Phishing Landscape 2023

A Study of the Scope and Distribution of Phishing

Interisle Consulting Group, LLC

9 August 2023

Executive Summary

Phishing defrauds millions of Internet users every year. Phishing attacks deceive victims with web sites that appear to be run by a trusted entity, such as a bank or a merchant, but are in fact controlled by a criminal. The phishing page is designed to persuade a victim to provide information that the phisher can use to steal money directly or obtain credentials that can be sold to other criminals.

The role of our Phishing Landscape studies is to collect and analyze reliable and longitudinally consistent data that companies and policymakers can use to mitigate the threat of phishing. We publish these data regularly at the Cybercrime Information Center.

For this study we collected six million phishing reports from 1 May 2022 to 30 April 2023 from four widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. From that data we identified more than 1.8 million unique phishing attacks. We also analyzed more than 11 million phishing reports collected over a three-year period, from 1 May 2020 to 30 April 2023. We added triennial measurements and analyses so that we could consider questions such as: "How has phishing evolved over a three-year period?" and "Are phishers doing business at the same registry, registrar, or web hosting services year after year?"

Phishing leverages Internet resources, exploits vulnerable technologies, and takes advantage of policy and legislative regimes that are siloed and often ineffective. Our study has measured and identified distinct and persistent patterns of exploitation and abuse over a three-year period, and stakeholders have known what is happening for a long time. But far from improving, the phishing landscape is worsening each year. Reviewing the data we have collected since 2020, we conclude that the prevailing uncoordinated and ineffective attempts to curb phishing are simply not working, and that a new strategy is required. In the report, we examine how policy regimes could fight phishing more pro-actively; how governments might encourage effective anti-phishing strategies; and how legal action against the individual organizations that provide resources to phishers could (and recently did) interrupt their criminal supply chain.

Our data show that:

The number of phishing attacks has tripled since May 2020

In addition, phishing attacks during this annual study period from May 2022 to April 2023 increased 65% over the previous study period (May 2021 to April 2022).

The number of unique domain names reported for phishing continues to increase

More than one million unique domain names were reported for phishing during the current period, the most we have observed since we began our observations in May 2020.

New gTLDs host a disproportionate and growing share of phishing domains

New gTLDs represent only 8% of registered domain names worldwide but 25% of domains used for phishing. Year after year, just 25 new gTLDs account for 90% of all new gTLD phishing domains.

Two-thirds of domain names reported for phishing across all TLDs were registered specifically to carry out phishing

Malicious domain name registrations are the most common way that phishers carry out their attacks. Preventing the registration of these domains, and taking them down quicky, should be a priority for the domain name industry.

Phishing that used subdomain providers more than doubled

More than 16% of all phishing attacks were launched from phishing pages hosted at subdomain service providers. 80% of those attacks were perpetrated using just eight subdomain service providers, illustrating how a service of this type can be used to create significant amounts of harm.

Freenom's demise redefined the phishing landscape

Phishing in the Freenom ccTLDs (.TK, .ML, .GA, .CF, and .GQ) was extensive for many years, because the domain names were free and Freenom anti-abuse measures were ineffective. In past years Freenom domains were used for 14% of all phishing attacks worldwide, and Freenom was responsible for 60% of the phishing domains reported in all the ccTLDs in November 2022. Freenom stopped offering registrations in January 2023, and its ccTLDs ceased to be a resource for new phishing domains.

Phishers prefer to host their web sites in the US

42% of all phishing attacks were concentrated in just five US-based hosting networks.

Criminals too easily acquire the resources they need for phishing

The current phishing mitigation strategy is not working. Stemming the persistent and growing tide of abuse will require effective mitigation measures and incentives for the organizations that — wittingly or not — facilitate cybercriminal activity. Coordination, cooperation, and consistent action across a broad range of stakeholders and actors in the phishing supply chain is the only effective way to make a significant impact on phishing.