



:> Overview

The results depicted here are based on the submissions from The Portuguese Abuse Open Feed - [@xSI_f33d](#) - during the fourth quarter, Q4, of 2020 in Portugal. This infographic includes an analysis of the phishing and malware campaigns that targeted Portuguese citizens.

:> Phishing and Malware Q4 2020

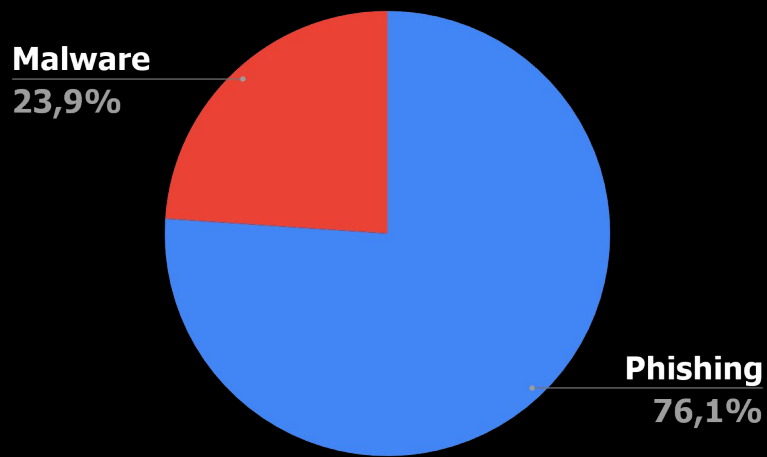


Figure 1: Volume of phishing and malware submissions (376) during Sep - Dec 2020 in Portugal.

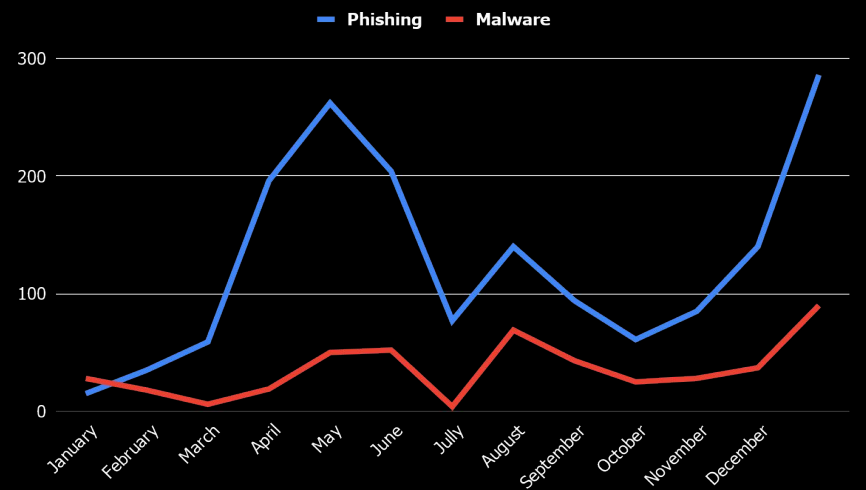


Figure 2: Number of phishing and malware campaigns from Jan to Dec of the year 2020.

:> Malware by Numbers

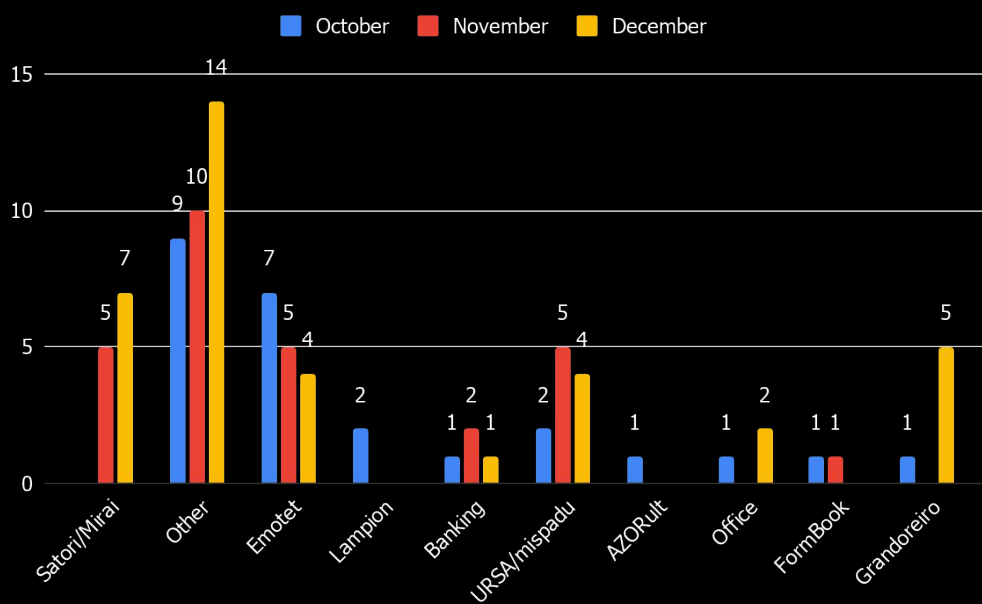


Figure 3: Number of malware submissions by category, during Q4 2020 in Portugal.

Malware Campaigns

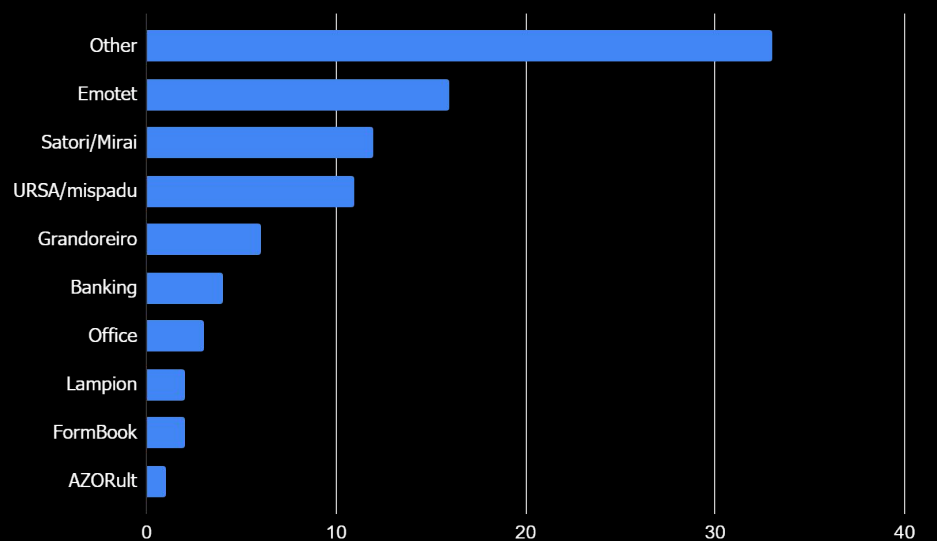


Figure 4: Comparison of overall malware samples (90) collected during Q4 2020 in Portugal.

:> Threats by Sector

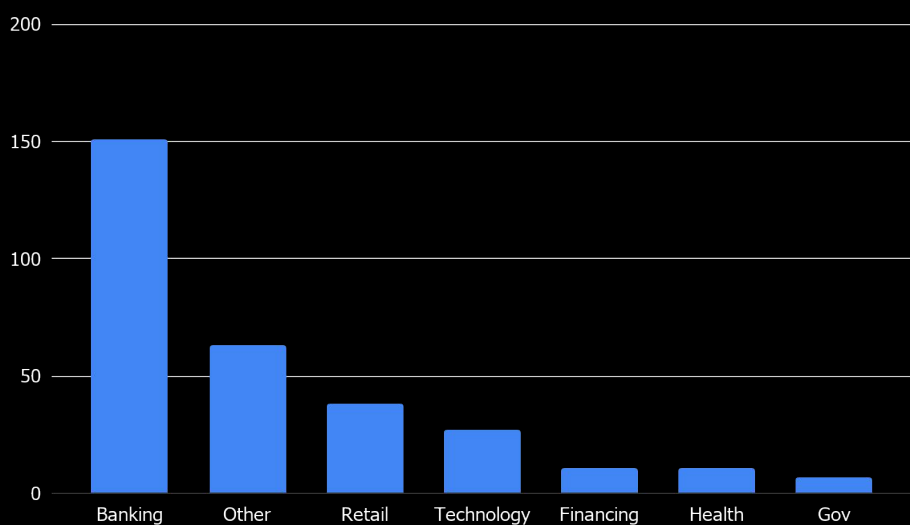


Figure 5: Number of phishing and malware campaigns by sector during Q4 2020 in Portugal.

:> Final Thoughts

Through the results obtained it is possible to verify that there was an increased number of phishing campaigns in Q4 2020 in contrast to Q3. One of the reasons that can explain this increase, was the **ANUBIS** campaign that occurred between Nov and Dec 2020 in Portugal.

In terms of malware, **Satori/Mirai** botnet, **Emotet**, and **URSA** trojan were the most active during Oct - Dez 2020. Also, **Grandoreiro** has been observed in December 2020.

Regarding the affected sectors, **Banking** was the most affected, followed by **Retail** and lastly by **Technology**.