Browser-based phishing attacks increased 198% in H2 2023





Browser security was analyzed in a recent report by Menlo Security. The report uncovered a 198% increase in browser-based phishing attacks in the second half of 2023 compared to the first half of the year. When specifically looking at attacks classified as evasive, the report found a 206% increase.

Evasive threats now make up 30% of total browser-based phishing attacks and include tactics such as SMS phishing (smishing), Adversary in the Middle (AITM) frameworks, image-based phishing, brand impersonation or Multi-Factor Authentication (MFA) bypass.

Over 550,000 browser-based phishing attacks were detected in the last 12 months. Legacy Reputation URL Evasion (LURE) attacks increased by 70% since 2022. LURE attacks are characterized by a method in which threat actors evade web filters that attempt to categorize domains based on implied trust.

More than 73% of LURE attacks originated from categorized websites, based on 1 million URLs analyzed in the report. Six days is the average latency between when a zero-hour phishing attack first appears and when it is finally added to the detection mechanism for traditional security tools.

Read the full report here.

https://www.securitymagazine.com/articles/100343-browser-based

-phishing-attacks-increased-198-in-h2-2023