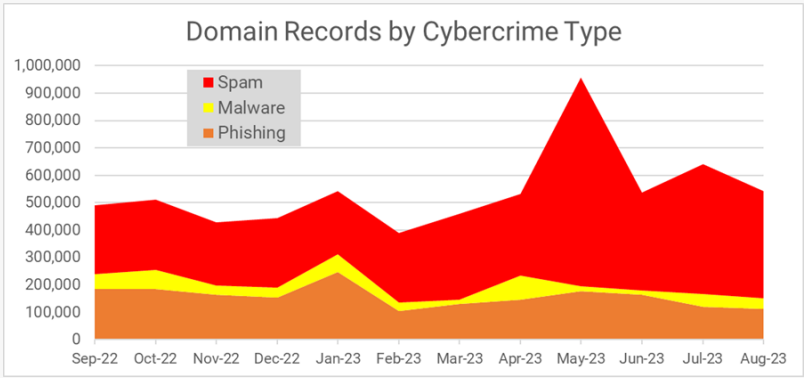
Interisle Cybercrime Supply Chain Study Finds Persistent Patterns of Exploitation and Abuse

Study reveals that criminals benefit from readily available and cheap supply chains that provide the Internet resources for malware, spam, and phishing attacks



Spam campaigns are the largest consumers of criminal domains

HOPKINTON, MA, UNITED STATES, October 23, 2023 /EINPresswire.com/ -- Interisle researchers, using data from the Cybercrime Information Center, analyzed more than 10 million cybercrime records and found distinct, persistent patterns of exploitation and abuse covering a 365-day period from September 2022 to August 2023.

The Cybercrime Supply Chain 2023 study examines malware, spam, and phishing together because they are so often used in combination or sequence. Dave Piscitello, co-author, and director of the Cybercrime Information Center project, explains that “An attacker creates or hacks into a cloud or hosting account and installs a malware that can send email. They use this malware to send phishing emails that lure users to fake sites where the user discloses their personal data. The attacker may instead send spam text messages to mobile devices that contain links to banking malware. These are but two examples of the kinds of sequences of attacks involving malware, spam, phishing, and more malware. Every incident along the way is a cybercrime. And they all make use of resources that criminals can obtain from inexpensive suppliers.”

These suppliers form an online cybercrime supply chain where everything from phishing kits and malicious software, email lists and mobile numbers, domain names and Internet addresses, and places to host attacks are readily and cheaply available. The Interisle study measures the Internet naming and addressing elements of this supply chain. The goal? To focus attention on the links in the supply chain where disruption can have meaningful impact.

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

- Nearly 5 million domain names were identified as serving as a resource for cybercrime.

- Over 1 million domain names reported for spam activity were registered in the new gTLDs.

- Over 500,000 subdomain hostnames were reported for serving as resources for cybercrime at 229 subdomain resellers.

- Criminals acquire domain names in volume: over 1.5 million domains exhibited characteristics of malicious bulk domain registration behavior.

- Brand infringement is commonplace in domains registered purposely by criminals to perpetrate cybercrimes. Exact matches of a well-known brand name were used in over 200,000 cybercrime attacks

-The United States had the most IPv4 addresses serving as resources for cybercrime activity. China, India, Australia, and Hong Kong rounded out the top 5.

There's simply too much cybercrime. Data Prot reports that scams comprise 2.5% of spam emails but that phishing, and the resulting identity theft, makes up 73%. The prolific Emotet banking malware is commonly distributed using spam infrastructures. IBM's data breach report estimates that recovery cost from a data breach resulting from a successful phishing attack was nearly $4.45 million.

The report's findings illustrate that the reactive efforts currently employed by the domain name and hosting industries, governments, and private sector organizations cannot curtail cybercrime and the harms it inflicts on Internet users. Interisle believes that adopting the well-known strategy of disrupting supply lines can be effective in mitigating cybercrime.

Interisle recommends implementation of measures that, working together, policy regimes, governments, service providers, and private sector can use to disrupt the cybercrime supply chain. These recommendations include:

1) Require registrars and registries to promptly (within 24 hours) investigate and suspend or cancel domain names that are purposely registered by criminals to commit online crimes, especially for cases where these registrants have amassed large batches of domain names.

2) Review the practice of bulk registration and develop policy to prevent abuse.

3) Adopt and enforce policies that protect Internet users from deceptive domain registrations, e.g., domains that contain exact matches of recognized brands.

4) Adopt policy to ensure that additional new TLDs do not result in a more abundant supply chain.

5) Develop a common supply chain disruption strategy for ccTLDs and gTLDs.

The report emphasizes that supply chain disruption requires cross-industry collaboration and explains that hosting operators must develop and promulgate broader web, cloud, and hosting industry best practices, including policies, operational practices, and technical solutions similar to those recommended for the domain industry.

Interisle's study was sponsored by the AntiPhishing 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. "The report makes clear the close connections among malware, phishing, spam, and domain abuse, and the strategies we need to combat them," said CAUCE president John Levine. "We're proud to have supported this important work." M3AAWG executive director Amy Cadagin concurs, adding that "This report underlines 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 not always trustworthy. M3AAWG is happy to support this study with our valued industry partners."

The Interisle report is available at https://interisle.net/CybercrimeSupplyChain2023.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, malware, and spam activity reports at the Cybercrime Information Center.

David Piscitello
Interisle Consulting Group
email us here
