Interisle Reports 17% Rise in Cybercrime, Fueled by 56% Increase in Phishing Attacks

BOSTON, MA, UNITED STATES, October 20, 2026 /EINPresswire.com/ -- Cybercrime is flourishing, according to Cybercrime Supply Chain 2026, a new study released by Interisle Consulting Group. The report analyzed more than 30 million malware, phishing, and spam attacks: a 17% annual growth in attacks overall including a 56% increase in phishing attacks. The study reveals that criminals continue to easily and cheaply acquire the resources for attacks.

The study found that nearly 24 million unique domain names were used in attacks, a 21% increase year over year. Bulk registration of domains for criminal purposes increased 50%. Overall, a staggering 11 million of the 24 million cybercrime-associated domains were bulk-registered. New generic Top-Level Domains (gTLDs) were again the most exploited of the TLD market segments, accounting for 43% of all cybercrime domains reported, far out of proportion to new gTLD total market share.

According to Carel Bitter, Spamhaus, “If you want to influence policy on DNS abuse, you need independent data, like Interisle’s studies. Almost half of the cybercrime domains in this study were bulk-registered. But when it's easy to acquire thousands of domains for a few dollars each – often without anyone asking who you are – we shouldn't be surprised. It's evidence like this that is needed to drive industry change and this is why we sponsor.”

Key report findings include:

• Malware, phishing, and spam attacks grew by 17%, to over 30 million attacks.

• Phishing attacks increased 56% over the last year. Over the last four years, the number of phishing attacks (and the number of domains used for phishing) has increased by about 500%.

• 11 million domains used in cyberattacks were registered in bulk, a 50% increase compared to last year. Attackers repeatedly registered large numbers of domain names over short periods of time to perpetrate cybercrime.

• Cybercriminals increased their use of free web site hosting and subdomain services as key resources for attacks over the past year. Over 1.1 million subdomain hostnames were found to be used in attacks. This represents an increase of 67% compared to last year.

“Criminals continue to source naming, hosting, and other resources wherever they are cheapest and easiest to acquire,” said Dave Piscitello, partner at Interisle and co-author of the report. “Strategies for combating cybercrime need to focus on making these resources harder and more costly for cybercriminals to obtain and the proceeds harder to monetize.”

The report urges greater oversight and accountability across the cybercrime supply chain, including these recommendations:

• Verify Customer Registration Information. Domain name and hosting providers should meaningfully verify registrant contact data, so that it is accurate and complete.

• Implement robust identity verification/certification requirements for parties wishing to register domain names in bulk. Limit the number of accounts that a customer can register at free web hosting providers and identify and block high-volume, automated account creation.

• Deploy automated systems to detect suspicious registration requests and use, deny cybercriminals access to resources, and shut down instances of abuse more quickly.

• Create “Trusted Reporter” programs across the domain name and hosting industries to facilitate swift suspension of cybercrime resources identified by recognized and trusted cybercrime monitors. APWG pioneered one such program and trialed it for two years starting in 2013 with 13 TLD Registries https://ecrimeresearch.org/amdos

Interisle notes that progress in making these resources harder for criminals to obtain has been slow. Governments may need to consider whether action is needed where private-sector approaches fail to curb criminal misuse.

The full report is available at https://interisle.net/cybercrimesupplychain2026.
Media contact: media@interisle.net

Interisle’s study was sponsored by the Anti Phishing Working Group (APWG, https://apwg.org), CAUCE (https://cauce.org), DomainTools (https:// www.domaintools.com), Meta, Inc. (https://meta.com), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG, https://m3aawg.org), Spamhaus (https://spamhaus.org) and SURBL (https://surbl.org).

David Piscitello
Interisle Consulting Group
+1 843-295-9329
Visit us on social media:
LinkedIn
Instagram
YouTube
Other

This press release can be viewed online at: https://www.einpresswire.com/article/950719171

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.