Phishing Landscape 2021

An Annual Study of the Scope and Distribution of Phishing

by

Greg Aaron

Lyman Chapin

David Piscitello

Dr. Colin Strutt

Interisle Consulting Group, LLC

22 September 2021

Interisle Consulting Group

Executive Summary

Phishing is a significant threat to millions of Internet users. Phishing attacks lure victims to a web site that appears to be operated by a trusted entity, such as a bank, a merchant, or other service. The web site, however, is a deception, a fake, and the site's fake content is designed to persuade a victim to provide sensitive information.

Our goal in this study was to capture and analyze a large set of information about phishing attacks, to better understand how much phishing is taking place and where it is taking place, and to see if the data suggests better ways to fight phishing. To do so we determined when attacks occur and how quickly phishers act. We studied where phishers get the resources that they need to perpetrate their crimes — such as where they obtain domain names, and what web hosting is used. This analysis can identify where additional phishing detection and mitigation efforts are needed and can identify vulnerable providers. We also report on the wide range of brands targeted by phishers, and how often they take advantage of the unique properties of internationalized domain names (IDNs).

To assemble a deep and reliable set of data, we collected 1,487,914 phishing reports from 1 May 2020 to 30 April 2021 from four widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. From that data we identified 695,823 unique phishing attacks.

Our major findings are:

The number of phishing attacks and domain names reported for phishing trended up over the yearly period. The number of reports we ingested from phishing feeds increased by 46% from the first quarter to the last quarter. We observed a 70% increase in phishing attacks and a 69% increase in unique domains reported for phishing.

When phishers register domains, they tend to use them quickly. 57% of domains reported for phishing were used within 14 days following registration and more than half of those were used within 48 hours. 89% of these *maliciously registered* phishing domain names were reported for phishing within 14 days following registration, and 98% of maliciously registered domain names were reported for phishing within the first year of registration.

Most phishing is concentrated at small numbers of domain registrars, domain registries, and hosting providers. We identified 497,949 unique domains used for phishing across the whole year. These domains were registered in 623 Top-level Domains (TLDs) and registered through 997 gTLD registrars. 69% of the domains used for phishing were in 10 TLDs; 69% were registered through 10 registrars.

Phishing attacks are disproportionately concentrated in new gTLDs (nTLDs). In June 2020, nTLDs represented 9% of domain names in the world but 18% of domains used for phishing. The new TLDs' market share decreased during our yearly reporting period (to 6% in March 2021), but phishing reported in the new TLDs increased to 21% during our yearly period.

Phishing domain registrations in some TLDs are overwhelmingly dominated by a small number of registrars. In some TLDs, 90% or more of the malicious domains were registered through one gTLD registrar.

Most phishing occurs on domains purposely (maliciously) registered for phishing attacks. 65% of domains associated with phishing attacks were maliciously registered. In the new TLD space,

70% of phishing domains reported in new TLDs were malicious. Twenty gTLD registrars accounted for 83% of all reported maliciously registered domains. Of these, the top four gTLD registrars (NameCheap, NameSilo, GoDaddy, and Public Domain Registry) account for 53%.

Ten hosting networks accounted for 41% of all phishing attacks. We identified 4,110 hosting networks (ASNs) where phishing web sites were reported; of these, four hosting networks (NameCheap, Cloudflare, Unified Layer, and Google) accounted for 28% of all phishing attacks.

11% of all phishing attacks took place using resources at subdomain service providers. Ten providers accounted for 90% of the phishing attacks hosted at subdomain service providers.

Phishers targeted 1,804 businesses or organizations during the 1 May 2020 to 30 April 2021 period. The top 10 brands targeted over the course of our annual period account for 46% of the reported phishing attacks.

We observed only a small overlap of phishing reports among the four feeds we monitored. This suggests that organizations could benefit from incorporating multiple sources of threat intelligence in their phishing defenses.

We under-report the phishing that takes place in certain regions. We suspect that this is the result of our limited access to phishing reports from these regions and challenges associated with data sharing from region to region.

Our data suggest that there may be opportunities for registry operators and registrars to identify maliciously registered phishing domains with a high degree of accuracy, often at the time of registration.

1. gTLD registrars and TLD operators are in an excellent position to identify and suspend malicious domain name registrations early, in some cases before they can be used victimize users and brands.
2. gTLD registrars and TLD operators possess key information – contact data and billing data – that no one else does. This data is highly useful for identifying malicious customers at the time of registration.
3. Domain name registrars or registry operators all have terms of service that allow them to suspend domains for malicious and illegal activity. Opportunities exist for registrars and registry operators to monitor for such activity, and to suspend domains for malicious purposes.