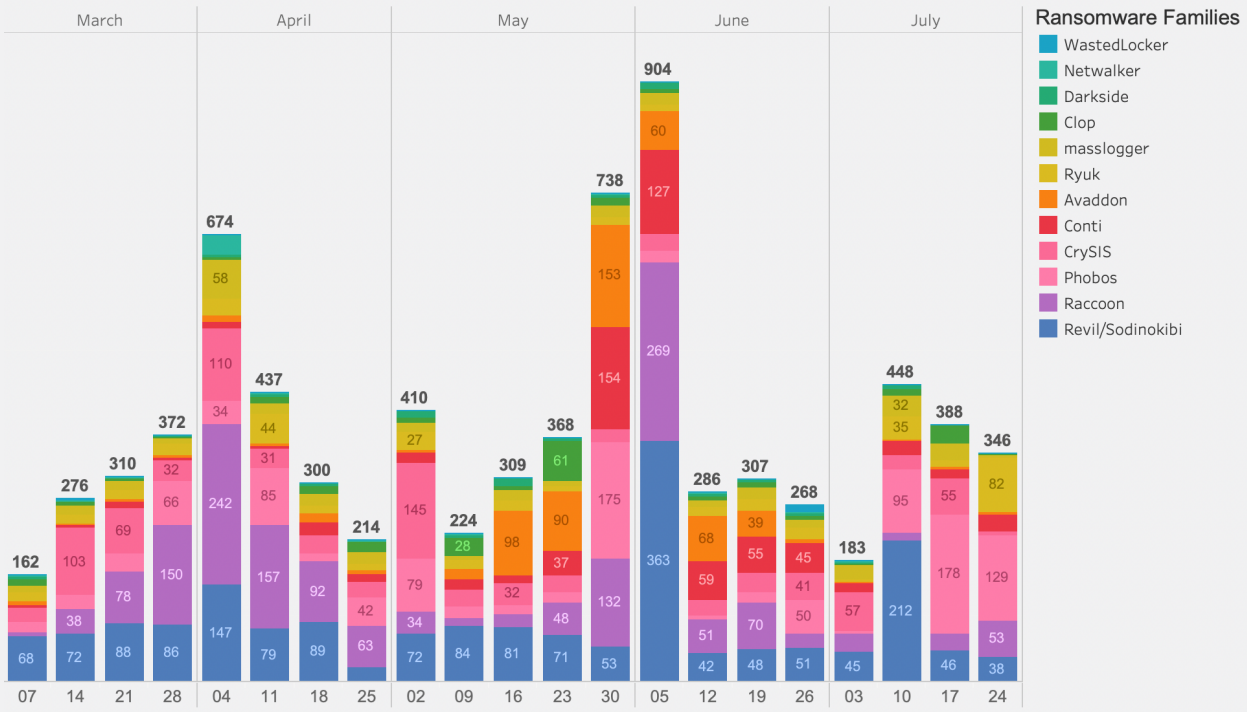
POLYSWARM

# Trending **Ransomware** Report

Report Sample -Random period-

This report reflects the types and respective volume of particular ransomware families that have targeted our customers and malware partners in the previous month.

## Weekly trend




## Period over period variance: context

- Raccoon (75%)
  - Raccoon is an information stealer used by cybercriminals to steal credentials that includes cryptocurrency wallets, credit card information, and user passwords. A new campaign, which uses a privacy tool as a lure has been spreading Raccoon stealer to target victims as its second stage payload

    Examples of recent 'First Seen' before VirusTotal:
    - 289ba811233a782f75871f0b1a4417ff458308bc24f67c2527dc04f05431b2aa
    - 011fd88065a43bfdc21c2e68cb9935edb235d943f8de642b4fc253377729196b

        - e5e6bdcd2631e986034d4472d258ed326256a9280dd5d97b7c6e0ad2cbd6335f

- Ryuk (154%)
    - Ryuk is back with a new variant that is targeting web servers. The ransomware gang, to add more pressure for the victims to pay, is impairing public websites with a Ryuk ransom note

      Examples of recent 'First Seen' before VirusTotal:
        - 18423515a069e92191f5f90a6eaf5d620b8588918a854575433f56703391bff5
        - 2b7cdaf1839a1d95be70a4a4f80b130171ea84c8fcd07f869eff5346c77a3e7d
        - 16af09eb9b70c967b0c97f41e4228d7277f8127cceabb7f332a9c42a85ec16ee

- Lockbit (+411%)
    - Lockbit is believed to be affiliated with a Russian ransomware gang and It was recently revealed that the operators behind are targeting companies with cyber insurance because experts will come in to handle the situation and they will end up getting paid. Lockbit recently introduced a new affiliate program that offers "the fastest data exfiltration in the market through a new tool called 'StealBit,' which can download 100 GB of data from compromised systems in just under 20 minutes.

      Examples of recent 'First Seen' before VirusTotal:
        - da9dc90b69e36c26676a335084256a6d32a7b008126cc5f94dd2a005edfa83f8
        - 50ae588921943ebd79715a559d221eadb3183958753d93e4637782e06cde8b94
        - 0d9825e26b0d58e74fcdaa09c73ab8e4f6bbe1ca4ded0ff601bb8d83ceba8d5c

- REvil/Sodinokibi (up 138%)
    - Dubbed as Russia's most aggressive ransomware, it has been very active recently. Among one of its highest profile campaigns we find an attack on a major meta supplier. Although the ransomware is prevalent due to the aggressiveness of the gang behind it, the network infrastructure supporting its ransom pages suddenly vanished as observed on July 13, 2021.

      Examples of recent 'First Seen' before VirusTotal:
        - f984ace0dd3d87323ca60a5e3297d1e53f6202c9fbd3a6b623a5755ff1506a89
        - a8fb86d92f347cce05681a76232306df5b48c0a5b1caf2047c13c33c88e74e73
        - 8b0906e6307a043163b0a0e6ea42be6a9b86a4d625617ce6490ed0ca4cc7bf00

- Phobos (-69%)
    - Recently upgraded to include fileless and evasive techniques to bypass detection technologies. It utilizes a paste site to host encrypted components, a typical abuse of free services to hide malware in plain sight. After the discovery of this abuse, the paste sites took down those pages that were hosting the ransomware.

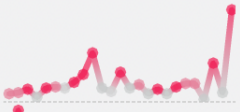
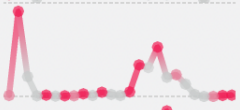
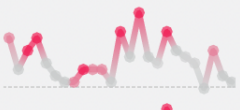
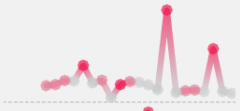
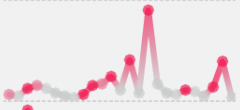
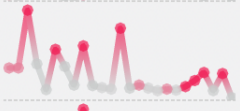
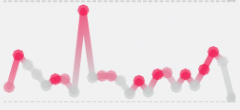
      Examples of recent 'First Seen' before VirusTotal:
        - f984ace0dd3d87323ca60a5e3297d1e53f6202c9fbd3a6b623a5755ff1506a89

- a8fb86d92f347cce05681a76232306df5b48c0a5b1caf2047c13c33c88e74e73
- 8b0906e6307a043163b0a0e6ea42be6a9b86a4d625617ce6490ed0ca4cc7bf00

## Period over period comparison

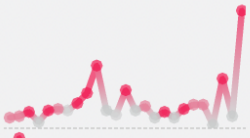
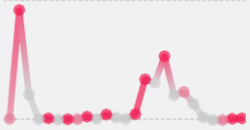
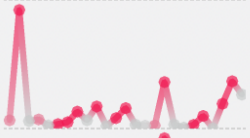
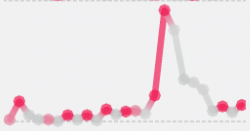
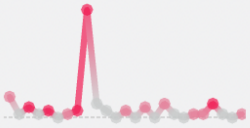
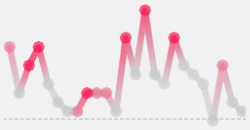
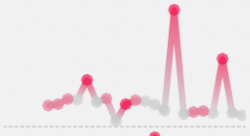
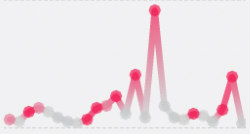
Fresh samples for many of the above-mentioned ransomware families have been added to our portal.

-100% 100%

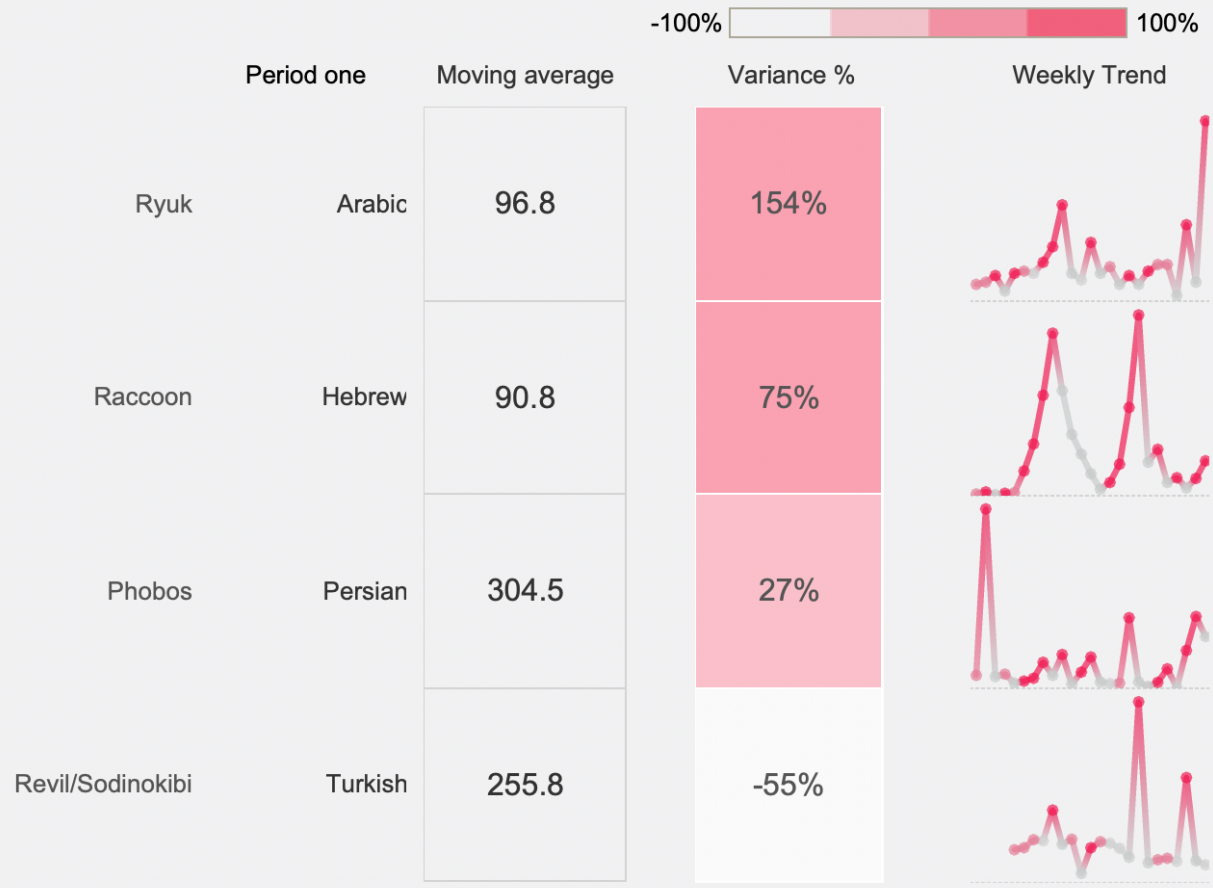
| | Period one | Moving average | Variance % | Weekly Trend |
|---|---|---|---|---|
| Ryuk | 82 | 32.3 | 154% |  |
| Avaddon | 5 | 2.8 | 82% |  |
| Raccoon | 53 | 30.3 | 75% |  |
| Phobos | 129 | 101.5 | 27% |  |
| Conti | 24 | 19.0 | 26% |  |
| Netwalker | 1 | 1.5 | -33% |  |
| Darkside | 1 | 2.3 | -56% |  |
| Revil/Sodinokibi | 38 | 85.3 | -55% |  |
| Clop | 3 | 11.0 | -73% |  |
| CrySIS | 7 | 35.0 | -80% |  |
| masslogger | 3 | 20.5 | -85% |  |

## Language-based samples by region

- **APAC**

| | Period one | Moving average | Variance % | Weekly Trend |
|---|---|---|---|---|
| Chinese | 273 | 80.6 | 154% |  |
| Korean | 17 | 6.9 | 82% |  |
| Japenese | 177 | 75.6 | 75% |  |
| Hindi | 430 | 253.8 | 27% |  |
| Korean | 80 | 47.5 | 26% |  |
| Indonesian | 3 | 3.8 | -33% |  |
| Thai | 3 | 5.6 | -56% |  |
| Vietnamese | 127 | 213.1 | -55% |  |
| Malai | 10 | 27.5 | -73% |  |

- **MENA**


-100%
100%
Period one
Moving average
Variance %
Weekly Trend
Ryuk
Arabic
96.8
154%
Raccoon
Hebrew
90.8
75%
Phobos
Persian
304.5
27%
Revil/Sodinokibi
Turkish
255.8
-55%