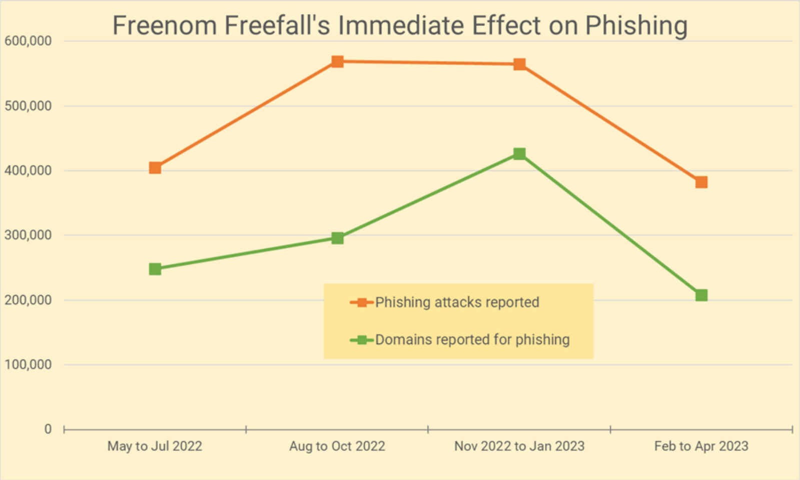
EINPRESSWIRE

Interisle study reveals that phishing attacks have tripled since May 2020, situation worsening each year

Study identifies distinct, persistent exploitation and abuse of Internet resources, reveals that criminals can trivially acquire everything they need to phish.



Freenom's freefall had an immediate effect on phishing activity

HOPKINTON, MA, USA, August 9, 2023 /EINPresswire.com/ -- Interisle Consulting Group today announced the publication of an industry report, Phishing Landscape 202, A Study of the Scope and Distribution of Phishing. Interisle researchers analyzed more than 11 million phishing reports collected from 1 May 2020 to 30 April 2023 to provide annual and triennial measurements of phishing.

Phishing continues to defraud millions of Internet users and businesses each year. The U.S. FBI estimates $2 billion in losses from a single form of phishing called business email compromise (BEC). And these self-reported figures vastly underestimate the harm and losses.Recovery from data breaches where phishing was the initial vector can exceed $5 million per attack.

Among the major findings in the study, Interisle reports that:

- The number of phishing attacks has tripled since May 2020, and has increased 65% over the previous yearly study period.
- The number of unique domain names reported for phishing continues to increase. More than 1 million unique domain names were reported for phishing during the current yearly period.

And the growth is concentrated:

- New gTLDs host a disproportionate and growing share of phishing domains. Year after year, 90% of phishing domains in new gTLDs are in just 25 new gTLDs.

- Phishers prefer to host their web pages in the US, and 42% of all phishing attacks were concentrated in just five US-based hosting networks.
- User accounts created to host phishing web sites at subdomain providers more than doubled. 80% of these attacks occurred on accounts created at just eight providers.

The most disturbing finding?

- Two-thirds of domain names reported for phishing across all TLDs were registered specifically to carry out a criminal act. Preventing the registration of these domains, and taking them down quicky, should be a priority for the domain name industry.

Phishing leverages Internet resources, exploits vulnerable technologies, and takes advantage of policy and legislative regimes that are siloed and often ineffective. Dave Piscitello, co-author and director of the Cybercrime Information Center project, notes that, "By examining phishing over a three-year period, we were able to answer questions such as 'Are phishers doing business at the same registry, registrar, or web hosting services year after year?' and 'How has phishing evolved over a three-year period?' Our data show that the largely independent efforts by the domain name and hosting industries, governments, and private sector organizations have done little to slow the growth of phishing and the damage it causes to Internet users around the world."

Pervasive phishing and other cybercrimes contribute to a lack of consumer trust in online services, which in turn creates a drag on economic opportunity. According to Dr. Colin Strutt, co-author, "The industry is in desperate need of a global strategy that will starve phishers and other criminals of easy access to resources. Our data reveal that it is trivial for criminals to acquire everything they need to phish. We must adopt effective mitigation measures and incentivize the organizations that, wittingly or not, facilitate cybercriminal activity in order to stem the persistent and growing tide of abuse."

Phishing is a global threat. Fighting it effectively will require worldwide policy and legislative attention, the cooperation of domain name registries and registrars, Internet and web hosting service providers, and national and international government agencies. In the report, Interisle discusses how policy regimes can be more proactive in mitigating phishing, how governments might encourage effective phishing mitigation strategies, and what past and recent successes in litigating organizations where phishers most frequently obtain resources they use in for their criminal activities. These recommendations include, for domain names registries and registrars:

1) Clear prohibition of the use of registered domain names to conduct fraudulent, illegal, or deceptive practices, including phishing.
2) Requirement for swift suspension or cancellation by registrars and registries of domain names that are identified as maliciously or abusively registered.
3) A duty for domain name registrars and registries to investigate reports of abuse in a timely manner that is clearly defined, and
4) Adoption of preventative, proactive anti-abuse techniques.

The report emphasizes that mitigation requires cross-industry collaboration, and explains that hosting operators must also commit to these or similar proactive measures. The report also encourages governments to consider taking a more prominent role in ensuring such cybercrimes are less likely to emanate from their namespace.

In the absence of more effective mitigation measures and broader cooperation, litigation has shown to be an effective tool in stemming abuse. Quoting from the report, "In late 2022, Freenom was sued by Meta and the impact was immediate.

By January 2023, Freenom stopped offering domains names, and the number of Freenom domains used for phishing quickly plummeted." The report reviews more than a decade of lawsuits involving domain names to demonstrate that litigation has shown to be an effective tool in stemming abuse.

The Interisle report is available at https://interisle.net/PhishingLandscape2023.html.

Interisle is engaged in a long-term effort to collect and analyze data on the way criminals obtain resources they use to perpetrate cybercrimes, so that Internet policy development can be informed by reliable intelligence based on data. As part of this effort, Interisle publishes quarterly phishing activity reports at the Cybercrime Information Center.

David Piscitello
Interisle Consulting Group
criminaldomainabuse@interisle.net