Cybercrime Supply Chain 2023

Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them

David Piscitello, Interisle Consulting Group
Dr. Colin Strutt, Interisle Consulting Group

23 October 2023

Study Sponsors

The following organizations provided financial support and peer review for this study.

Anti-Phishing Working Group (APWG) is an international coalition of counter-cybercrime responders, forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, NGOs, and multilateral treaty organizations operating as a non-profit organization. Its directors, managers, and research fellows advise national and sub-national governments as well as the United Nations (Office on Drugs and Crime) as recognized experts (as defined by the Doha Declaration of 2010 and Salvador Declaration of 2015) as well as multilateral bodies and organizations. https://apwg.org/

Coalition Against Unsolicited Commercial Email (CAUCE) is an all-volunteer Internet end-user trust and safety advocacy organization. The CAUCE Board of Directors provides Internet advocacy and consultation with governments, NGOs, law enforcement agencies, and trade associations. The mission of CAUCE is to defend the privacy rights of Internet users and support anti-abuse work in all its forms. CAUCE focuses on messaging security: email, direct message, text, or social media discourse. CAUCE provides instruction and professional development to law enforcement agents and security researchers in developing nations, in-person or remotely, by demonstrating the latest tools and techniques in cyber-investigations. CAUCE provides input to governmental and international policy, regulation, and law, and supports published research projects that advance its stated goals. https://www.cauce.org/

Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) provides a collaborative global trusted forum that brings industry together to help fight and prevent Internet online abuse. Working with members, industry groups, and global partners, M3AAWG will continue its efforts to help prevent online abuse, focusing on protecting communications, data privacy and security, and the supply chain. https://www.m3aawg.org/

Executive Summary

Three cybercrimes – malware, spam, and phishing – are a collective plague on society and economies worldwide. Malware can infect any device connected to a network. Malware attacks are criminal or nation-state activities that cost governments, corporations, and individuals hundreds of billions of dollars every year. Malware ("bots") send spam messages, operating from cloud or hosting service accounts or compromised devices. These bots provide delivery methods for messages that contain lures to phishing pages or malware download sites. Modern day spam is rarely benign: as a delivery system, spam is almost always a component of a subsequent cybercriminal activity. Phishing attacks lure victims to web sites that appear to be run by a trusted entity but are in fact controlled by a criminal, defrauding millions of Internet users every year.

Taken together, these cybercrimes have global impact. Cybercriminals routinely exploit Internet resources to launch these attacks, affecting consumers, businesses, and economies globally. They are pervasive and contribute to a lack of consumer trust in online services, which in turn creates a drag on economic opportunity.

Criminals who perpetrate these cybercrimes enjoy an enormous economic advantage over defenders and responders. They can acquire resources from 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 all readily and cheaply available.

Systems warfare is a strategy that attempts to disrupt the operations of an adversary's functions. This report contends that applying a similar strategy to mitigate cybercrime can be effective. However, to employ such a strategy requires the ability to accurately measure particular elements of the cybercrime supply chain. Measurements collected by Interisle and presented in this report focus attention on the links in the supply chain where disruption can have meaningful impact.

For this study, Interisle collected malware, spam, and phishing reports from eleven publicly and commercially available threat intelligence or reputation services covering a one-year period. From these, we identified the Internet naming, addressing, and hosting resources that criminals use to conduct over 10 million cybercrime attacks and where criminals went to acquire these attack resources. We then ranked Top-Level Domain (TLD) registries, TLD registrars, hosting providers, and subdomain resellers that criminals most frequently exploited to obtain resources, using both raw counts and comparative metrics.

Interisle measured and identified distinct and persistent patterns of exploitation and abuse over a one-year period. While some of these patterns are familiar to cybersecurity practitioners and law enforcement, our data revealed the widespread existence of some less popularly known exploitations of domain registration and hosting services. The findings from this study underscore a previous Interisle finding, that the prevailing uncoordinated and ineffective attempts to curb cybercrime are not working, and that new strategies are required. The recommendations explain how cooperative, pro-active, and cross-sector efforts by governments, private sector, and public policy communities could disrupt the cybercrime supply chain.

Our data show that:

Nearly 5 million domains were reported for serving as a resource for cybercrime

Spam campaigns are the largest consumers of criminal domains: three-quarters of the domain names used in cybercrimes were identified as spam domains.

Cybercriminals often quickly use domain names they register for cybercrimes

47% of phishing domains are reported within 14 days and 54% are reported within 30 days.
28% of spam domains are reported within 14 days and 33% are reported within 30 days.

New gTLDs continue to provide a greenfield opportunity for cybercrime activity

Over 1 million domains were reported for spam activity from September 2022 to August 2023. A handful of the new gTLDs account for most of the cybercrime activity. The five most exploited new gTLDs account for 46% of the cybercrime domains reported across all new gTLDs.

Subdomain reseller services have become even more attractive as free domain registrations from operators like Freenom become scarce

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

Criminals exploit bulk registration services to acquire domain names for cybercrimes

Over 1.5 million domain names exhibited characteristics of malicious bulk domain registration behavior. Bulk registrations accounted for one-third of the malicious domain registrations reported for serving as resources for cybercrimes.

Brand infringement is commonplace in domains registered by criminals to perpetrate cybercrimes

Exact matches of a brand name appeared in 206,040 cybercrime records, 169,835 domain names, and 22,679 subdomain reseller host names.

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

China and the United States accounted for 7 of the 10 hosting networks that hosted the most malware. Combining spam, phishing, and malware records in this study, China and the United States accounted for 8 of 10 hosting networks with the highest cybercrime activity.