info@wazuh.com
https://wazuh.com

Malware detection report

Verify that your systems are configured according to your security policies baseline.

2024-04-16T17:10:08 to 2024-05-16T17:10:08

rule.groups: rootcheck AND cluster.name: wazuh

Most common rootkits found among your agents

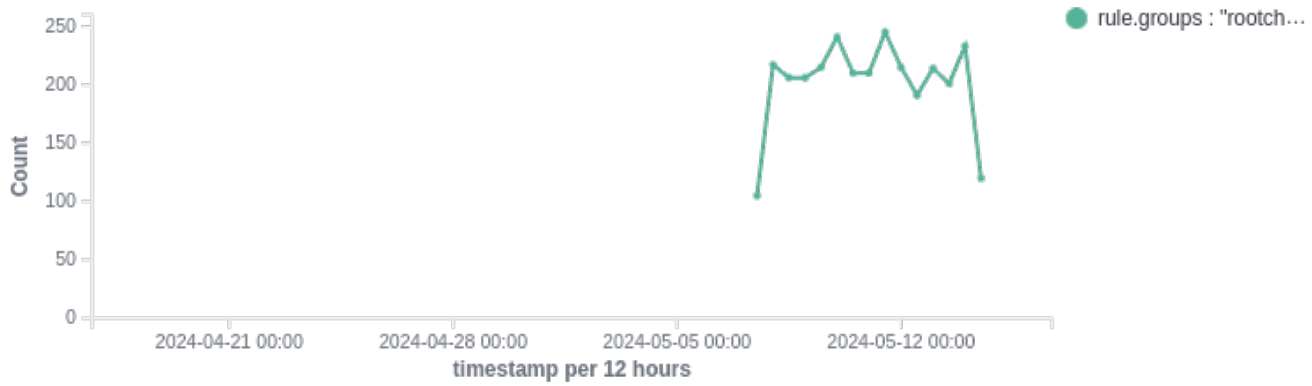
Rootkits are a set of software tools that enable an unauthorized user to gain control of a computer system without being detected.

Top	Rootkit
1	Omega
2	Volc
3	Monkit
4	Knark

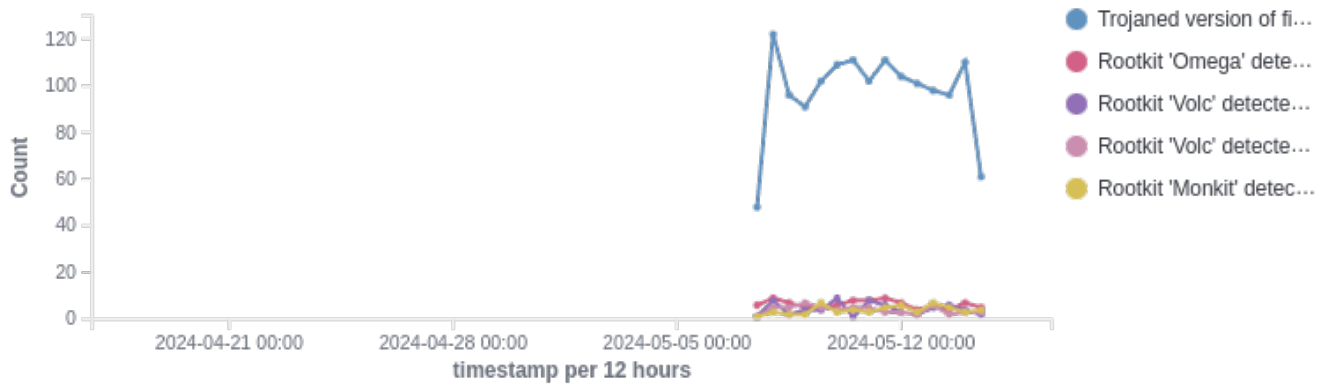
No agents have hidden processes

No agents have hidden ports

Emotet malware activity



Rootkits malware activity



Security alerts

Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id	Count
2024-05-07 12:00	ip-10-0-0-180.us-west-1.com	T1017	Lateral Movement	Windows Adware/Spyware a	9	518	2
2024-05-07 12:00	Ubuntu	T1017	Lateral Movement	Windows Adware/Spyware a	9	518	1
2024-05-08 00:00	RHEL7	T1017	Lateral Movement	Windows Adware/Spyware a	9	518	1
2024-05-08 12:00	RHEL7	T1017	Lateral Movement	Windows Adware/Spyware a	9	518	1

1 2

Alerts summary

Description	Control	Count
Host-based anomaly detection event (rootcheck).	Trojaned version of file detected.	1462
Host-based anomaly detection event (rootcheck).	Rootkit 'Omega' detected by the presence of file '/dev/chr'.	96
Host-based anomaly detection event (rootcheck).	Rootkit 'Volc' detected by the presence of file '/usr/bin/volc'.	65
Host-based anomaly detection event (rootcheck).	Rootkit 'Volc' detected by the presence of file '/usr/lib/volc'.	59
Host-based anomaly detection event (rootcheck).	Rootkit 'Monkit' detected by the presence of file '/usr/lib/libpikapp.a'.	58
Host-based anomaly detection event (rootcheck).	Rootkit 'Knark' detected by the presence of file '/dev/.pizda'.	57
Host-based anomaly detection event (rootcheck).	Rootkit 'Monkit' detected by the presence of file '/lib/defs'.	57
Host-based anomaly detection event (rootcheck).	Rootkit 'Knark' detected by the presence of file '/proc/knark'.	55
Host-based anomaly detection event (rootcheck).	Rootkit 'Bash' detected by the presence of file '/tmp/mclzaKmfa'.	50
Host-based anomaly detection event (rootcheck).	Rootkit 'TRK' detected by the presence of file '/usr/bin/sourcemask'.	49
Windows Adware/Spyware application found.	-	29