Interisle Study Reveals Alarming Rise in Online Abuse and Identifies Exploitable Links in Cybercriminal's Supply Chains

Year-over-year findings show that cybercriminals exploit of lax policies to easily and cheaply obtain resources for phishing, malware, and spam campaigns.

HOPKINTON, MA, UNITED STATES, November 18, 2024 /EINPresswire.com/ -- Interisle Consulting Group researchers, using data from the Cybercrime Information Center, analyzed 16 million cybercrime events to expose a dramatic rise in criminal exploitation of name, address, hosting, and financial supply chains.

The Cybercrime Supply Chain 2024 report provides actionable insights for those aiming to curb cybercrime.

Cybercrime is a highly profitable business. Dave Piscitello, co-author, explains that "Cybercrime flourished in environments where permissive policies or business practices of suppliers allowed criminals to easily and cheaply access resources with little or no risk or punishment".

Like any other business, cybercriminals must gather the supplies and services needed to conduct their operations. Interisle's study uses a business supply chain framework to analyze how criminals obtain key Internet resources.

Co-author Karen Rose adds, "Analyzing cybercrime as a business revealed insights into the factors that fueled a criminal trade economy and made it lucrative. This economy transacts with the legitimate economy to convert illicit proceeds into cash".

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

• The total number of malware, phishing, and spam attacks grew year-over-year by nearly 54%, to nearly 16.3 million attacks. Spam doubled, from 4 million to 8 million attacks.

• Consumption of domain name resources by cybercriminals increased 81%. Over 8.6 million unique domains were used in cyberattacks compared to 4.8 million last year.

• Over 2.6 million domains used in cyberattacks were registered in bulk, a 106% increase compared to last year.

• Nearly 1.2 million subdomain hostnames were found to be used in attacks, an increase of over 114% compared to last year.

• New generic top-level domains (gTLDs) accounted for 37% of cybercrime domains reported while holding only 11% of the total domain name market.

• The number of IPv4 addresses reported for hosting cybercrime nearly doubled in both China and India.

Efforts to make it more difficult and costly for criminals to acquire these resources, conduct crimes, and "launder" criminal proceeds would help reduce the profitability and allure of the business.

Among Interisle's recommendations:

• Implement rigorous identify verification / certification requirements for parties wishing to bulk register domain names.

• Limit the number of accounts and subdomains that a customer can register with free or inexpensive web hosting (subdomain) providers.

• Expand the deployment of automated systems to screen for suspicious resource registration and use patterns.

•Create "Trusted Reporter" programs across industry to facilitate swift suspension of cybercrime resources identified by recognized and trusted cybercrime monitors.

• Penalize service providers that consistently and disproportionately supply cybercriminals with attack resources or incentivize them to stop.

Interisle notes that sustainable change will only occur if a broad range of stakeholders (including governments, where necessary) step up and implement real-world solutions to reduce criminal access to resources.

Interisle's study was sponsored by the Anti Phishing Working Group (APWG, https://apwg.org), CAUCE (https://cauce.org), and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG, https://m3aawg.org). Collectively, these organizations represent thousands of cybersecurity, public advocacy, service providers, and industry professionals worldwide.

APWG Secretary General Peter Cassidy said, "this report corroborates a long-observed cybercriminal behavior: inexpensive domain registrations and lax verification policies facilitate criminality. If DNS and hosting operators won't intervene to mitigate cybercrime by way of

industry policies, they'll be compelled by interventions under sovereign law. The NIS2 directive of 2022 is hopefully the beginning of that intervention process. APWG encourages EU member states to engage with senior Internet operations and engineering authorities to identify DNS and hosting practices as they transpose NIS2's directives to sovereign law."

"The report makes clear the close connections among malware, phishing, spam, and domain abuse, and presents strategies we need to effectively mitigate them," said CAUCE president John Levine.

"M3AAWG is proud to support this important work with our valued industry partners," said M3AAWG executive director Amy Cadagin. "This report highlights the importance of best practices and anti-abuse capabilities for DNS, email, and cloud providers. Legitimate providers must remain vigilant, as they are operating in an environment that is often far from trustworthy."

The Cybercrime Supply Chain 2024 report is available at https://interisle.net/CybercrimeSupplyChain2024.pdf.

Interisle publishes measurements of where criminals obtain resources they use to perpetrate cybercrimes at the Cybercrime Information Center and offers cybercrime awareness videos at https://www.youtube.com/@cybercrimeinfocenter.

David Piscitello
Interisle Consulting Group
email us here
Visit us on social media:
Facebook
