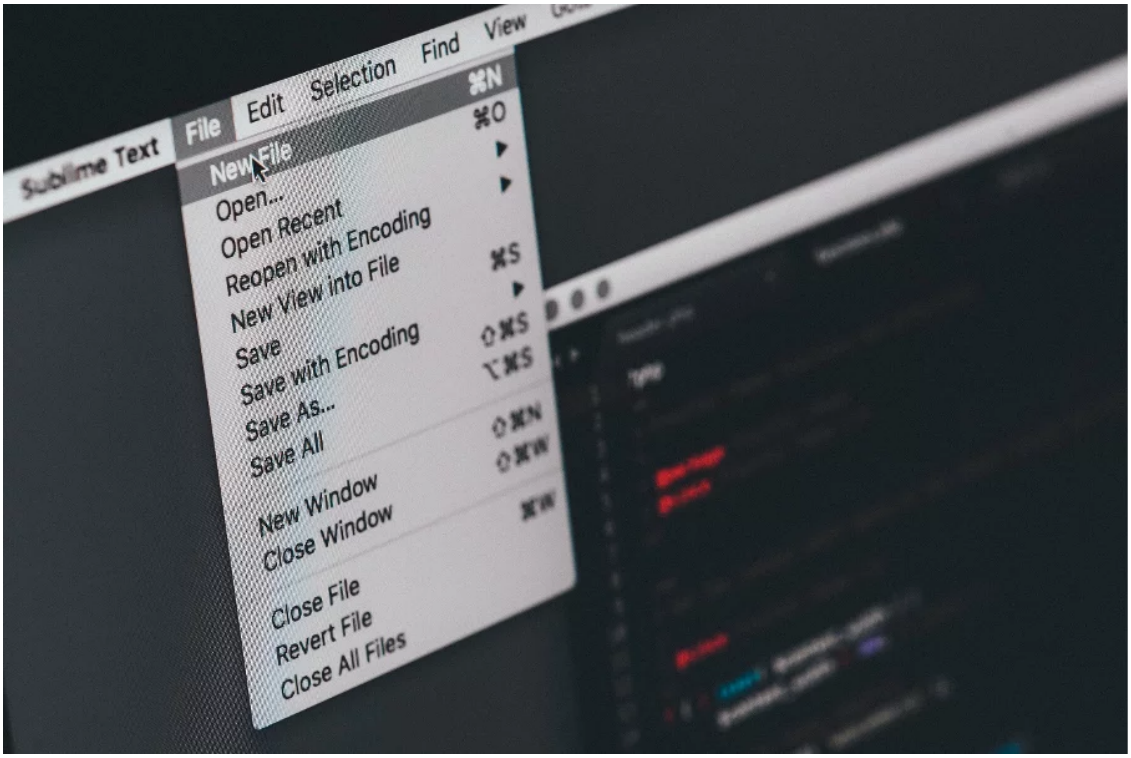
PDF files more dangerous than Executables – Report reveals



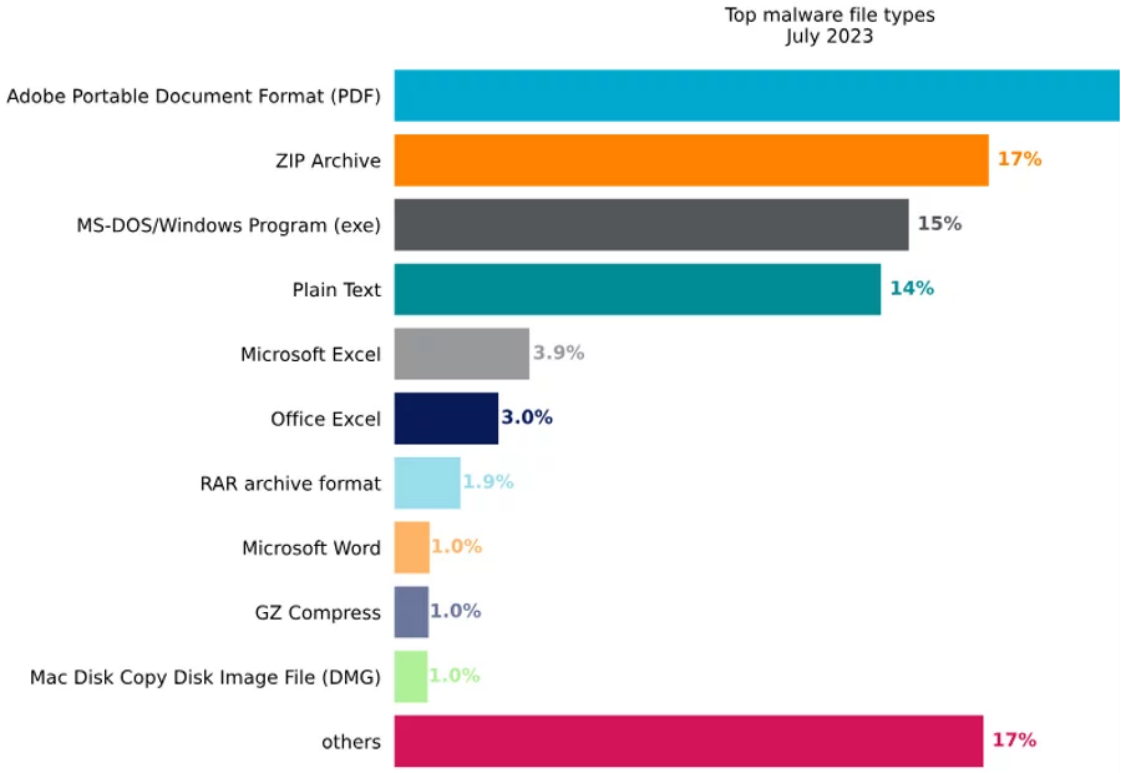
By: Daniel Iwugo

Last week, Netskope's Threat Labs released a statistics report for July, 2023 with the aim of providing insights into active threats against organisations.

Netskope is a cybersecurity company based in the United States, specializing in cloud and network security. The report concentrated primarily on malware delivery, types, and families.

Report Details

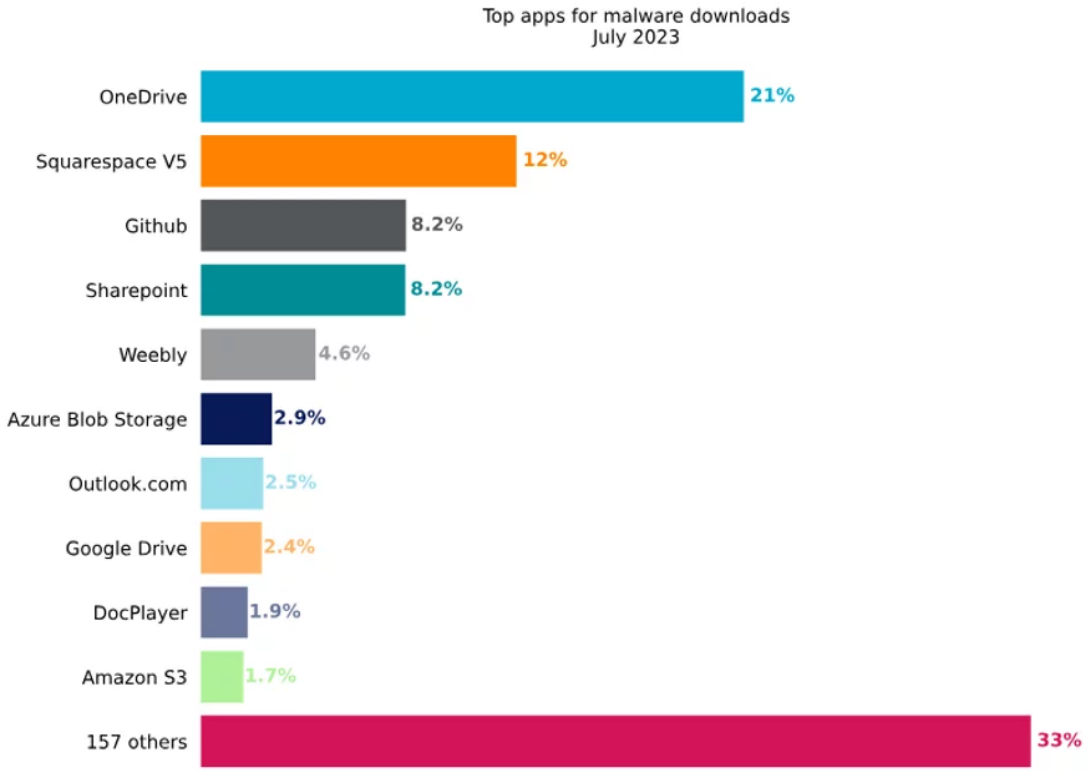
According to the report, malicious PDF files took first place as the most common malware file type. Closely followed behind was ZIP archive files, which could possibly be attributed to SFX archives. Third place was Microsoft Windows Executable files, followed by Plain text and Microsoft Excel files.



Top malware file types ¦ Source: Netskope

Netskope also delivered reports on cloud malware delivery, noting that 57% of all malware downloads originated from cloud hosted apps. 167 apps were also found to host malware, which is a slight increase from just over 120 back in January.

Microsoft's OneDrive stayed at the top of the list, with Squarespace, GitHub, SharePoint, and Weebly following close behind. It was noted that the total percentage of cloud downloads from OneDrive had fallen, indicating that threat actors are possibly moving to more viable hosting options.



Top apps for malware downloads ¦ Source: Netskope

Threat actors seemed to getting more creative, as 71% of malware downloads detected by Netskope were either new variants of pre-existing ones, or new entire families. Trojans took the top spot with 56%, with fishing lures, backdoors and file-based exploits in second and third place respectively.

Mitigations

Here are some suggestions to protect you and your organisation from cloud-based malware:

1. Inspect all web and cloud downloads carefully.
2. Ensure security controls inspect the content of popular archive files.
3. Setup policies to block downloads from apps and sites that not necessarily used.
4. Block downloads of files from newly registered domains.

Tags: ADVISORY APT CYBERSECURITY ESPIONAGE MALWARE

RECENT POSTS

The CYSED Dictionary: Email

What is Dark AI?

PDF files more dangerous than Executables – Report reveals

ALL CATEGORIES

Awareness

Bussiness

Child Online Safety

Cybercrime