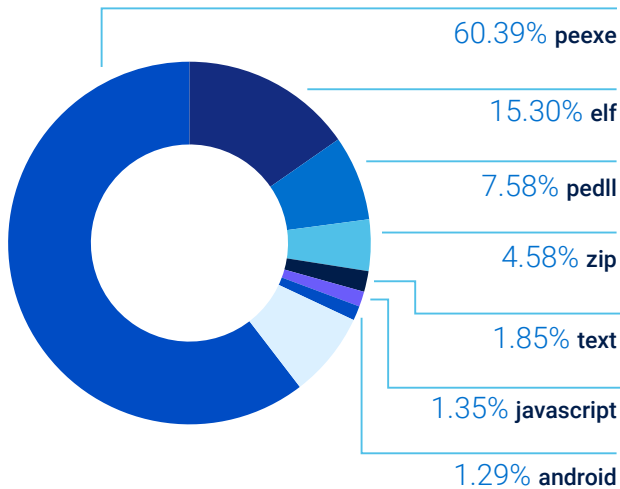


Malware

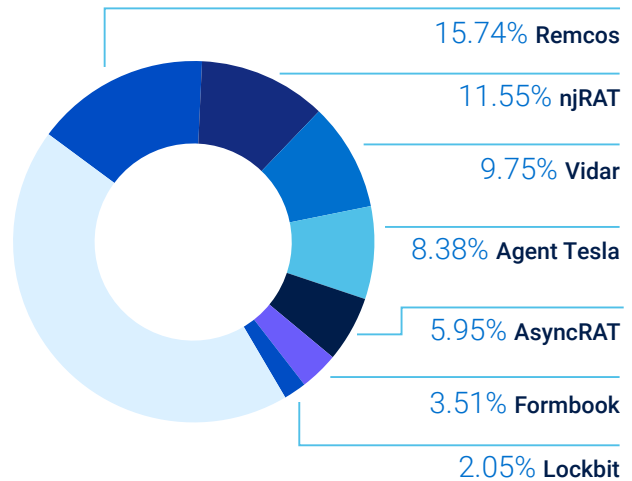
2024 Q1 Global Threat Intelligence Report



FILE TYPE



TRENDING MALWARE



SEVERITY



SECURITY VENDOR DETECTION RATE



NOTEWORTHY MALWARE CAMPAIGNS

- Ivanti Connect Secure zero-day vulnerabilities exploited to deploy multiple malware families
- Water Hydra exploited a Microsoft Defender SmartScreen zero-day to drop DarkMe malware
- DarkGate malware campaign used zero-day in Microsoft Defender to infect users
- Russia-linked COLDRIVER evolves, leveraging custom malware based on Google TAG research
- PurpleFox malware campaign infects thousands of computers in the Ukraine
- MoqHao campaign targets Android users located in Europe and Asia