Related Insights

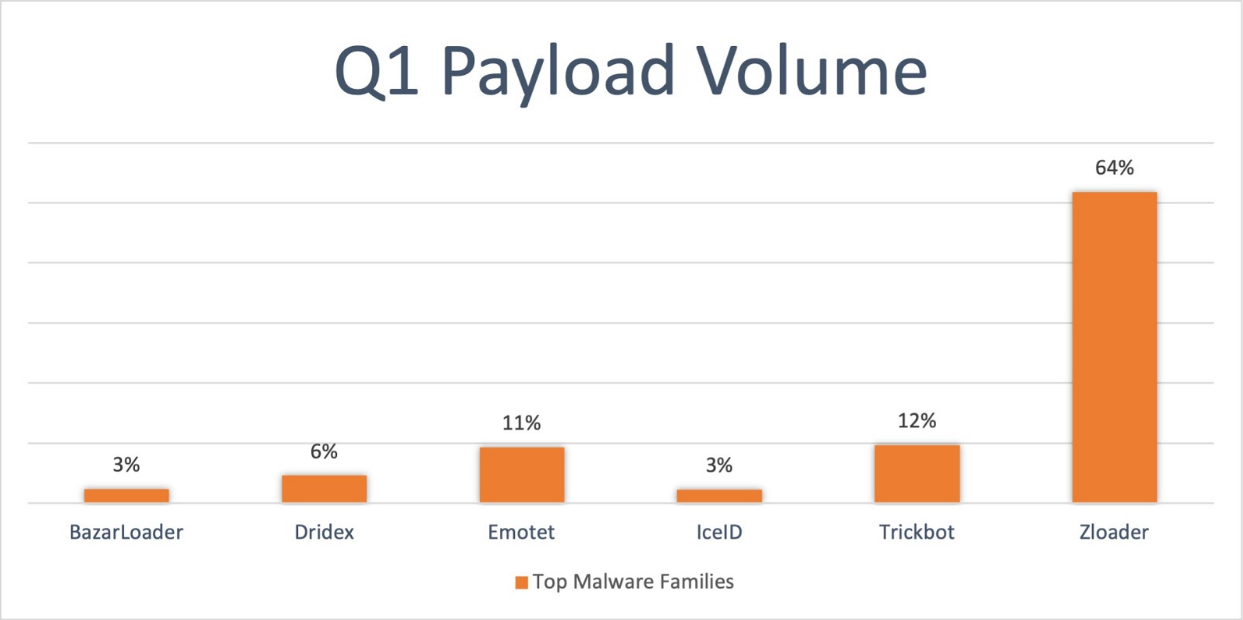
April 21, 2021

Get The Latest Insights

By Jessica Ellis | April 21, 2021

Malicious payloads delivered via email phishing continue to drive access to sensitive infrastructures and result in data compromise for enterprises. In Q1 of 2021, attack methods including malware campaigns have contributed to a 564% increase in individuals affected by a data leak, as well as a 12% increase in publicly-reported compromise.
As we continue to see leaks and widespread reports of ransomware attacks on organizations that may result in data made public, PhishLabs is monitoring the reported volume of payloads identified in user inboxes. The below are the top malware families targeting enterprises during Q1.

In Q1, ZLoader comprised almost 65% of all reported payload activity, dominating the overall volume of desktop malware. Although ZLoader started 2021 quietly, a one-day spike in attacks during February represented one of the greatest upticks for a single payload that we have observed in a 24-hour period in over a year.

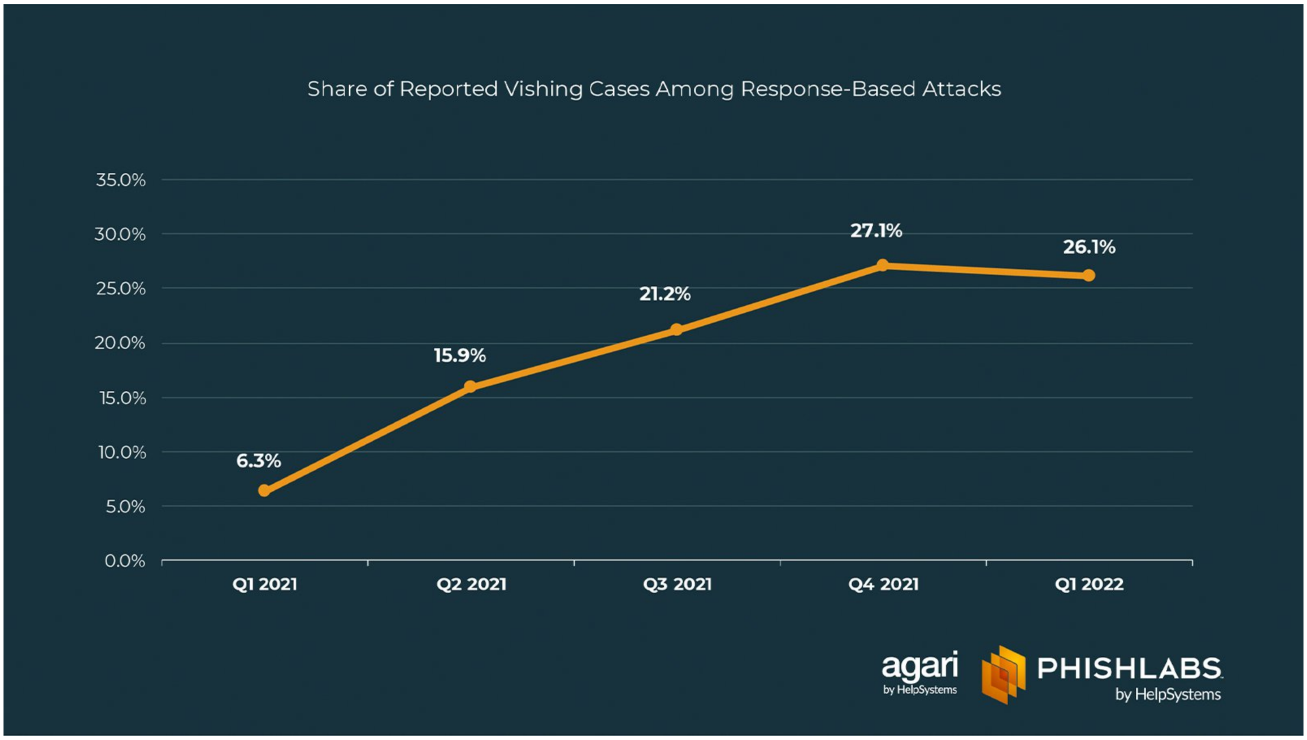


Since then, ZLoader has shown a strong presence, owning 79% of dropper activity in March. ZLoader is a multi purpose malware-as-a-service (MaaS) that has maintained consistently high activity since 5/1/2020.

Trickbot was reported in 12% of all payload attacks during Q1, with activity prompting a Joint Cybersecurity Advisory from CISA and the FBI. This represents a 15% increase in attacks from Q4 2020.
Although attacks grew, Trickbot numbers still barely overcame the volume of former leading malware Emotet, before Emotet operations were dismantled. Emotet was the dominant MaaS for threat actors prior to January.
Despite ZLoader operators deploying a significantly higher level of attacks during Q1, the overall volume of reported payload families decreased by 14% from Q4 2020. This is the lowest number of overall payload volume since Q2 2020.

This decrease could indicate that threat actors are increasingly using malware associated with MaaS models to carry out attacks, rather than creating campaigns around a broader variety of families not traditionally linked with these services.

Additional Resources:

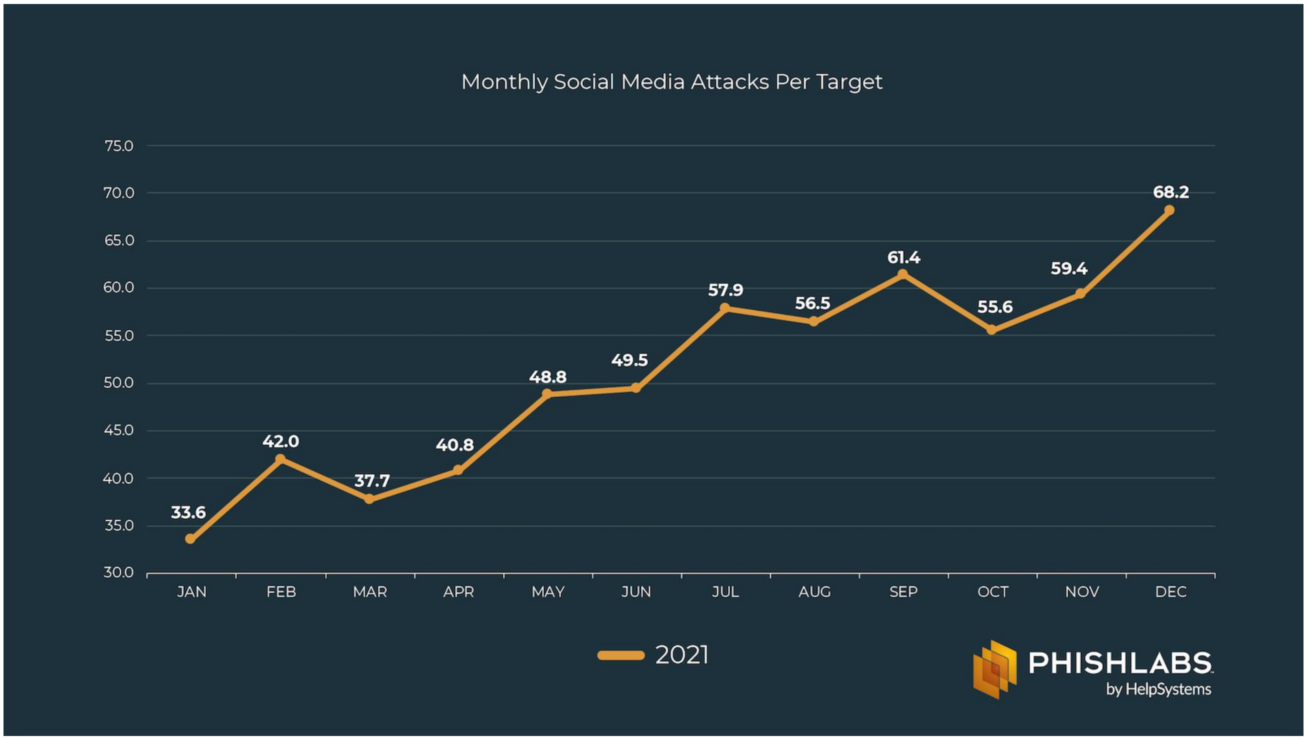


Vishing Attacks Are at an All-Time High, Report Finds

Vishing attacks have increased almost 550 percent over the last twelve months, according to Agari and PhishLabs' Quarterly Threat Trends & Intelligence Report.

Qbot Payloads Dominate Q1

Qbot payloads targeting enterprises contributed to almost three quarters of all email-based malware since the beginning of 2022.



Social Media Attacks Double in 2021 According to Latest PhishLabs Report

Social Media attacks targeting organizations increased 103% in 2021, according to PhishLabs' Threat Trends & Intelligence Report.