, {'identifi '$open_r', 'offset': 19 'matched_data': '6f7065 {'identifier': '$open_r 2358, 'matched_data': ' {'identifier': '$open_r 2514, 'matched_data': ' {'identifier': '$open_r 2892, 'matched_data': ' {'identifier': '$open_r 3067, 'matched_data': ' {'identifier': '$open_r 3467, 'matched_data': ' {'identifier': '$open_r 3742, 'matched_data': ' {'identifier': '$open_r 4956, 'matched_data': ' {'identifier': '$open_r 6004, 'matched_data': ' {'identifier': '$id_rsa 2196, 'matched_data': '69645f727361'}, {'iden '$id_rsa', 'offset': 22 'matched_data': '69645f
LOW	Suspicious_Persistence_Simulation	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack e_malicious_package/__i 'meta': {'description': code that creates persi mechanisms and also upd writes files.', 'author Skultety', 'category': 'persistence', 'priorit 'strings': [{'identifie 'offset': 3278, 'matche '63726f6e746162'}, {'id '$cron', 'offset': 3312 'matched_data': '63726f {'identifier': '$cron', 3341, 'matched_data': '63726f6e746162'}, {'id '$cron', 'offset': 3362

		'matched_data': '63726f {'identifier': '$cron', 3473, 'matched_data': '63726f6e746162'}, {'id '$cron', 'offset': 3748 'matched_data': '63726f {'identifier': '$open', 1945, 'matched_data': ' {'identifier': '$open', 2358, 'matched_data': ' {'identifier': '$open', 2514, 'matched_data': ' {'identifier': '$open', 2892, 'matched_data': ' {'identifier': '$open', 3067, 'matched_data': ' {'identifier': '$open', 3467, 'matched_data': ' {'identifier': '$open', 3742, 'matched_data': ' {'identifier': '$open', 4956, 'matched_data': ' {'identifier': '$open', 6004, 'matched_data': ' {'identifier': '$write' 4975, 'matched_data': '2e7772697465'}, {'iden '$write', 'offset': 608 'matched_data': '2e7772
HIGH	Suspicious_System_Info_Collection	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack e_malicious_package/__i 'meta': {'description': code that collects syst information such as use hostname, OS details, P version, and environmen variables.', 'author': Skultety', 'category': 'reconnaissance'}, 'str [{'identifier': '$uname 4402, 'matched_data': '706c6174666f726d2e756e {'identifier': '$getuse 4434, 'matched_data': '676574706173732e676574 {'identifier': '$hostna 'offset': 4522, 'matche '706c6174666f726d2e6e6f {'identifier': '$hostna

		'offset': 4622, 'matche '736f636b65742e67657468 5'}, {'identifier': '$s 'offset': 4555, 'matche '706c6174666f726d2e7379
HIGH	Suspicious_Process_Execution	{'file': 'sandbox/downloaded_pac d/sample_malicious_pack e_malicious_package/__i 'meta': {'description': code that opens or spaw processes using subproc modules, or executes su commands.', 'author': ' Skultety', 'category': 'strings': [{'identifie '$subprocess_popen', 'o 'matched_data': '737562707 26f636573732e {'identifier': '$subpro 'offset': 3730, 'matche '737562707 26f636573732e {'identifier': '$os_pop 'offset': 1941, 'matche '6f732e706f70656e'}, {' '$cmd1', 'offset': 1814 'matched_data': '637572 {'identifier': '$cmd1', 1913, 'matched_data': '6375726c20'}]}