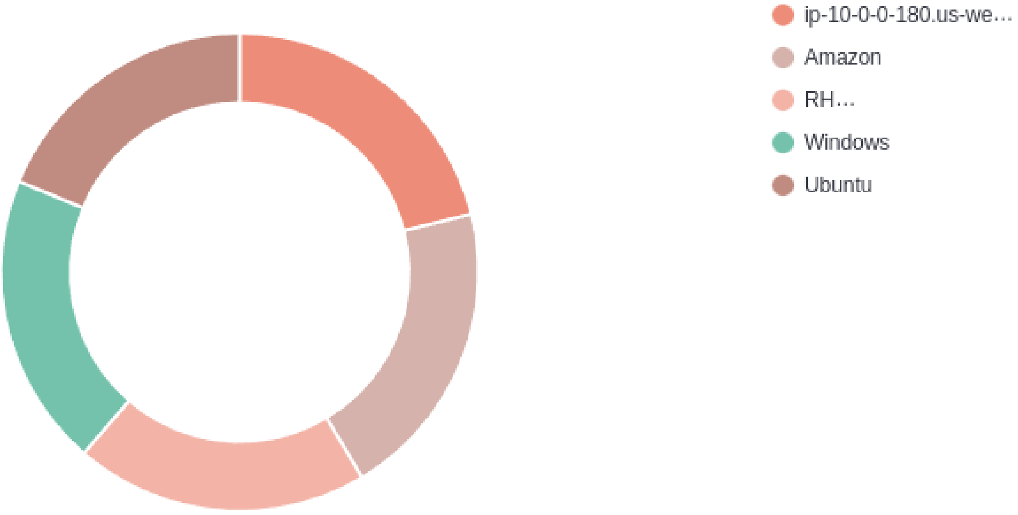
VirusTotal report

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

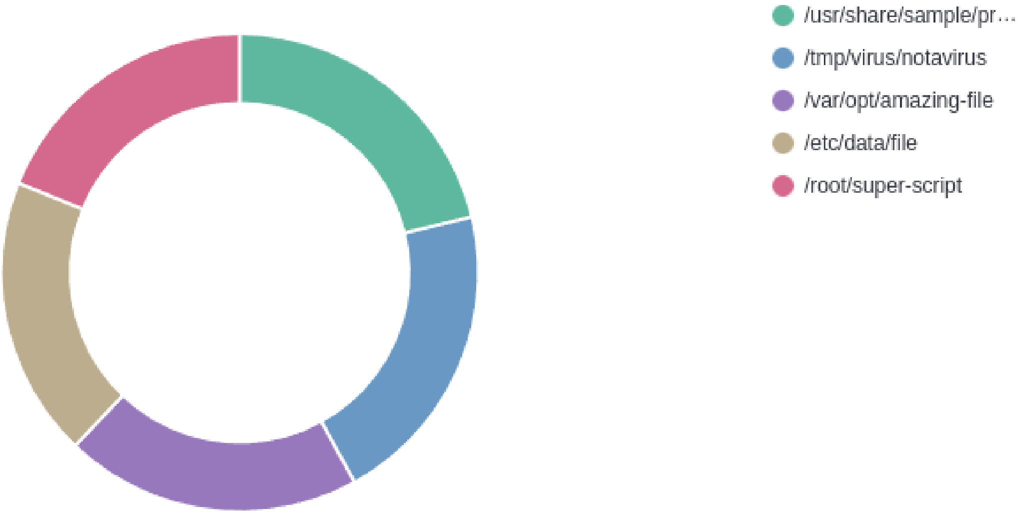
2024-04-16T17:35:48 to 2024-05-16T17:35:48

cluster.name: wazuh AND rule.groups: virustotal

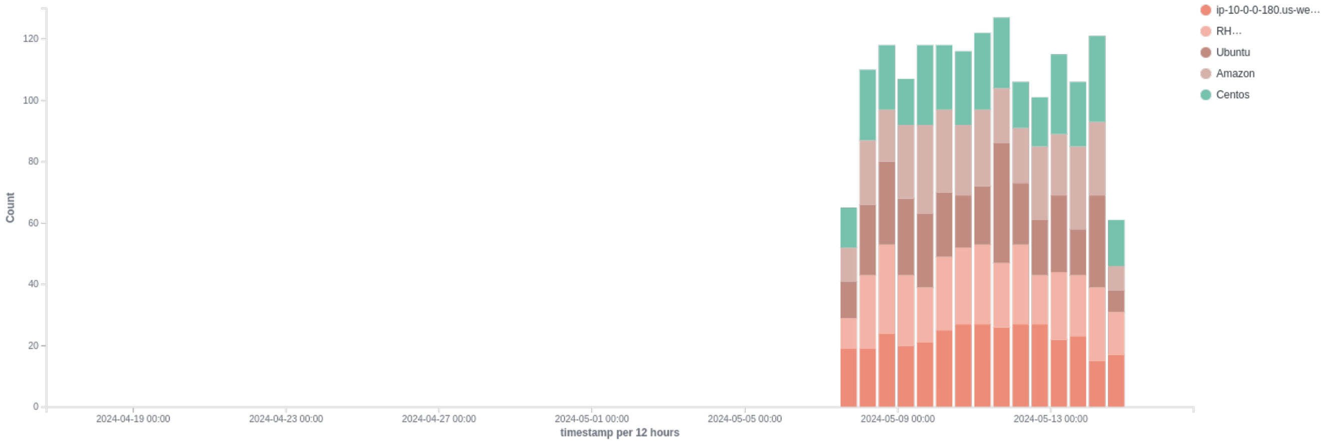
Top 5 agents with unique malicious files



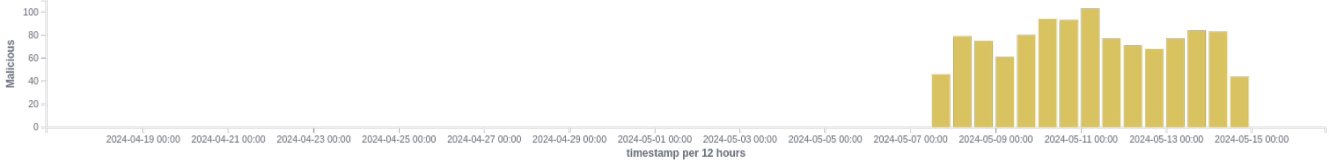
Last scanned files



Alerts evolution by agents



Malicious files alerts evolution



Last files

File	Link	Count
/usr/share/sample/program	https://www.virustotal.com/gui/file/1bbf37332af75ea682fb4523afc8e61adb22f47	49
/tmp/virus/notavirus	https://www.virustotal.com/file/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa	59
/var/opt/amazing-file	https://www.virustotal.com/file/275a021bbfb6489e54d471899f7db9d1663fc695e	56
/etc/data/file	https://www.virustotal.com/file/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa	46
/root/super-script	https://www.virustotal.com/file/275a021bbfb6489e54d471899f7db9d1663fc695e	45
/etc/sample/script	https://www.virustotal.com/gui/file/1bbf37332af75ea682fb4523afc8e61adb22f47	43

‹ 1 ›

1,135

- Total malicious -

2,259

- Total Positives -

3,000

- Total -

Alerts summary

Rule ID	Description	Level	Count
1101	VirusTotal: Alert - No records in VirusTotal database	10	1
1101	VirusTotal: Alert - No records in VirusTotal database	15	1
1101	VirusTotal: Alert - /etc/data/file - 4 engines detected this file	15	1
1101	VirusTotal: Alert - /etc/data/file - 54 engines detected this file	7	1
1585	VirusTotal: Alert - /etc/data/file - 7 engines detected this file	4	1
1585	VirusTotal: Alert - /etc/sample/script - 51 engines detected this file	12	1
1585	VirusTotal: Alert - /usr/share/sample/program - 6 engines detected this file	2	1
1585	VirusTotal: Alert - No records in VirusTotal database	1	1
2407	VirusTotal: Alert - /etc/sample/script - 26 engines detected this file	8	1
2407	VirusTotal: Alert - /tmp/virus/notavirus - 3 engines detected this file	7	1
2407	VirusTotal: Alert - /usr/share/sample/program - 10 engines detected this file	2	1
2407	VirusTotal: Alert - No records in VirusTotal database	5	1
2717	VirusTotal: Alert - /etc/data/file - 58 engines detected this file	6	1
2717	VirusTotal: Alert - /tmp/virus/notavirus - 5 engines detected this file	3	1
2717	VirusTotal: Alert - /usr/share/sample/program - 40 engines detected this file	6	1
2717	VirusTotal: Alert - /var/opt/amazing-file - 37 engines detected this file	15	1
273	VirusTotal: Alert - /etc/data/file - 39 engines detected this file	1	1
273	VirusTotal: Alert - /etc/data/file - 8 engines detected this file	5	1
273	VirusTotal: Alert - /tmp/virus/notavirus - 58 engines detected this file	9	1
273	VirusTotal: Alert - /tmp/virus/notavirus - 60 engines detected this file	15	1
2807	VirusTotal: Alert - /etc/data/file - 52 engines detected this file	9	1
2807	VirusTotal: Alert - /var/opt/amazing-file - 50 engines detected this file	6	1
2807	VirusTotal: Alert - /var/opt/amazing-file - 55 engines detected this file	4	1
2807	VirusTotal: Alert - No records in VirusTotal database	14	1
3379	VirusTotal: Alert - No records in VirusTotal database	2	1
3379	VirusTotal: Alert - No records in VirusTotal database	11	1
3379	VirusTotal: Alert - /usr/share/sample/program - 50 engines detected this file	3	1
3379	VirusTotal: Alert - /var/opt/amazing-file - 50 engines detected this file	14	1
357	VirusTotal: Alert - /root/super-script - 44 engines detected this file	2	1
357	VirusTotal: Alert - /var/opt/amazing-file - 28 engines detected this file	11	1
357	VirusTotal: Alert - /var/opt/amazing-file - 63 engines detected this file	7	1
357	VirusTotal: Alert - No records in VirusTotal database	10	1
3936	VirusTotal: Alert - /tmp/virus/notavirus - 0 engines detected this file	15	1
3936	VirusTotal: Alert - /tmp/virus/notavirus - 27 engines detected this file	14	1
3936	VirusTotal: Alert - /var/opt/amazing-file - 39 engines detected this file	3	1
3936	VirusTotal: Alert - No records in VirusTotal database	9	1
4029	VirusTotal: Alert - /root/super-script - 31 engines detected this file	15	1
4029	VirusTotal: Alert - /root/super-script - 64 engines detected this file	3	1
4029	VirusTotal: Alert - /var/opt/amazing-file - 61 engines detected this file	5	1

Rule ID	Description	Level	Count
4029	VirusTotal: Alert - No records in VirusTotal database	14	1
4241	VirusTotal: Alert - /root/super-script - 12 engines detected this file	7	1
4241	VirusTotal: Alert - /root/super-script - 41 engines detected this file	4	1
4241	VirusTotal: Alert - /root/super-script - 49 engines detected this file	9	1
4241	VirusTotal: Alert - /var/opt/amazing-file - 24 engines detected this file	6	1
4515	VirusTotal: Alert - /etc/sample/script - 6 engines detected this file	8	1
4515	VirusTotal: Alert - /root/super-script - 5 engines detected this file	3	1
4515	VirusTotal: Alert - /tmp/virus/notavirus - 37 engines detected this file	11	1
4515	VirusTotal: Alert - /var/opt/amazing-file - 26 engines detected this file	5	1
4810	VirusTotal: Alert - /tmp/virus/notavirus - 38 engines detected this file	4	1
4810	VirusTotal: Alert - /usr/share/sample/program - 27 engines detected this file	9	1
4810	VirusTotal: Alert - /usr/share/sample/program - 57 engines detected this file	4	1
4810	VirusTotal: Alert - No records in VirusTotal database	13	1
4959	VirusTotal: Alert - No records in VirusTotal database	1	1
4959	VirusTotal: Alert - No records in VirusTotal database	5	1
4959	VirusTotal: Alert - No records in VirusTotal database	14	1
4959	VirusTotal: Alert - /tmp/virus/notavirus - 33 engines detected this file	7	1
5123	VirusTotal: Alert - /etc/data/file - 24 engines detected this file	6	1
5123	VirusTotal: Alert - /root/super-script - 36 engines detected this file	5	1
5123	VirusTotal: Alert - /tmp/virus/notavirus - 24 engines detected this file	15	1
5123	VirusTotal: Alert - /var/opt/amazing-file - 38 engines detected this file	10	1
5137	VirusTotal: Alert - /etc/data/file - 31 engines detected this file	3	1
5137	VirusTotal: Alert - /etc/sample/script - 15 engines detected this file	3	1
5137	VirusTotal: Alert - /usr/share/sample/program - 18 engines detected this file	11	1
5137	VirusTotal: Alert - No records in VirusTotal database	4	1
5872	VirusTotal: Alert - /root/super-script - 37 engines detected this file	10	1
5872	VirusTotal: Alert - /tmp/virus/notavirus - 42 engines detected this file	8	1
5872	VirusTotal: Alert - /var/opt/amazing-file - 52 engines detected this file	1	1
5872	VirusTotal: Alert - No records in VirusTotal database	6	1
1138	VirusTotal: Alert - /etc/data/file - 50 engines detected this file	1	1
1138	VirusTotal: Alert - /var/opt/amazing-file - 25 engines detected this file	2	1
1138	VirusTotal: Alert - No records in VirusTotal database	6	1
1269	VirusTotal: Alert - No records in VirusTotal database	3	1
1269	VirusTotal: Alert - No records in VirusTotal database	12	1
1269	VirusTotal: Alert - /etc/data/file - 62 engines detected this file	4	1
129	VirusTotal: Alert - No records in VirusTotal database	2	1
129	VirusTotal: Alert - No records in VirusTotal database	6	1
129	VirusTotal: Alert - /etc/sample/script - 2 engines detected this file	15	1
1322	VirusTotal: Alert - /etc/data/file - 45 engines detected this file	10	1
1322	VirusTotal: Alert - /etc/sample/script - 53 engines detected this file	14	1
1322	VirusTotal: Alert - /usr/share/sample/program - 37 engines detected this file	2	1

Rule ID	Description	Level	Count
1412	VirusTotal: Alert - /etc/data/file - 30 engines detected this file	3	1
1412	VirusTotal: Alert - /root/super-script - 51 engines detected this file	13	1
1412	VirusTotal: Alert - /root/super-script - 60 engines detected this file	11	1
1512	VirusTotal: Alert - /root/super-script - 46 engines detected this file	15	1
1512	VirusTotal: Alert - /tmp/virus/notavirus - 28 engines detected this file	1	1
1512	VirusTotal: Alert - /tmp/virus/notavirus - 47 engines detected this file	10	1
1577	VirusTotal: Alert - /root/super-script - 54 engines detected this file	14	1
1577	VirusTotal: Alert - /tmp/virus/notavirus - 0 engines detected this file	2	1
1577	VirusTotal: Alert - /var/opt/amazing-file - 14 engines detected this file	11	1
1761	VirusTotal: Alert - /etc/data/file - 33 engines detected this file	8	1
1761	VirusTotal: Alert - /usr/share/sample/program - 49 engines detected this file	1	1
1761	VirusTotal: Alert - /var/opt/amazing-file - 9 engines detected this file	10	1
1798	VirusTotal: Alert - /root/super-script - 8 engines detected this file	4	1
1798	VirusTotal: Alert - /usr/share/sample/program - 33 engines detected this file	3	1
1798	VirusTotal: Alert - /usr/share/sample/program - 57 engines detected this file	7	1
1821	VirusTotal: Alert - /etc/data/file - 61 engines detected this file	3	1
1821	VirusTotal: Alert - /etc/sample/script - 17 engines detected this file	12	1
1821	VirusTotal: Alert - /tmp/virus/notavirus - 51 engines detected this file	8	1
2176	VirusTotal: Alert - /etc/data/file - 41 engines detected this file	9	1