cybersixgill

# Cybersixgill's Malware Report (Weekly)

2024-08-26

## Top 10 Most Popular Malware

In the last 7 days, the most popular malware discussed in the underground has been lumma.

| |
|---|
| lumma |
| lumma stealer |
| vidar |
| hamsa |
| stealc |
| evilginx |
| redline |
| redline stealer |
| ninja |
| samurai |

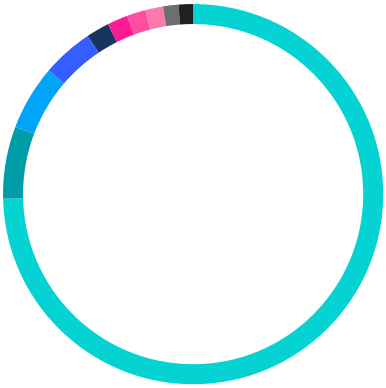
## Top Malware-related Forums

In the last 7 days, these have been the most popular forums where threat actors have been discussing malware, accounting for 83% of all forum conversations on malware.

| | |
|---|---|
| 4chan | **62%** |
| rutor | **6%** |
| xss | **5%** |
| prizrak | **4%** |
| cracked | **5%** |
| jvarchive | **5%** |
| labrc | **4%** |
| turkhackteam | **3%** |
| carmasters | **3%** |
| exploit | **3%** |

## Top Malware-related Telegram groups

In the last 7 days, these have been the most popular Telegram groups where threat actors have been discussing malware.



| | |
|---|---|
| ◆ ◆1519348402) ◆◆תילא/מרכז/דרום/צפון כיוון) | 74% |
| ◆ PUSAT PROMOSI (1392352091) | 6% |
| ◆ LummaC2 | Public (1944757940) | 5% |
| ◆ SPYHACKERZ {PRIV} SOCIALS | OFFICIAL GROUP (1261870274) | 4% |
| ◆ Combos grupo plex Email pass y user pass (1711430236) | 1% |
| ◆ Loaders and Carders(worldwide) ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆ (1454251053) | 2% |
| ◆ GOD OF BANKS (1687602916) | 2% |
| ◆ BlessUp 4PF◆◆ (1753420350) | 2% |
| ◆ Handelgroep (1207791184) | 2% |
| ◆ C BANKS ◆◆ (1692941424) | 2% |

## Top Malware-related Discord groups

In the last 7 days, these have been the most popular Discord groups where threat actors have been discussing malware.

| | |
|---|---|
| HackTheBox | **40%** |
| Grey Hack | **14%** |
| The BDS World | **9%** |
| TASVideos.org Official Discord Channel | **6%** |
| Dropout Phreaks | **6%** |
| Sneakers | **6%** |
| WhiteHat Hacking | **6%** |
| Raptoreum | **5%** |
| /r/Droger | **4%** |
| Moon Cooks | **4%** |

## Fully Undetectable (FUD) Malware

Threat actors often mention the acronym FUD - Fully undetectable - with relation to malware, suggesting that the malicious software is not detectable by common anti-virus vendors.

In the last 7 days, Cybersixgill detected the following conversations mentioning FUD malware in the underground.

| |
|---|
| CRAXS-RAT-VIP |
| TheFatRat |
| 500-tools |
| FUD-APK-CRYPTER |
| XWorm-Rat |
| bo2k168kb-stealer |