EINPRESSWIRE

Interisle study reveals phishers have expanded their supply chain to target more users

Analysis of 15 million phishing attacks collected over four years reveals how and where cybercriminals find free or cheap resources for phishing campaigns

HOPKINTON, MA, UNITED STATES, July 23, 2024 /EINPresswire.com/ -- Interisle Consulting Group today announced the publication of an industry report, Phishing Landscape 2024, A Study of the Scope and Distribution of Phishing. The study measures phishing activity over the last year, examines how phishers operate, and recommends strategies to disrupt how and where phishers get their resources.

Interisle's fourth annual study examines nearly four million phishing reports collected from May 2023 to April 2024 and provides historical measurements using over 15 million phishing reports collected at the Cybercrime Information Center over a four year period.

Findings from the study:

- The total number of phishing attacks grew by nearly 50,000 attacks compared to last year, to just under 1.9 million incidents worldwide.

- Phishing attacks hosted at subdomain providers increased by 51% to over 450,000 reported names, representing 24% of all phishing attacks.

- The use of the decentralized InterPlanetary File System to host and launch phishing attacks also increased 1,300% to 19,000 reported phishing sites.

- After the demise of the phish-friendly Freenom, cybercriminals moved to using inexpensive domain names in new gTLDs. 42% of all domains reported for phishing were registered in new gTLDs, compared to 25% last year.

- The registration of high volumes of domain names at one time (bulk registration) accounts for 27% of all domain names used in phishing attacks.

- Four of the top five hosting providers used by phishers to host phishing attacks were based in the United States.

- Domain name registration policies significantly affect the level of phishing in a TLD. Robust customer verification requirements adopted by ccTLDs in Europe and the Asia-Pacific region correlate with lower levels of phishing activity.

According to Interisle partner and study contributor Karen Rose, “Our study shows that clear and known patterns of resource abuse continue, such as the use of bulk registration and new gTLDs. We also see an increase in the exploitation of alternative resources including subdomain and gateway providers. Additional study findings also demonstrate that market changes and policies can have a significant impact.”

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. Interisle recommends several measures to disrupt the phishing supply chain and effectively remediate phishing attacks.

- Implement digital identify verification for parties wishing to bulk register domain names.

- Adopt digital identity verification programs across the domain name, subdomain, and hosting industries.

- Deploy automated systems to screen for suspicious patterns of domain name and subdomain registrations.

- Implement more effective, proactive procedures to identify the use of hosting resources for cybercrime.

- Create “Trusted Reporter” programs across industry to facilitate swift suspension of phishing resources identified by recognized and trusted cybercrime monitors.

"Most phishing now occurs on services offered by a small number of companies,” said Greg Aaron, Interisle Associate and an expert on cybercrime. “These are companies that offer hosting, domain names, and other resources that phishers need to run their attacks. If a handful of these companies can make it harder for phishers to use their services, the public will be better protected.”

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.

The Interisle report is available at https://interisle.net/insights/phishing-landscape-2024-an-

annual-study-of-the-scope-and-distribution-of-phishing.

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