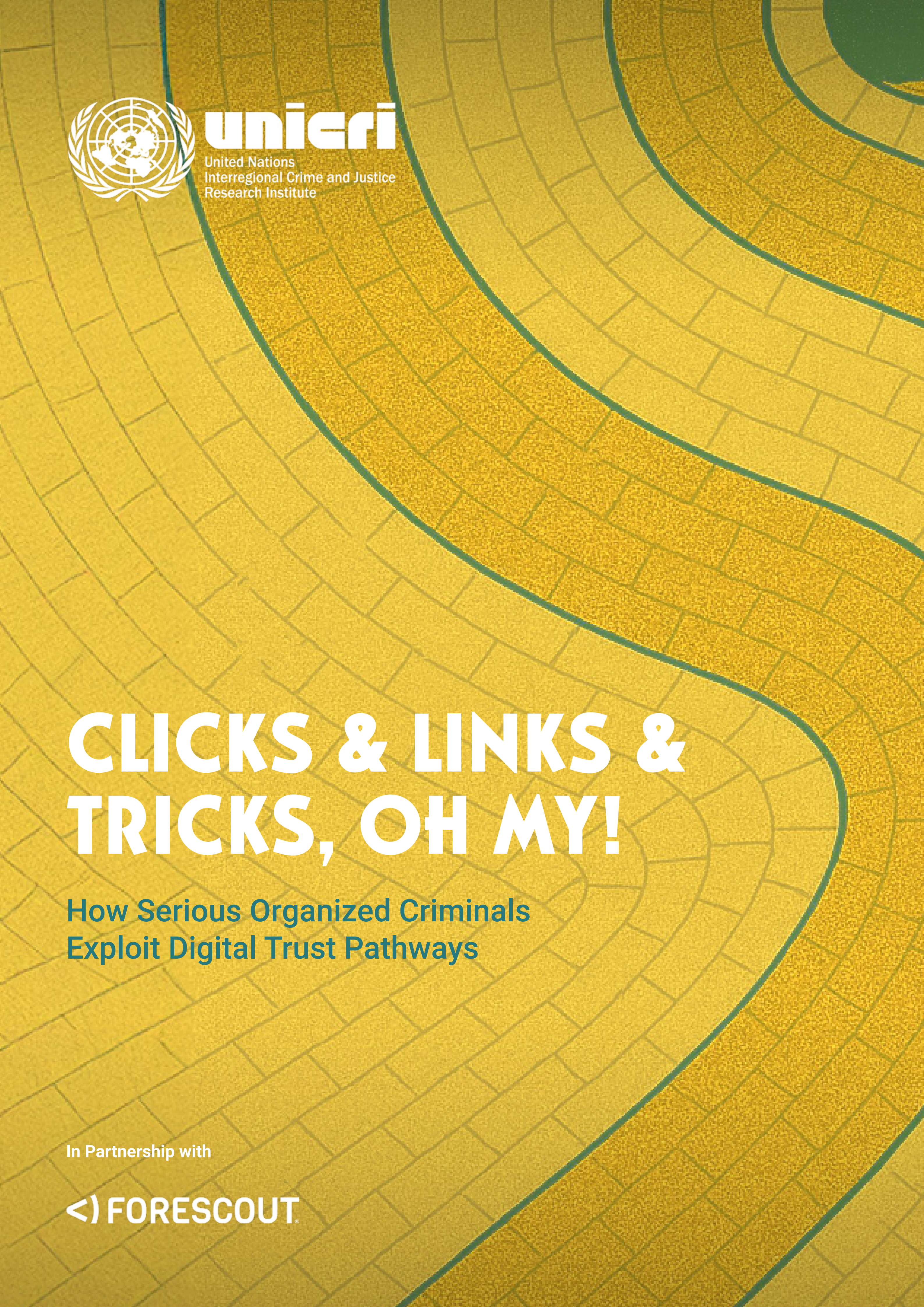

unicri

United Nations
Interregional Crime and Justice
Research Institute

CLICKS & LINKS & TRICKS, OH MY!

How Serious Organized Criminals Exploit Digital Trust Pathways

In Partnership with

FORESCOUT

Viale Maestri del Lavoro,10

10127 Turin, Italy

Website: www.unicri.org

E-mail: unicri.publicinfo@un.org

CLICKS & LINKS & TRICKS, OH MY!

How Serious Organized Criminals Exploit Digital Trust Pathways

Disclaimer

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of the United Nations Interregional Crime and Justice Research Institute (UNICRI) or contributory organizations, and do not imply any endorsement. The content of this publication may be quoted or reproduced in part, provided that the source of information is acknowledged. UNICRI would like to receive a copy of the document in which this publication is used or quoted.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

This report is the product of an initiative led by the United Nations Interregional Crime and Justice Institute (UNICRI). It was written by Janey Young under the guidance of Odhran McCarthy and Ottavia Galuzzi, with editing by Marina Mazzini and design by Marianna Fassio.

UNICRI wishes to extend its gratitude to all the individuals and entities that contributed to the preparation of the report by sharing expert insights, supporting research and data collection services, or peer reviewing the draft. Particular thanks and appreciation are due to Forescout Technologies, Inc., for their extensive collaboration throughout this research and the invaluable insights provided at each stage of its development and the Global Cybersecurity Forum for providing a platform to share the findings of this study at its 2025 Annual Meeting in the Kingdom of Saudi Arabia.

Foreword

Trust is at the heart of our growing online ecosystem. Every time we click a link, enter a password, or visit a website, we are placing faith in unseen systems to be legitimate, secure, and protective of our data. It is this invisible fabric of trust that allows the digital world to function. Yet the very same digital pathways of trust are increasingly being manipulated and exploited by organized criminal actors. This report examines how domains, URLs, and web traffic systems, which were designed to sustain the Internet in confidence, are being exploited to sustain serious and organized crime.

This is part of UNICRI's broader Cybercrime and Online Harms workstream, which seeks to bridge the gap between complex technical threats and practical, human-centered solutions, ensuring that the digital ecosystem remains safe and secure, and not a vector of exploitation for malicious actors. Through this workstream, we have explored the hidden infrastructures of the dark web, encrypted communication platforms and the exploitation of Cybercrime-as-a-Service markets by terrorists; we have examined the human impact of cybercrime on access to justice in Africa by centering the experiences of victims; and we have mapped the abuse of digital technologies by violent extremist groups across South America, Africa, and Asia. More recently, we have broken new ground, filling important gaps in our understanding of video gaming and online harms by looking at the intersection with violent extremism in Africa and Southeast Asia. Collectively, this corpus of knowledge illustrates both the diversity and the interconnectedness of online threats and provides UNICRI with a foundation for its work in this increasingly important space.

As with those efforts, this report is not only about threats. It is about resilience. By gathering insights from global research and practitioner engagement, it reinforces the importance of anticipating risks, building capacity, and fostering multistakeholder cooperation. Safeguarding digital trust is not a technical task alone: it is a collective responsibility that requires governments, law enforcement, industry, and civil society to act together. At UNICRI, we are committed to advancing this dialogue and supporting concrete solutions so that the Internet continues to be a driver of inclusion, innovation, and security, and not a lawless space for exploitation.

Leif Villadsen
Acting Director, UNICRI

Executive Summary

The integration of digital infrastructure into every dimension of modern society has created not only opportunities for innovation and growth, but also new avenues for exploitation by serious and organized criminal actors. This report examines the systematic manipulation of fundamental Internet components – domain names, uniform resource locators (URLs), and web traffic systems – which increasingly serve as the foundation for a broad spectrum of illicit activities. These elements, collectively referred to in this report as 'digital trust pathways', are being strategically misused to facilitate, expand, and conceal criminal operations on a global scale.

Cybercriminals are highly adaptive, leveraging the open and decentralized architecture of digital infrastructure to exploit vulnerabilities. Their operations are scaled and maintained through a backbone of cybercrime – phishing, pharming, spam, malware and botnets – which themselves are underpinned by sophisticated exploitation of digital trust pathways. These exploitations include domain registration abuse (e.g., typosquatting and homograph attacks), URL exploitation (e.g., dynamic generation and abuse of shortening services), and traffic manipulation (through malicious redirects and cloaking). These practices are increasingly automated by programmatic tools like domain generation algorithms (DGAs), fast-flux DNS, and traffic distribution systems (TDS).[1] [2] This automation not only enhances their reach but also strengthens their resilience towards detection and disruption.

This combination of automated techniques and supportive infrastructure allows threat actors to evade traditional detection mechanisms, rapidly reconfigure operations, and, in doing so, intensify the global threat landscape.

The consequences of such exploitation extend well beyond technical breaches, with digital trust pathway abuse now central to the commission of many traditional serious organized crimes, such as example identity theft, large-scale financial fraud (including business email compromise (BEC) and investment scams), ransomware extortion, distribution of child sexual abuse material (CSAM), human trafficking, and intellectual property crime. These crimes are not new, they are longstanding offences that have been amplified, anonymized, and globalized through the systematic misuse of digital infrastructure. Trust, once the cornerstone of the Internet's design, is thus repurposed as a vehicle for exploitation.

Emerging technologies further complicate this environment. Blockchain-based domain systems, while offering resilience and autonomy, currently lack adequate governance and dispute resolution mechanisms, creating opportunities for permanent malicious registrations. Similarly, artificial intelligence (AI) serves as both a defensive tool and a potential enabler for criminal activity, supporting the production of convincing phishing campaigns, polymorphic URLs, and deepfake content. The growth of

[1] "Beneath the Surface: Detecting and Blocking Hidden Malicious Traffic Distribution", accessible at: https://unit42.paloaltonetworks.com/detect-block-malicious-traffic-distribution-systems/.

[2] "Fast Flux: A National Security Threat", accessible at: https://www.ic3.gov/CSA/2025/250403.pdf.

Cybercrime-as-a-Service (CaaS) models further enhances the threat landscape by lowering the barrier to entry, enabling less technically skilled actors to deploy advanced capabilities with relative ease and contributing to the commoditization of cybercrime.

Responding to these challenges requires more than fragmented or reactive approaches. The report calls for a coordinated, multistakeholder response that combines technical innovation, strengthening of global frameworks, and enhanced international cooperation. Priority areas include reinforcing globally adopted standards, improving mechanisms for information sharing, building capacity among policymakers and users, and developing foresight capabilities to anticipate and mitigate emerging risks.

Ultimately, safeguarding the digital ecosystem requires recognizing that domains, URLs, and web traffic systems are not peripheral artefacts. Rather, they are the building blocks of the Internet and are abused as crucial elements enabling cybercrime. Their protection must therefore be approached as a shared international responsibility, fundamental to preserving digital trust and ensuring an open, safe, and secure Internet for all.

Table of Content

SETTING THE SCENE

Introduction

The increasing integration of digital infrastructure into the fabric of society has ushered in transformative opportunities across all regions of the world, contributing significantly to economic growth, social development, and improved access to essential services. The expansion of global Internet connectivity – now central to communication, governance, commerce and education – has become a cornerstone of inclusive development, bridging geographic divides and fostering cross-border cooperation.

However, as Internet adoption accelerates across both developed and developing contexts, the gains of digital transformation are increasingly shadowed by complex, transnational security risks. The very infrastructure that enables sustainable and inclusive digital progress is being systematically repurposed by serious and organized criminal actors, as well as groups such as hacktivists and state-sponsored threat actors. At the centre of this challenge lie the Internet's foundational components – domain names, uniform resource locators (URLs), and web traffic systems – which are not merely technical building blocks but also critical enablers of trust. Their manipulation allows illicit actors to facilitate, scale, and obscure a wide spectrum of criminal activity, undermining confidence in the digital ecosystem on which societies and economies now depend.

Organized criminal actors have shown a remarkable capacity to adapt to rapid technological change, leveraging the anonymity, automation, and borderless nature of the Internet to build resilient and scalable operational models. Through strategic exploitation of digital trust pathways, illicit actors have now developed increasingly sophisticated forms of criminal activity: from credential harvesting and business email compromise (BEC), to cyber-extortion campaigns, manipulative fraud schemes, to crimes involving violence and coercion. These crimes are now initiated and sustained through the deceptive deployment of exploited 'digital trust pathways', delivered via emails, websites, social media platforms, and messaging services, all of which serve as conduits for compromise and exploitation.

The proliferation of these methods reflects a broader shift toward what can be described as 'trust exploitation at scale'. This phenomenon refers to the systematic manipulation of legitimate-looking digital environments to deceive individuals, penetrate secure systems, and execute unlawful actions. It is against this backdrop that this report seeks to examine how the exploitation of this core infrastructure has become a critical enabler for a broad range of online harms.

Objectives

The report seeks to move beyond surface-level threat identification by providing an analysis of how domains, URLs and web traffic systems function within the broader ecosystem of serious and organized crime. It traces the evolution of their abuse, from early obfuscation techniques and basic spoofing strategies, to the emergence of highly advanced programmatic models. These contemporary tools make use of automation, artificial intelligence, and precision–based social engineering to mount increasingly targeted, scalable, and evasive campaigns – posing significant challenges to traditional cybersecurity frameworks and detection tools.

This report was prepared by UNICRI through its Cybercrime and Online Harms workstream to inform discussions around cybercrime at the 2025 Annual Meeting of the Global Cybersecurity Forum held in the Kingdom of Saudi Arabia. By fostering a shared understanding of these evolving threats, the report intends to catalyze coordinated action leveraging the 2025 Annual Meeting as a platform to contribute to the development of globally informed, locally effective security strategies.

Designed with a broad audience in mind, including policymakers responsible for national security and digital governance, law enforcement agencies tasked with investigating and prosecuting cybercrime, cybersecurity professionals in both public and private sectors, civil society organizations contributing to the fight against cybercrime and academic researchers seeking to deepen their understanding of this critical domain, the report is structured to provide insights for both technical and non-technical readers, ensuring accessibility without compromising technical depth.

Methodology

The research employs a mixed-methods approach. Semi-structured interviews and questionnaires were conducted with a diverse range of stakeholders, including representatives from law enforcement, regulatory authorities, international organizations, cybersecurity firms, domain and cloud infrastructure providers, and major content platforms. These insights provided first-hand perspectives on the scale, impact, and evolving nature of digital trust pathway abuse.

A comprehensive review of academic literature, institutional reports, legal frameworks, and national policies was conducted. In parallel, selected cases were analyzed to illustrate specific techniques and outcomes, spanning multiple regions, types of crime, and varying levels of technical sophistication. Technical threat intelligence efforts, including in collaboration with Forescout Technologies, Inc., focused on examining malicious domains, redirect paths and link manipulation methods to identify systemic abuse patterns.

All research activities were conducted in accordance with international ethical standards, with participant consent obtained, data anonymized where appropriate, and legal protocols strictly followed throughout the investigative process.

Key Concepts and Terms

For the purposes of this report, the term 'digital trust pathway abuse' will be used as opposed to 'Domain Name System (DNS) abuse', as it better captures the elements relevant to this report – namely the misuse of domain names, URLs, and web traffic systems that serve as the Internet's core trust pathways. The term DNS abuse is interpreted in strictly technical terms by the Internet Corporation for Assigned Names and Numbers (ICANN) – the non-profit organization responsible for coordinating the global system of unique identifiers on the Internet – which limits the analytical scope of this research. By contrast, the framing of digital trust pathways recognizes the broader ecosystem in which domains, URLs, and web traffic systems are systematically misused to facilitate criminal activity. This framing is intended to better reflect the realities of the threat landscape, where technical and content abuses are closely intertwined and cannot be easily disentangled in practice.

A MAZE OF DECEPTION: WEB EXPLOITATION TYPOLOGIES

This section examines the typologies underpinning the exploitation of digital trust pathways by serious and organized criminal actors. Criminals employ these techniques – domain name manipulation, abuse of URL structures, and web traffic redirection – often in combination – to strategically scale illicit operations and obscure attribution. The activities described are not isolated technical incidents but deliberate, systemic distortions of domain-based infrastructure. The sophistication and scale of these methods are increasing, with many deployed automatically or programmatically, creating a complex and evolving threat landscape.

While this report focuses on the most prevalent patterns of abuse today, the rapid evolution of the digital environment demands continuous monitoring and anticipatory analysis. Mapping the typologies is essential to understanding the operational methods of serious and organized criminal groups, and categorizing these recurring patterns provides critical insight into how illicit actors expand their operations, evade detection, and weaponize mechanisms of trust.

Notably, the exploitation of digital trust pathways also marks a convergence point where criminal innovation frequently outpaces both regulatory safeguards and technical defences. Recognizing and analyzing these abuses is therefore vital not only for cybersecurity practitioners, but also for international governance bodies charged with preserving the integrity of the global digital ecosystem.

The Art of Digital Deception

Domain Registration Abuse

At the foundation of Internet infrastructure lies the Domain Name System (DNS) – the protocol designed to translate human-readable domain names into machine-readable Internet Protocol (IP) addresses. Functioning as the silent backbone of the Internet, DNS enables the seamless navigation of the web. However, many of the features that enable efficiency and scalability – openness, decentralization, and minimal verification – also render it a highly attractive vector for exploitation by organized criminal actors.

A fundamental tactic employed by threat actors involving the DNS is the intentional registration of deceptive domain names. These deceptive domains leverage linguistic familiarity, visual deception, and semantic trickery to mislead users and evade security controls. They are meticulously designed to bypass both user security instincts and automated filters, serving as prime vehicles for phishing or malware. Their objective is to deceive users into clicking on what they believe to be a legitimate site, capitalizing on simple human error.

Common methods include typosquatting, where criminals register domains resembling legitimate websites but with minor typographical deviations (e.g., g00gle[.]com instead of google.com). Similarly, attackers employ homograph domains, which substitute visually similar characteristics from other scripts (such as a Cyrillic ‘a’ that appears identical to a Latin ‘a’) or Punycode – a character encoding method that converts non-ASCII characters[3] into a format compatible with the DNS allowing users to register internationalized domain names (IDN)[4] in their native languages. For instance, if a browser supports IDNs, xn--pple-4xa[.]com would typically display as apple.com, visually mimicking the true apple.com. Beyond typographic manipulation, more and more actors are resorting to gibberish domains to evade detection, registering randomized or nonsensical domain names (e.g., B4arp834sch[.]life).

Illicit actors also manipulate Top-Level Domains (TLDs) to enhance perceived legitimacy or avoid detection. These are the last part of the domain name located after the dot (e.g., .com, .uk, .fr), used to categorize websites by purpose, geographic location or other criteria and governed by ICANN. There are several different types of TLDs, but two stand out as most relevant for illicit activities: country-code TLDs (ccTLD) and generic TLDs (gTLD). A significant portion of this abuse is highly concentrated with certain country-code Top-Level Domains (ccTLDs), like .ru (Russia), .cn (People’s Republic of China) or .co (Colombia) and generic TLDs (gTLDs) such as .com, .xyz and .top, which have attracted significant attention. These combined with broader names like .online (suggesting general web presence), .shop (implying genuine e-commerce), or .live (which can be used for streaming scams), enhance the deception. Furthermore, services that offer complimentary domain registration (e.g., .tk, or .cf) provide low-cost, disposable infrastructure opportunities, and ‘TLD hopping’, where the same second-level domain is repeatedly re-registered across different TLDs (e.g., example.tk; example.or; example.cf). These are popular tactics used to extend the lifespan of malicious sites and frustrate takedown efforts. The challenge is compounded by the failure of some gTLD operators to fully enforce DNS abuse mitigation rules. A case example of this was the .top registry which was served a notice of breach due to several failures.[5] Notably, the issues were only remediated a year after the notification.

Analysis conducted by Forescout for this study underscores the scale of the challenge. Almost 12,000 domains involved in malware communication were analyzed over a six-month period.[6] The findings reveal clear patterns of exploitation: generic top-level domains (gTLDs) accounted for 88.2% of malware-associated domains while 11.8% used country-code TLDs. Among ccTLDs, .ru (Russia) was the sole entry in the top ten most abused TLDs, accounting for 4.1% of total abused domains and 35% of

[3] Non-ASCII characters are any characters, such as symbols, accented letters, or characters from non-Latin alphabets, that are not part of the original 128-character ASCII set. ASCII (American Standard Code for Information Interchange) is a character encoding standard that assigns numeric codes to letters, numbers, and symbols. It includes printable characters like A-Z, a-z, 0-9, and punctuation, as well as non-printable control characters used to manage data flow and device functions.

[4] Internationalized Domain Names (IDNs) are web addresses that use characters from non-Latin scripts, such as Arabic, Chinese, or Cyrillic, or Latin-based characters with diacritics (accent or cedilla), allowing for domain names in native languages.

[5] “ICANN - Notice of Breach of Registry Agreement”, accessible at: https://www.icann.org/uploads/compliance_notice/attachment/1225/hedlund-to-wenxia-16jul24.pdf.

[6] Amine Amri, Michele Campobasso, Daniel dos Santos, and Forescout Research - Vedere Labs, "From URLs to Malware: How Threat Actors Abuse Domain Name Security in 2025", Forescout, September 2025, accessible at: https://www.forescout.com/blog/from-urls-to-malware-how-threat-actors-abuse-domain-security-in-2025/.

all ccTLD-related abuse. Most domain names (75%) were algorithmically generated gibberish domains, combining random letters, numbers, and words. 10% sought to impersonate known brands, while 15% referenced sectors (e.g., “finance”, “health”) without imitating specific organizations. The concentration of registrars – accredited organizations that manage the reservation and sale of domain names to the public – was also noted as pronounced, with the top 10 registrars accounting for 54.1% of malicious domains, while the top 100 registrars covered more than 90%.

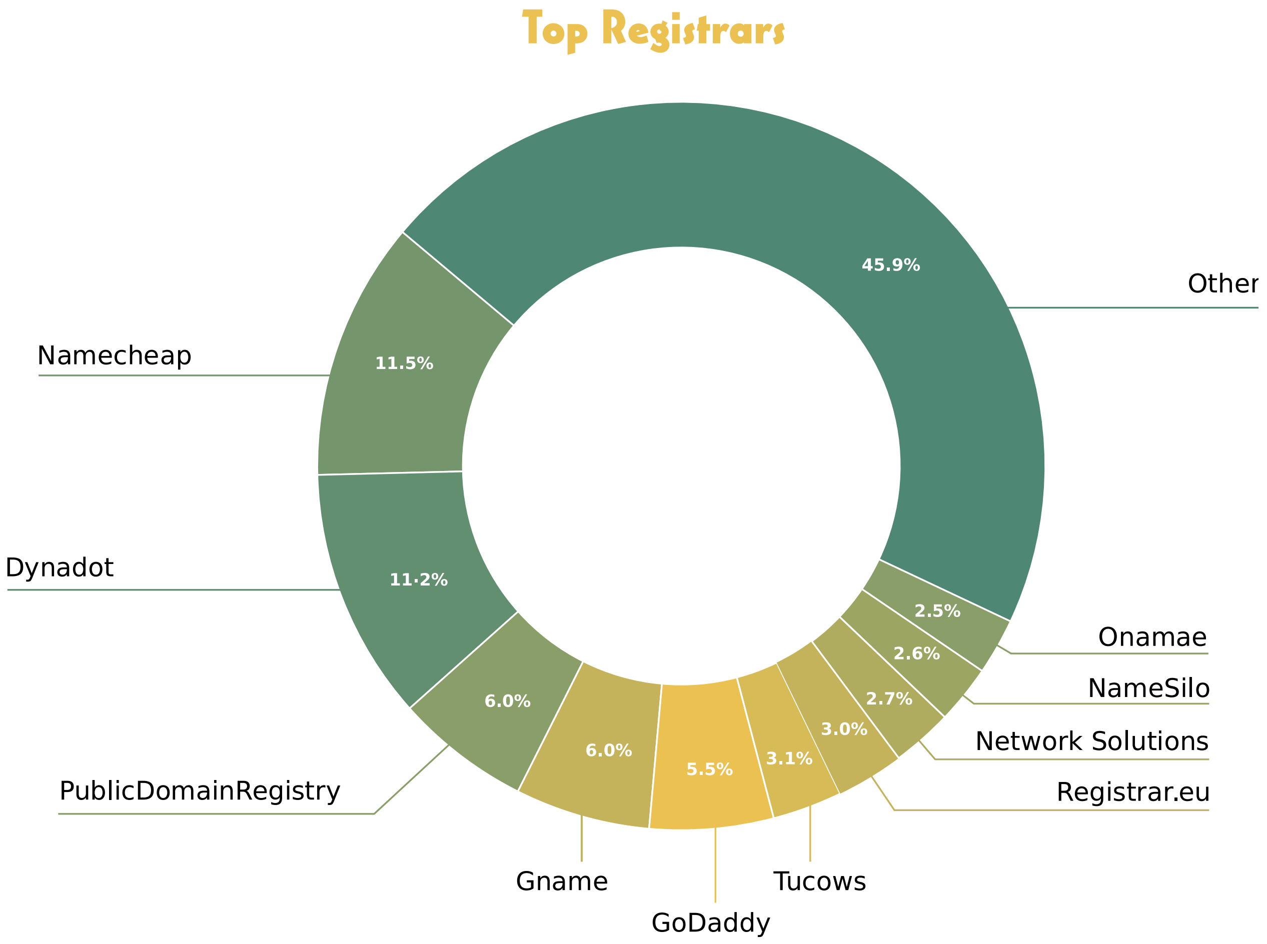

Figure 1: Forescout – Registrars most frequently abused by malware

Nearly all (98%) of domains used for illicit purposes were initially registered for one year, although 43% expired or were ‘sinkholed’ – a defensive measure that reroutes malicious traffic to a secure controlled server to prevent further abuse – before that due to coordinated interventions by registrars, law enforcement and the cybersecurity community.

These findings show domain registration abuse remains a systemic vulnerability in the global digital ecosystem. A lack of efficient security and compliance, including slow remediation by registries and registrars and minimal Know Your Customer (KYC) verification, combined with low-cost, easily accessible malicious registrations, allows criminals to generate large volumes of disposable domains, supporting short-lived campaigns that evade detection and complicate attribution.

Case Example: Domain Registration Abuse in Emotet Campaigns

Emotet, one of the most pervasive malware families, evolved from a banking trojan into a global botnet and malware delivery platform. Delivered through phishing emails with weaponized attachments, it used malicious scripts to contact attacker-controlled infrastructure and download payloads such as Trickbot, Qbot, and Ryuk ransomware. Central to these operations was the large-scale abuse of domain registrations: operators continuously registered inexpensive, deceptive domains – such as *analyticscosm[.]com* and *fulfillmententertainment[.]com* – to host payloads and serve as command-and-control nodes. By rotating short-lived domains across generic TLDs, Emotet ensured resilience against takedown efforts, turning disposable registrations into the backbone of a durable and scalable malware ecosystem.[7] [8]

Subdomain Abuse

Building on the malicious registration of domain names, threat actors are increasingly exploiting subdomains – the hierarchical segments that extend from a primary domain (e.g., blog.example.com) – to deceive users and conceal malicious infrastructure within trusted ecosystems.

Subdomain exploitation occurs through several interconnected techniques. One of the most covert is domain shadowing, in which attackers gain unauthorized access to a legitimate domain's DNS management panel. Without altering the main website, they silently create numerous rogue subdomains (e.g., update.legitcompany[.]com) that point to attacker-controlled infrastructure. These subdomains are often used for phishing, malware delivery, or command-and-control (C2) operations, operating undetected within the trusted boundaries of the parent domain.

Closely related is subdomain impersonation (or spoofing), which focuses on the visual construction of subdomains that mimic familiar brand or internal naming conventions. These domains are designed to exploit user trust by using familiar URL structures. For example, a phishing link like docs.microsoft.com.securityupdate[.]ru uses a trusted prefix to obscure the fact that the true domain is securityupdate[.]ru. Similarly, a domain such as hr.yourcompany.org.cloud-login[.]info may appear legitimate to employees, who are then deceived into disclosing credentials to a fraudulent portal.

A third notable method, involves the abuse of user-generated subdomain services, in which criminals exploit legitimate platforms – such as blogging sites, frontend hosting platforms (FHPs), or project management tools – to create their own subdomains. Forescout has observed a sharp increase in this

[7] "Emotet Threat Briefing", accessible at: https://www.forescout.com/resaources/emotet-threat-briefing/.

[8] "Emotet Bulletin", accessible at: https://cyberint.com/blog/research/emotet-bulletin/.

practice, with FHPs in particular growing in popularity since 2021.[9] Their appeal lies in offering low-cost or free hosting tiers with automation features that allow new domains to be rapidly deployed from existing projects or templates to user-specified or randomly generated subdomains. This makes the process both inexpensive and highly scalable. Furthermore, FHP domains and IP addresses generally carry a positive reputation, and threat actors can exploit this trust to bypass domain- and hosting-based filtering mechanisms. In practice, this enables attackers to register deceptive subdomains – such as paypal-verify.blogspot[.]com or microsoft-support.wordpress[.]com – without ever compromising the underlying platform. This form of abuse is particularly insidious because it inherits the legitimacy of the hosting service itself, making detection more difficult and remediation more complex.

Case Example: Zoom Subdomain Spoofing for Malware Distribution

Forescout documented how attackers exploited legitimate frontend hosting providers, including surge.sh and pages.dev, to create subdomains impersonating Zoom. Domains such as zoomhdens.surge[.]sh and zoom016.pages[.]dev hosted fraudulent update pages that mimicked Zoom's interface, even loading a genuine favicon from zoom.us to enhance credibility. Victims were prompted to download a supposed update, which in reality delivered a trojaned version of ConnectWise ScreenConnect, a remote access tool frequently abused to seize control of compromised systems. This case illustrates how subdomain spoofing on legitimate frontend hosting platforms can be leveraged to deliver malware while evading traditional detection and takedown efforts.[9]

Domain Hijacking

Beyond the initial crafting of deceptive domains and subdomains, malicious actors further capitalize on opportunities for manipulation via domain hijacking, otherwise known as 'domain takeovers'. This encompasses a wide range of tactics aimed at unlawfully transferring control of Internet domains without the consent of the rightful owner, posing significant risks to both private and public sector entities.

Active domain hijacking occurs when a cybercriminal gains unauthorized access to legitimate and active domains, often through exploiting a security vulnerability in the domain's content management system (CMS), web server, or via stolen credentials. Expired domain compromise occurs when legitimate domain owners fail to renew their domains and the domains are re-registered by malicious actors who exploit residual search engine rankings, backlinks, or brand trust to host malicious content or redirect users. Once a domain is compromised, the attacker can use it to host malicious content, inject malware, or redirect traffic to fraudulent sites, leveraging the domain's established reputation to bypass security filters and deceive users.

[9] Michele Campobasso, Amine Amri, Daniel dos Santos, and Forescout Research - Vedere Labs, "Revamped Phishing Techniques: How Telegram and Front-End Hosting Platforms Scale Campaigns", Forescout, September 2025, accessible at: https://www.forescout.com/blog/revamped-phishing-techniques-how-telegram-and-front-end-hosting-platforms-scale-campaigns/.

Case Example: Subdomain Takeover by Hazy Hawk

In mid-2025, cybersecurity firm Infoblox exposed a campaign by the threat group Hazy Hawk that systematically hijacked abandoned or misconfigured subdomains of trusted organizations, including Bose, Panasonic, and the U.S. CDC. The attackers exploited residual DNS records left behind after cloud services were decommissioned, enabling them to claim full control over these subdomains. Victims visiting these hijacked subdomains were exposed to malicious content delivered via abused digital trust pathways, such as malware download prompts disguised as urgent security alerts, tech support scams, or fake software updates. By leveraging the reputation of legitimate domains, the actors bypassed security filters and exploited user trust, highlighting the risks posed by unmaintained or mismanaged domain assets.[10]

Manipulating the Path: URL Abuse and Traffic Manipulation

URL Abuse

While the DNS plays a foundational role in directing Internet traffic, it represents only the first layer of web navigation. Beyond the resolution of domain names lies the full uniform resource locator (URL) – a more complex construct encompassing the protocol (http:// or https://), domain, path (e.g., /login), query parameters, and fragments. Malicious actors increasingly exploit this granular structure to deceive users, bypass security mechanisms, and weaponize ordinary web content delivery systems. This deeper manipulation of the web's architecture reflects a growing sophistication in how threat actors repurpose everyday Internet functions for cybercriminal ends.

One of the most prevalent techniques used to exploit URL structures is URL obfuscation – a visual deception technique whereby a URL is intentionally distorted to obscure its true purpose. Methods include inserting misleading or encoded characters, constructing excessively long strings that mask malicious intent, or embedding deceptive credentials (e.g., http://login.example.com@malicioussite[.]com) that deceive users into trusting a malicious destination. Closely related is the abuse of URL shortening and protection services. Legitimately designed to increase convenience and improve link sharing – particularly on platforms with character limits – services like Bitly, TinyURL, or enterprise URL protection tools can be leveraged by threat actors to conceal the final destination of a link. This not only hides malicious endpoints but can also bypass security filters that rely on reputation scoring or pattern recognition, where malicious actors embed phishing URLs within trusted URL-rewriting services to evade detection.

A more adaptive tactic involves dynamic URL generation, whereby malicious URLs are created programmatically, often unique to each user or session. This approach complicates detection, as no static pattern

[10] "Cloudy with a Chance of Hijacking Forgotten DNS Records Enable Scam Actor", accessible at: https://blogs.infoblox.com/threat-intelligence/cloudy-with-a-chance-of-hijacking-forgotten-dns-records-enable-scam-actor/.

exists for security tools to track. Dynamic URLs also enable threat actors to monitor the effectiveness of campaigns in real-time, tailoring payloads or redirect paths based on user interaction, geographic location, or engagement metrics. Combined with URL obfuscation and service abuse, these tactics form a multi-layered threat that can exploit user trust, bypass traditional defenses, and facilitate credential theft, fraud, and malware delivery at scale.

Case Example: Exploiting URL Protection Services in Phishing Campaigns

Between May and July 2024, Barracuda Networks identified a series of sophisticated phishing attacks targeting Microsoft 365 users. These campaigns demonstrated advanced URL abuse techniques, leveraging trusted URL protection services to mask malicious links and evade detection.

Threat actors exploited legitimate URL protection services by embedding phishing URLs within these services, which are typically used to scan and rewrite links for security purposes. By doing so, the malicious links bypassed traditional security measures, as the rewritten URLs appeared legitimate to both users and security systems. This method allowed threat actors to conceal their phishing destinations, making it more challenging for security tools to identify and block the malicious content.

The phishing emails often impersonated trusted services, such as DocuSign or password reset notifications, and included obfuscated URLs that redirect users to credential-harvesting sites. This approach not only deceived users but also circumvented security filters that rely on URL reputation and pattern recognition. The use of trusted URL protection services in this manner highlights the evolving tactics of cybercriminals in exploiting legitimate infrastructure to facilitate malicious activities

This case underscores the importance of comprehensive security measures that go beyond traditional URL filtering, emphasizing the need for advanced detection capabilities to identify and mitigate sophisticated phishing threats.[11]

Traffic Manipulation

Beyond URL abuse, malicious actors frequently manipulate how users are redirected across the web – often without their awareness or consent. These redirection techniques are designed to channel users through layers of seemingly benign content before ultimately delivering a malicious payload.

[11] "Threat Spotlight: Attackers abuse URL protection services to mask phishing links", accessible at: https://blog.barracuda.com/2024/07/15/threat-spotlight-attackers-abuse-url-protection-services?utm_source=chatgpt.com.

Malicious redirects remain one of the most widespread tactics. These involve deliberate redirection mechanisms implemented through HTTP response codes, JavaScript functions, HTML meta refresh tags, or server-side scripting. The user is moved from a legitimate-looking page to a phishing site, exploit kit, or malware dropper. While these transitions often occur seamlessly and without user interaction, the browser's address bar typically reflects the change – leaving some trace visible to the user or detectable by security tools.

Invisible redirection techniques, by contrast, operate with greater subtlety. Rather than redirecting the user to a new page, these methods silently load malicious content in the background of the existing site. Threat actors commonly use hidden iframes, zero-pixel elements, or off-screen HTML and CSS – controls of the visual appearance of a website, including colors, layouts, fonts, and spacing components – to embed or trigger malicious resources. The user remains on the same page and may have no visual indication that an external payload has been executed. These techniques are a hallmark of drive-by download attacks, where malware is silently installed without any user interaction – simply visiting a compromised page can be sufficient.

A more advanced method of network traffic redirection is cloaking, where different content is selectively served depending on the request origin. For example, a benign version of a webpage might be displayed to search engine crawlers or automated security scanners, while human users are presented with a phishing form or exploit. This targeted content delivery enables threat actors to evade automated detection while ensuring the malicious payload reaches the intended victim.

Finally, URL injection represents a further layer of advanced abuse, whereby attackers embed malicious URLs into the legitimate structure, content, or database of trusted websites. Typically enabled through vulnerabilities such as Structured Query Language (SQL) injection or Cross-Site Scripting (XSS) within content management systems, this technique effectively weaponizes reputable sites as unwitting redirectors. Visitors are silently channelled to harmful destinations, including phishing portals, malware loaders, or fraudulent content, all under the guise of trusted domains. A prominent example of this practice is malvertising, where attackers inject malicious code into seemingly legitimate advertisements that are then distributed through reputable online advertising networks. These deceptive ads can automatically redirect users to malicious websites – often without any interaction – resulting in malware infections, credential theft, or exposure to large-scale fraud.

Case Example: Magecart's Silent Attack on E-commerce

In 2023, Magecart attackers demonstrated a significant evolution in their methods by compromising e-commerce sites through highly evasive, client-side attacks. Instead of using visible fake payment forms, the campaigns relied on a range of invisible techniques to silently steal payment information. Attackers injected malicious code into websites using hidden HTML elements that were not visible to the user. These scripts were also concealed through an invisible, single-pixel image with its width and height set to zero, which ensured that the skimming payload was loaded and executed without any visible change to the site. The malicious scripts were designed to silently collect a customer's payment information as they typed it into the legitimate checkout form. The attackers used sophisticated data exfiltration methods, such as an invisible IMG element,[12] to send the stolen data to an attacker-controlled server in the background. This silent redirection meant that the victim's browser URL never changed, and the payment appeared to process normally, leaving the user unaware that their data had been stolen. The attackers gained a foothold by exploiting vulnerabilities in poorly secured content management systems (CMS) and third-party JavaScript libraries, injecting their code into backend files and database tables. By operating with such stealth, these Magecart campaigns successfully evaded many traditional security measures and compromised millions of credit card records, causing significant financial and reputational damage to affected companies.[13]

Strategic Redirection

Malicious actors are increasingly focused on strategically manipulating both the destinations to which users are sent and the reasons they appear to be sent there. Rather than relying on bulk spam or drive-by-download approach, they employ selective domain infrastructure manipulation as a central tactic. This strategic manipulation centres on deceiving users by compromising familiar platforms, co-opting trusted environments, or exploiting natural user behavior – transforming routine online activity into vectors for exploitation.

One of the most insidious examples of strategic redirection is the watering hole attack. Rather than targeting individuals directly, attackers compromise legitimate websites frequented by their intended audience – such as industry portals, government service sites, or supply chain partners. By injecting malicious scripts or redirect mechanisms into these trusted sites, they create a passive infection vector that silently compromises visitors. The strategy leverages the implicit trust users place in the site itself, allowing malware delivery or credential theft to occur with minimal suspicion.

Another high-impact method is Search Engine Optimization (SEO) poisoning. Here, malicious actors exploit the algorithms of search engines to artificially boost the visibility of harmful sites. They may create content-rich but fraudulent websites loaded with popular search terms, or employ link-farming techniques – where a network of websites link to each other to artificially boost search engine rankings – to generate fake traffic and backlinks[14] to increase rankings. These tactics increase the likelihood that users will click malicious results, directing them to phishing pages, scam sites, or exploit kits masquer-

[12] IMG element is used to insert images into an HTML page.

[13] "The Art of Concealment: A New Magecart Campaign That's Abusing 404 Pages", accessible at: https://www.akamai.com/blog/security-research/magecart-new-technique-404-pages-skimmer; "Navigating the maze of Magecart: a cautionary tale of a Magecart impacted website", accessible at: https://blog.cloudflare.com/navigating-the-maze-of-magecart/.

[14] Backlinks are links on one website that point to a page on another website, functioning as a "vote of confidence" or citation from one site to another.

ading as legitimate information sources. In effect, threat actors weaponize the search process itself – turning information-seeking behavior into a path for compromise.

While the methods above focus on technical manipulation, a far-reaching and often more effective approach relies on the art of social engineering – the psychological manipulation of people into performing actions or divulging confidential information. Malicious actors use deception and influence to deceive individuals into making security mistakes, often by appealing to emotions like urgency, fear, or a desire to be helpful. The scale of this threat is immense, as a significant majority of cyber-attacks begin with a social engineering component, often delivered by means of a simple email. These attacks bypass even the most sophisticated technical defenses by exploiting the single weakest link in any security chain: the human user. For instance, phishing and spear phishing campaigns use fraudulent emails or messages that appear to come from a trusted source, like a colleague or a financial institution. These messages are crafted to pressure the recipient into clicking a malicious link, downloading an infected attachment, or providing sensitive data like login credentials. The sheer volume and increasing sophistication of these attacks make them a primary vector for ransomware, data theft, and financial fraud, costing organizations and individuals billions of dollars annually.

The above list of strategic approaches is not exhaustive, but demonstrates how modern cybercrime extends beyond technical exploitation into the manipulation of attention, trust, and routine user habits. These approaches represent an operational shift from brute targeting to refined influence over how and where users engage online.

Scaling the Threat: Automation, Bots and Code-Driven Exploits

As the digital ecosystem becomes increasingly automated, so too do the methods of its exploitation. While earlier sections examined the misuse of domains and URLs principally through human deception, threat actors are now scaling their operations through 'programmatic exploitation' – the use of automated systems, scripts, malware, and botnets to manipulate the very infrastructure that underpins web navigation. This mechanized approach enables attackers to operate at speeds and scales that outpace traditional detection mechanisms, allowing for more persistent and concealed abuse of domains and web paths.

One of the most strategically relevant techniques in this category is the deployment of Domain Generation Algorithms (DGAs). Rather than depending on static Command-and-Control (C2) infrastructure, DGAs can generate thousands of pseudo-random domain names daily. These domains act as potential rendezvous points between infected machines and the malicious actor's servers. This rapid generation and rotation of the domain enables malware to maintain reliable communication channels while evading blacklists and takedown efforts. Even when security teams detect and block some domains, others quickly replace them – creating a moving target that is difficult to suppress. DGAs effectively weaponize the domain name system as a rotating maze of concealed pathways for sustaining illicit control and data exfiltration.

Complementing this are fast-flux techniques, in which domain names are rapidly assigned and redirected to a changing set of compromised IP addresses, often part of a wider botnet. This tactic fragments the delivery and hosting infrastructure of malicious content – such as phishing sites, exploit kits, or payloads – across multiple systems worldwide. The continual shifting of endpoints acts as a smokescreen, hindering attribution and takedown, while enabling threat actors to keep critical pathways available to users or bots accessing them. In combination with DGA, fast-flux creates a resilient, layered redirection system that mirrors the legitimate behaviours of Content Delivery Networks (CDNs), further complicating detection.

Programmatic exploitation also facilitates more sophisticated user targeting processes using Traffic Distribution Systems (TDS). These systems analyse incoming traffic based on browser fingerprints, geolocation, device type, or referral sources, and dynamically redirect users accordingly. While appearing benign to automated scanners or security researchers, the same URL can deliver malicious content – including malware, phishing pages, or fraudulent redirects – to users meeting attacker-defined criteria. This selective exposure is a central feature of many modern domain-abuse campaigns, enabling threat actors to conceal their intent while preserving operational efficiency.

Case Example: Avalanche: How Cybercriminals Used Programmatic Exploits

Active from 2009 until its takedown in 2016, Avalanche was a criminal service platform that supported at least 20 different malware families, including Zeus, Dridex, and GozNym. It stands as a prime example of programmatic domain and URL exploitation in history. The platform's resilience stemmed from its sophisticated abuse of domain infrastructure, relying on domain generation algorithms (DGAs) to automatically create thousands of unique domain names for command-and-control communications. Avalanche went further by employing a double fast-flux hosting system, a technique that rapidly rotated both the IP addresses and the DNS name servers themselves, obscuring the infrastructure behind a continuously shifting network of compromised machines. The platform also used traffic distribution systems (TDS) to programmatically redirect users to malicious payloads or phishing pages based on factors like their geolocation or browser type. This combination of techniques enabled the infection of an estimated 500,000 systems worldwide, leading to financial losses in the hundreds of millions of euros. In 2016, a coalition of over 30 countries successfully dismantled the network, seizing or sinkholing over 800,000 malicious domains and taking down 39 servers in a coordinated international law enforcement operation.[15]

A further dimension of exploitation is the automated abuse of legitimate web platforms and services, including cloud infrastructure, content delivery networks, and messaging Application Programming Interfaces (APIs). Here, malicious actors use bots to programmatically register large numbers of domains or accounts, inject malicious links, or host transient exploit kits. Because these activities occur within trusted services, detection is often delayed or suppressed by the inherent credibility of the hosting provider.

This technique allows threat actors to operate under the radar, using compromised or fraudulently obtained infrastructure to propagate concealed pathways and manage campaign logistics at scale. A concerning trend is the use of social media platform bots, which allows threat actors to scale their operations through an integrated and highly effective pipeline. This modus operandi leverages social media platforms as an instant, secure, and resilient command-and-control channel. Instead of relying on traditional backend infrastructure to receive stolen credentials, threat actors embed bot Application Programming Interface (API) keys directly into the phishing pages hosted on Frontend Hosting Platforms (FHPs). When a victim enters their information, the credentials are automatically and instantly relayed to the malicious actor's private social media chat or channel. This combination offers several advantages to threat actors: the entire process, from deploying a new phishing page to receiving stolen data, can be automated allowing a single actor to manage campaigns spanning hundreds of domains simultaneously. They can use bots and channels to manage campaigns without fear of swift takedowns, unlike with traditional malicious infrastructure, and the entire operation can be executed with minimal financial investment, often leveraging free FHP tiers.

[15] "'Avalanche' network dismantled in international cyber operation", accessible at: https://www.europol.europa.eu/media-press/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation.

Forescout explored this concept in more detail in their blog, 'Revamped Phishing Techniques: How Telegram and Front-End Hosting Platforms Scale Campaigns’. They reported that the number of unique domains using Telegram bot APIs and FHPs doubled from mid-June to mid-July 2025 and, using a dataset of 4145 unique API keys, observed that 28% of keys used more than one domain, with some of these using hundreds indicating large-scale campaigns.[16] This demonstrated how automated FHP deployment and Telegram bot functionality represents a significant leap in the scalability of phishing attacks, allowing low-skilled threat actors to conduct highly efficient, global campaigns with unprecedented ease.

Case Example: The Vercel.app and Telegram Pipeline

Forescout reported an example of this new threat model where threat actors impersonated popular corporate services like Microsoft and DocuSign, hosting deceptive login pages on reputable FHP domains like Vercel.app and Netlify.app. Crucially, stolen credentials were not sent to an easily blocked C2 server. Instead, they were instantly exfiltrated to the actor’s mobile device via a Telegram bot API key embedded directly in the phishing page code. This provided a secure, real-time channel for data collection, making the entire operation both robust and difficult to disrupt.[17]

Collectively, these programmatic strategies underscore a critical shift where they are dynamically exploited using automated programs, a transformation that magnifies the threat landscape, enabling malicious actors to deploy high-speed, evasive, and persistent campaigns that exploit the trust and openness of the web’s foundational architecture. Addressing this layer of abuse requires defenders to move beyond static lists and signature-based detection, and shifting toward behavioural analytics, traffic pattern monitoring, and systematic collaboration with registries, hosting providers, and DNS operators.

[16] Michele Campobasso, Amine Amri, Daniel dos Santos, and Forescout Research - Vedere Labs, "Revamped Phishing Techniques: How Telegram and Front-End Hosting Platforms Scale Campaigns", Forescout, September 2025, accessible at: https://www.forescout.com/blog/revamped-phishing-techniques-how-telegram-and-front-end-hosting-platforms-scale-campaigns/.

[17] Michele Campobasso, Amine Amri, Daniel dos Santos, and Forescout Research - Vedere Labs, "Revamped Phishing Techniques: How Telegram and Front-End Hosting Platforms Scale Campaigns", Forescout, September 2025, accessible at: https://www.forescout.com/blog/revamped-phishing-techniques-how-telegram-and-front-end-hosting-platforms-scale-campaigns/.

BEYOND THE BREACH: CONSEQUENCES AND OUTCOMES

The exploitation of digital trust pathways by serious and organized criminal groups is not an end in itself but a tactical enabler – used to initiate, escalate, and monetize broader criminal campaigns. Domains, URLs, and traffic systems are the connective tissue of the cybercrime ecosystem: they serve as entry points, distribution channels, and execution mechanisms. They are the concealed scaffolding of digital exploitation – the technical foundations upon which threat actors construct campaigns.

Yet, the typologies only tell part of the story as the ultimate impact of cybercrime is only realized through the criminal objectives these techniques enable. Motivations behind such exploitation span a broad spectrum of cybercrime, from offences entirely digital in nature, where infrastructure is weaponized to propagate spam, distribute malware, sustain botnets, or orchestrate phishing and pharming attacks, to traditional crimes such as fraud, extortion, or coercion that are facilitated and amplified by digital tools. These cybercrimes are also not isolated events, they form sequential stages that culminate in an operational continuum involving multiple threat actors each playing a part in achieving the ultimate end goal. In practice: a single malware campaign may function simultaneously as a vector for credential theft, a platform for ransomware deployment, or a conduit for financial fraud.

To disrupt such activity, the response must not only address the technical scaffolding of abuse but also the operational outcomes it supports. As such, this report now moves beyond typologies to focus on the more technical methods that scale and sustain cybercrime, and the end goal motivations that drive it.

The Backbone of Cybercrime

Organized cybercrime relies on sophisticated methods that sustain its operations. Techniques such as phishing, pharming, malspam, malware, botnets, and Cybercrime-as-a-Service form the operational backbone, enabling criminals to scale their activities, evade detection, and maintain persistent control over digital infrastructure. Understanding these mechanisms is essential before turning to the underlying motivations and broader societal impacts that drive such illicit activity.

Scaling Reach and Manipulation: Phishing, Pharming, and Spam

Phishing remains the most versatile and adaptable delivery vector in organized cybercrime. Once associated with crude mass-mailing scams, it has evolved into a highly engineered operation designed for credibility and scale. Threat actors exploit domain deception techniques, such as typosquatting, homograph domains, and subdomain spoofing, and construct URLs that mimic legitimate entities. Hypertext Transfer Protocol Secure (HTTPS) certificates, redirect chains, and obfuscated parameters further obscure intent, creating the illusion of authenticity. Within this infrastructure, a malicious link becomes more than a lure:

it is the pivot point through which credentials are harvested, malware is delivered, and financial fraud is initiated. Phishing is not an isolated practice but rather an embedded element of criminal workflows, sustaining Business Email Compromise (BEC), ransomware distribution, and access-for-sale models on dark markets. Increasingly personalized and adaptive, these campaigns use cloaking and analytics to adjust in real time – evading automated filters and prolonging infrastructure viability.

The evolution of phishing techniques reflects this constant innovation. Alongside familiar variants such as vishing (voice-based phishing) and smishing (SMS phishing), attackers have introduced QR code phishing ('quishing'), which weaponizes seemingly benign QR codes to redirect victims to malicious URLs or deliver harmful payloads. More recently, the so-called ClickFix technique has emerged, where fake error or CAPTCHA pop-ups instruct users to copy and paste malicious code or download a trojanized update.[18] By turning a victim's own actions into the infection vector, ClickFix lowers technical barriers for threat actors while increasing the likelihood of bypassing automated defences. Together, these developments highlight the expanding arsenal of phishing methods and reaffirm the central role of domains, URLs, and web traffic systems as the structural enablers of deception and compromise.

Case Example: Rhadamanthys and the Rise of ClickFix

Following the takedown of the previously dominant Lumma infostealer, Forescout observed the emergence of a new variant, Rhadamanthys. Campaigns associated with Rhadamanthys employed the ClickFix technique, in which victims were presented with fraudulent verification prompts that induced them to paste malicious PowerShell commands. These commands then contacted attacker-controlled domains and retrieved payloads via authentication-protected URLs, a design intended to evade basic detection mechanisms. Obfuscated across multiple stages, the infection chain ultimately deployed Rhadamanthys version 0.7.0, capable of harvesting credentials, cookies, browser data, and cryptocurrency wallets. This case exemplifies both the rapid evolution of infostealer malware and the critical role of domain infrastructure and web traffic systems in facilitating large-scale cybercrime.[19]

Pharming attacks operate at a deeper level, subverting the technical mechanisms that mediate digital trust. By manipulating DNS records, router settings, or host files, malicious actors redirect users to fraudulent replicas of trusted services without any overt user action. Where phishing depends on user engagement, pharming removes this, so that victims may type the correct URL yet still arrive at an attacker-controlled page.

[18] "Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025", accessible at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[19] "Infostealer Watch: Will Lumma's Takedown Help Rhadamanthys' Rise?", accessible at: https://www.forescout.com/blog/infostealer-watch-will-lummas-takedown-help-rhadamanthys-rise/.

This redirection exploits hijacked, expired, or misconfigured domains, weaponizing trust in the DNS system itself. For organized criminal groups, pharming is particularly attractive because of its stealth: compromise occurs invisibly, enabling long-term credential harvesting or malware delivery without triggering suspicion. As such, pharming illustrates the infrastructural dimension of URL exploitation – where deception occurs not at the surface of user interaction, but within the architecture of the Internet itself.

Malspam, often dismissed as nuisance traffic, remains foundational to the criminal supply chain. It is the primary mass-distribution channel for phishing lures, malicious links, and reconnaissance probes. Criminal groups exploit bulk-registered or hijacked domains to embed malicious URLs within seemingly routine communications – billing notices, shipping updates, internal memos, or promotional offers.

Malspam infrastructure often leverages botnets to distribute high-volume campaigns across global IP ranges, thereby evading filtering systems. Cloaked redirect chains, URL shorteners, and encoded parameters can obscure the true destination of links. Many campaigns also employ domain generation algorithms (DGAs) or expired domains to bypass reputation-based defences. In this way, malspam sustains cybercrime at industrial scale, providing the distribution engine that initiates user engagement and drives victims into the wider web of exploitation.

Case Example: DarkGate Loader Malspam Campaign

In mid-2023, researchers identified a global malspam campaign delivering the DarkGate loader, an 'as-a-service' tool designed to gain footholds and deploy secondary payloads. The campaign relied on large volumes of phishing-style emails that embedded malicious links in attachments or message bodies. Victims who clicked were redirected through obfuscated URLs, often hidden behind encoded parameters or chained redirects, before reaching attacker-controlled sites hosting the loader. Once installed, DarkGate enabled credential theft, fraud, access-as-a-service, and the deployment of additional tools such as ransomware or remote access trojans (RATs). The case highlights how digital trust pathways remain central to organized cybercrime workflows, turning a single phishing lure into a multi-stage conduit for broader exploitation and monetization.[20]

[20] "DarkGate Loader Malspam Campaign", accessible at: https://www.forescout.com/resources/darkgate-loader-malspam-campaign/.

Sustaining Control and Persistence: Malware and Botnets

Malware is the weaponized outcome of delivery mechanisms such as phishing, pharming, and spam. Rarely delivered as direct attachments, contemporary malware is accessed almost exclusively through malicious URLs embedded in emails, fake websites, ads, or compromised platforms. These URLs are often hosted on disposable or repurposed domains, masked through redirect chains or cloaking services that block automated analysis. Some campaigns also employ fast-flux DNS or bulletproof hosting to maintain operational continuity.

Whether ransomware, infostealers, or remote access trojans, malware payloads today are modular and adaptive. Infection can escalate from initial compromise to full network control, enabling extortion, espionage, or theft of financial and personal data. Here, domain exploitation is not merely a gateway – it is the delivery architecture that allows malicious code to circulate, adapt, and persist within target environments.

Botnets embody the industrialization of cybercrime. These distributed networks of infected machines are the engines that sustain persistent campaigns: distributing spam, hosting phishing content, enabling credential stuffing, launching denial-of-service attacks, and mining cryptocurrencies.

Their resilience lies in their control structures, which are almost universally domain-based. Command-and-control (C2) infrastructure relies on rotating domains generated algorithmically, or on fast-flux techniques that obscure server locations by constantly shifting IP addresses. Increasingly, botnets embed C2 instructions into legitimate but compromised domains, making detection and takedown significantly harder.

For organized crime groups, botnets are not merely technical tools but scalable business assets. They provide automation, persistence, and resilience – the qualities that allow cybercrime to operate continuously across borders and industries. Their reliance on domain infrastructure abuse underscores the necessity of DNS-layer visibility and systemic monitoring as essential countermeasures.

Case Example: Chaya_002 Malware Cluster

Forescout recently investigated a malware cluster called Chaya_002 that disguises itself as legitimate software installers, including Google Chrome, Microsoft Teams, and Microsoft Edge. Threat actors exploit digital trust pathways – the links and sites users inherently trust – to trick them into downloading malicious files. For example, compromised pathways such as *apple-online[.]shop* and scripts embedded via *tayakay[.]com/analytics.js* redirect users to other infected sites, where the malware is staged for download.

Once executed, Chaya_002 gathers system and network information, establishes persistence, and communicates with command-and-control servers to enable further attacks. The malware constantly evolves, with file names, hosting locations, and digital signatures changing to evade detection.

This case underscores the dual risk of abuse of digital trust pathways – manipulated links, compromised sites, and multi-stage redirection – and the human element, where users are misled into running what appears to be legitimate software.[21]

Industrialization of the Threat: Cybercrime-as-a-Service (CaaS)

The industrialization of these threats is most visible in the rapid growth of Cybercrime-as-a-Service (CaaS), which has commoditized nearly every element of a cyber-attack – from phishing kits and botnet rentals to pre-packaged exploit tools. By dramatically lowering the barrier to entry, CaaS transforms cybercrime from an activity once restricted to skilled operators into an accessible, scalable enterprise. This has broadened the threat landscape, enabling a wider and more diverse range of criminal actors to exploit digital trust pathways with increasing frequency, reach, and unpredictability.

In Europol's Internet organized Crime Threat Assessment (IOCTA)[22], phishing-as-a-service was highlighted as a particularly fast-growing segment within this market. Here, ready-made products, services, and victim data are packaged and sold to criminal actors and networks, regardless of their level of organization or technical expertise. Phishing kits – widely available on dark markets and forums – contain all the components necessary to conduct large-scale social-engineering campaigns. Typically, these kits include code for fraudulent webpages that closely mimic legitimate payment platforms or well-known services, often accompanied by instructions for drafting convincing phishing emails. Once deployed, the URLs of these counterfeit pages are distributed through phishing, spam, or malvertising campaigns, frequently orchestrated via botnet-based droppers to automate delivery and maximize reach. For criminals targeting financial data and access to payment systems, such kits and associated tools have become indispensable, illustrating how CaaS not only expands participation in cybercrime but also systematizes its methods of deception and exploitation.

[21] "Sly Malware Found in Fake Google Chrome and MS Teams Installers", accessible at: https://www.forescout.com/blog/sly-malware-found-in-fake-google-chrome-and-ms-teams-installers/.

[22] "Steal, deal and repeat - How cybercriminals trade and exploit your dataInternet Organised Crime Threat Assessment (IOCTA) 2025", accessible at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

The Criminal End Goals

While phishing, pharming, spam, malware, and botnets are malicious in their own right, it is important to recognize that their primary role is as enablers. They provide the essential delivery systems, persistence mechanisms, and amplification tools that allow more traditional criminal enterprises to scale in the digital age. Many of these crimes, such as theft, fraud and exploitation, have always relied on deception and a supporting infrastructure. What has changed is the medium. The very same manipulations of domain infrastructure that distribute spam, sustain botnets, and scale traditional crime, also provide the anonymity, resilience, and cross-border reach for offences that once depended on face-to-face interaction or physical intermediaries. Instead, a deceptive link is now the invitation to a fraudulent investment platform. A hijacked domain is the digital storefront for counterfeit goods. A hidden URL is the covert gateway to illegal marketplaces or extremist financing campaigns. The result is not simply the digitization of crime, but its multiplication and anonymization. The broader domain infrastructure must not therefore be considered as passive technical artefacts but rather as strategic levers that enable both the expansion and the concealment of traditional criminal economies.

Data and identity theft is one of the most common and impactful outcomes of domain and URL exploitation. Phishing portals, pharming redirects, and spoofed login pages funnel victims into disclosing sensitive details: email credentials, banking logins, social media accounts, or healthcare identifiers. The stolen information is then monetized in multiple ways: directly through account takeovers, indirectly via dark market resale, or strategically as a foothold for further compromise.

Business Email Compromise (BEC) exemplifies this continuum. By impersonating trusted domains or embedding links to counterfeit invoice portals, organized groups trick employees into authorizing fraudulent transfers amounting to millions of dollars. Each success relies not only on social engineering but also on the structural credibility of manipulated domains.

Case Example: The $42 Million Invoice

In mid-2024, a commodity firm in Singapore fell victim to a sophisticated Business Email Compromise (BEC) scam, which is a prime example of how these crimes work in the modern digital landscape. The fraud began when the firm received an email that appeared to be from one of its regular suppliers. However, the email was a spoofed version of the supplier's legitimate address, with a slightly altered domain name designed to look identical at a glance.

The fraudulent email instructed the firm to wire a pending payment of $42.3 million for services to a new bank account in Timor-Leste. Unaware of the deception, the company authorized the transfer.

The BEC criminals had successfully exploited the trust associated with a familiar business relationship and the structural credibility of a legitimate-looking domain.

Within days, the firm realized the fraud and immediately reported it to the Singapore Police Force. Authorities were able to rapidly coordinate with their counterparts in Timor-Leste. This swift international cooperation allowed them to intercept and freeze $39.3 million of the stolen funds before the scammers could fully launder the money. This case exemplifies the critical role of both social engineering and domain manipulation in BEC, while also demonstrating the effectiveness of rapid international collaboration in combating these borderless crimes.[23]

Fraud remains the most damaging and prolific cyber-enabled criminal outcome. Investment scams, romance frauds, advance fee schemes, and tech support frauds all deploy the same technical strategies: domains that mimic legitimate institutions, shortened or obfuscated URLs that mask their true destination, and malicious links embedded in emails, social media, advertisements, or instant messages.

The rise of fraudulent investment platforms illustrates the industrialization of these techniques. Thousands of domains are generated daily using domain generation algorithms, creating lookalike trading portals. Victims are funnelled through redirect chains and cloaking layers before arriving at dashboards designed to instill trust, often complete with fabricated returns. Once deposits are made, accounts are frozen or wiped, leaving no recourse.

Romance fraud – sometimes, though controversially, referred to as “pig butchering” – relies on the same infrastructure, though applied with more intimate manipulation. Links delivered in personal messages, often shortened through services like Bitly or TinyURL, redirect victims to fake fundraising pages or fraudulent crypto wallets. Here, the obfuscation of URLs masks not just the destination, but also the emotional trap being set, transforming trust into an instrument of theft.

Advance fee scams extend this logic further. Victims receive legal-looking correspondence directing them to domains that mimic law firms or banks, often registered days before the campaigns launch. A masked hyperlink becomes the lever through which victims are convinced to pay for prizes, inheritances, or opportunities that do not exist.

[23] “Police recover over USD 40 million from international email scam”, accessible at: https://www.interpol.int/en/News-and-Events/News/2024/Police-recover-over-USD-40-million-from-international-email-scam.

Case Example: Global Crypto Scam Pyramid Scheme

Palo Alto Networks' Unit 42 uncovered a global campaign of fraudulent cryptocurrency platforms structured as pyramid schemes. The platforms, often promoted through social media, lured tens of thousands of victims with promises of high returns. The scammers operated by creating an average of 15 new domains per day and distributing access via both websites and fraudulent Android-based mobile applications. The victims were deceived by professional-looking dashboards that tracked fabricated returns, with their funds being stolen in a Ponzi-like fashion before they were ultimately locked out of their accounts.[24]

It should be noted that not all cyber fraud exploitation ends in direct theft. Increasingly, criminal groups are monetizing victim traffic itself. Redirect chains embedded in malicious links lead users through ad-fraud networks or other affiliated scams, where each click generates revenue. Victims may pass through multiple intermediate domains before landing on malicious or fraudulent content, with each transition generating income for the attacker. This form of exploitation converts the infrastructure of the Internet into a business model: hijacked domains, manipulated DNS, and obfuscated URLs are repurposed not just to deceive but to generate profit through volume.

Ransomware has become one of the most disruptive outcomes of web infrastructure abuse, where domains and URLs act as the scaffolding for delivery, execution, and extortion. Malicious domains are often registered solely to host ransomware payloads, command-and-control (C2) servers, or data-leak portals used in double-extortion schemes. Obfuscated URLs embedded in phishing emails or redirects from compromised websites serve as the initial click-path, guiding victims to exploit kits or payload repositories. Fast-flux networks and bulletproof hosting providers further shield these domains from takedown, ensuring the persistence of infrastructure across campaigns. Once deployed, ransomware operators increasingly leverage 'shaming sites' hosted on attacker-controlled domains to pressure victims by threatening public exposure of stolen data. In this way, ransomware illustrates not only the economic damage of cybercrime but also how digital trust pathways are strategically weaponized to sustain attacks, enforce ransom demands, and maximize coercive leverage over victims.[25]

The exploitation of digital infrastructure further extends into crimes of physical coercion and abuse. Domain infrastructure abuse has become a systemic tactic in the distribution of Child Sexual Abuse Material (CSAM), underscoring the role of domain infrastructure as a critical enabler of persistent online child sexual exploitation and abuse. In 2023, the Internet Watch Foundation (IWF) identified 238 different top-level domains (TLDs) exploited to distribute child sexual abuse material – a 14% increase over

[24] "Investigating Scam Crypto Investment Platforms Using Pyramid Schemes to Defraud Victims", accessible at: https://unit42.paloaltonetworks.com/fraud-crypto-platforms-campaign/.

[25] "Top-level domain hopping", accessible at: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/top-level-domain-hopping/.

2022. Generic TLDs (gTLDs) were particularly impacted, rising by 47%, from 97 in 2022 to 143 in 2023.[26] Additionally, the Internet Watch Foundation reported widespread 'top-level domain hopping' activity to evade takedown. In 2023, 222 such domain strings hopped at least once, totalling 300 individual hops moving their second-level domain names to a new TLD.

Registries, registrars, and hosting providers can play a pivotal role in disrupting the distribution of CSAM. Under ICANN's framework, contracted parties are expected to address 'DNS abuse', and many extend this responsibility to CSAM through 'trusted notifier' schemes with bodies such as the IWF and the National Centre for Missing and Exploited Children (NCMEC). These arrangements allow accredited reports to trigger the rapid suspension of offending domains.

However, enforcement remains uneven as ICANN's contracts do not explicitly define DNS abuse, leaving action related to CSAM, and other traditional content-driven crime, voluntary and inconsistent across the industry. As such, some gTLD operators have been slow to implement CSAM trusted notifier schemes, while systemic issues, such as minimal registrar due diligence, opaque WHOIS data, and slow response times, allow domains linked to CSAM to persist. Verisign, operator of .com and .net, has drawn particular criticism for delays in implementing trusted notifier programmes and for a lack of transparency on takedown action. These gaps highlight how fragmented obligations and governance failures continue to provide opportunities for persistent exploitation of domain infrastructure by CSAM networks.

Continuing on the theme of exploitation, criminals involved in human trafficking use deceptive advertising to lure victims to malicious websites or embed malicious links in fake job advertisements, escort listings, or social media profiles. These links often redirect to password-protected sites or encrypted landing pages, where victims are advertised or recruited under false pretenses. Domains are cycled or re-registered frequently, creating a rolling infrastructure of exploitation that is highly resistant to takedown.

INTERPOL has identified this as a rapidly evolving global threat in which human trafficking victims are not only exploited but also co-opted into perpetuating the criminal enterprise.[27] Initially recruited through deceptive job advertisements and trafficked under false promises, these individuals are forced to operate from 'scam centres,' conducting large-scale online fraud. Once ensnared, victims are compelled to use digital platforms to carry out investment scams, romance fraud, and cryptocurrency scams – via phishing links, spoofed websites, and manipulated social media URLs – effectively recruiting and ensnaring new victims into the same cycle. What began in Southeast Asia has now spread to offices and rental compounds across West Africa, the Middle East, and beyond, illustrating how the system continuously regenerates itself through its own human targets.

[26] "Abuse of Top-Level Domains (TLDs)", accessible at: https://www.iwf.org.uk/annual-report-2023/trends-and-data/abuse-of-top-level-domains-tlds/.

[27] "INTERPOL issues global warning on human trafficking-fueled fraud", accessible at: https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud.

The success of these operations depends heavily on deceptive use of URLs and web pathways – from fake job portals designed to recruit both victims and scam targets, to socially engineered messages embedding links redirecting to fraudulent scam platforms. These platforms are often structured to evade filters through look-alike domain names, multi-stage redirections, and short-lived hosting setups.

INTERPOL's 2023 "Orange Notice" warning highlights how these scam centres exploit digital trust pathways to orchestrate both trafficked labour and global financial fraud. This dual physical and online threat model underscores the role of domain infrastructure abuse as both recruitment and fraud vectors in a single criminal ecosystem.[27]

Counterfeiting and Intellectual Property (IP) crime increasingly exploit digital trust pathways to evade detection and facilitate illicit sales. Maliciously registered domains impersonate legitimate brands, while cloaked subdomains – sometimes referred to as 'deep links' by the IP stakeholder community – direct buyers straight to infringing products and grant access to product pages that bypass automated scanning. Counterfeit marketplaces also operate through superficially benign listings, with hidden instructions or encoded links shared via social media platforms, encrypted chats, or other private channels – a discreet ecosystem of dark commerce.

Within this ecosystem, a common tactic is the 'hidden link' system used on e-commerce platforms, where counterfeit listings would otherwise be prohibited. Sellers publish off-platform catalogs displaying genuine branded products alongside product codes and hyperlinks. When a buyer clicks the hyperlink, it resolves to a listing that shows only generic images and neutral descriptions. The buyer identifies the counterfeit item by matching the product code to the generic listing.[28]

This system is further sustained because sellers operate at scale through social media platforms like Facebook, Telegram, Instagram, and TikTok, where they can instruct buyers not to mention brand names in communications or reviews and not to upload photographs of the real products. Feedback is deliberately kept vague ("good quality," "fast shipping") to avoid moderation.

Importantly, although many consumers are deceived by counterfeit schemes, there is a growing group of willing participants, reflecting a shift in the victim profile. In the case of hidden links, consumers are no longer deceived – they knowingly select counterfeit goods. Here, the true victims are the intellectual property rights owners, who suffer the broader harms of counterfeiting.

This dual-faceted strategy highlights the sophistication of modern IP crime: the same web-based techniques – combining deep links and hidden links – can target both uninformed consumers and seemingly consenting participants, exploiting the structure and policies of legitimate e-commerce platforms to facilitate large-scale counterfeit distribution while minimizing the risk of detection.

[28] "11 ways to detect Aliexpress' hidden links", accessible at: https://www.redpoints.com/blog/aliexpress-hidden-links/.

Case Example: Amazon's "Hidden Links" Lawsuit

In 2023, Amazon's Counterfeit Crimes Unit filed a lawsuit against two social media influencers, Kamryn Russell and Ashley Hawat, along with other co-conspirators, after uncovering a sophisticated counterfeit operation reliant on hidden links. The group promoted luxury goods through social media, directing followers to Amazon listings that, on the surface, appeared entirely legitimate. The product pages were generic, with neutral wording and images carefully stripped of any brand identifiers.

Behind this façade, however, the links acted as gateways to counterfeit trade. Followers who were aware of the scheme understood that purchasing through these listings would result in receiving counterfeit luxury goods rather than the unbranded items shown. By embedding this system of covert redirection, the network was able to mask illicit sales and bypass Amazon's automated detection mechanisms, which are designed to filter out infringing listings.[29]

Moving on from counterfeiting and IP crime, but still within the theme of willing participants, extremist networks likewise employ web exploitation and obfuscation tactics to minimize detection risks while fundraising and recruiting. Initial outreach often begins on Telegram or other encrypted messaging or social media platforms, where links to propaganda or recruitment materials are shared. These frequently take the form of concealed or shortened URLs that redirect users to donation pages hosted on bulletproof services, and often mirrored on the dark web. To frustrate law enforcement efforts, domains are rotated rapidly, while links embedded in encrypted messaging platforms guide individuals toward radicalization content or closed forums.

[29] "Amazon Sues Alleged Counterfeiters in 'Hidden Links' Scheme", accessible at: https://www.pymnts.com/news/security-and-risk/2023/amazon-sues-alleged-counterfeiters-in-hidden-links-scheme/.

Case Example: Islamic State Cyber-Enabled Fundraising via Website Abuse

In 2020, U.S. authorities dismantled a cyber-enabled terror finance scheme linked to the Islamic State in Iraq and the Levant (ISIL/Da'esh), coordinated by Murat Cakar, who managed select Da'esh hacking operations. The scheme exploited websites to solicit funds under the guise of selling COVID-19 protective equipment. One such site, FaceMaskCenter[.]com, falsely claimed to sell FDA-approved N95 masks in large quantities, targeting global customers, including hospitals and other critical institutions in the United States.

The website, along with four associated Facebook pages, was used to generate revenue that ultimately supported Da'esh operations. Law enforcement seized the website and the associated cryptocurrency accounts, disrupting both the fraudulent sales and the funding stream to Da'esh. The case illustrates how terrorist organizations have adapted to the digital era, leveraging online platforms, e-commerce fronts, and cryptocurrency to fundraise and sustain operations.[30]

The cases outlined above represent only a fraction of the diverse criminal outcomes and consequences enabled by web infrastructure abuse. While a comprehensive analysis of every crime type lies beyond the scope of this report, the examples provided illustrate how the fusion of traditional criminal motives with the manipulation of digital trust pathways has transformed the scale, reach, and sophistication of organized crime and other criminal activities. The very infrastructure that supports legitimate commerce and communication has been systematically repurposed into a resilient engine of exploitation. Addressing this challenge requires a shift in perspective: digital trust pathways must be understood not as ancillary tools, but as a strategic element of contemporary criminal enterprise.

[30] "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns", accessible at: https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns/.

EMERGING THREATS: BLOCKCHAIN DOMAINS AND AI-DRIVEN EXPLOITATION

Although the exploitation of digital trust pathways is now a well-established threat, two emerging elements consistently surfaced as priority concerns during the course of the research – blockchain-based domain systems and artificial intelligence (AI). These threats are not wholly new and many are already observable in the current landscape, but their rapid growth, evolving modalities, and lack of comprehensive analysis make them particularly pressing. Both technologies offer clear and legitimate benefits, yet they also present new avenues for abuse by serious and organized criminals. By leveraging these tools, criminal actors are positioned to enhance operational resilience, evade detection mechanisms, and scale their illicit activities in ways that remain poorly understood and insufficiently mitigated.

Blockchain-Based Domain Systems

Among the emerging technologies reshaping the domain ecosystem, blockchain-based domain systems stand out as both a significant innovation and a potential enabler of cybercrime. Unlike the traditional Domain Name System (DNS) – coordinated under the oversight of ICANN and subject to established governance and dispute resolution processes – blockchain-based domains are decentralized, immutable, and tied directly to cryptographic wallet ownership. This model offers novel opportunities for resilience, user autonomy, and identity sovereignty, but also introduces critical vulnerabilities that are already being exploited.

Recent mapping by Oxford Information Labs and the French Association for Cooperative Internet Naming (AFNIC) identified more than 7.2 million blockchain domains registered in 2023 alone, noting Verisign's quarterly DNS registration estimates blockchain registrations to be approximately 0.5% of all domain activity worldwide. These are distributed across multiple providers such as Ethereum Name Service (ENS), Unstoppable Domains, and Zilliqa Name Service, each adopting different operating models. For example, some allow the registration of entire top-level domains, while others offer second-level names under existing blockchain extensions such as .eth, .crypto, or .wallet, and DNS integrations are inconsistent.[31]

This fragmented and fast-growing ecosystem has created both opportunities for innovation and new challenges for stability. The benefits of blockchain-based domains are clear, as they can provide strong protection against hijacking or unauthorized transfer, since ownership is secured through private keys. They offer resilience against censorship and can support decentralized applications (dApps) and self-sovereign identity infrastructures, enabling users to exert greater control over their digital presence. These are all features that align with legitimate aspirations for greater autonomy, privacy, and security in online interactions.

[31] "Mapping Blockchain Domain Providers: 10 Key Findings from Oxford Information Labs and AFNIC", accessible at: https://oxil.uk/blog/mapping-blockchain-domain-providers-10-key-findings-from-oxford-information-labs-and-afnic.

However, the absence of governance and dispute resolution mechanisms has created an environment ripe for abuse. Once registered, a blockchain domain cannot be reclaimed or suspended by central authorities, even in cases of fraud, infringement, or criminal misuse. Namespace collisions – where blockchain top-level domains overlap with or pre-empt ICANN-managed domains – further complicate the landscape, generating confusion for users and offering criminals new avenues for deception.31 For instance, a blockchain-registered .wallet or .crypto address could be leveraged in phishing campaigns or fraudulent investment schemes, with few practical means of intervention. Similarly, research shows that blockchain registries can map human-readable names to the InterPlanetary File System (IPFS) content identifiers (CIDs), and, since phishing campaigns are already leveraging IPFS for decentralized content storage, the combination of these technologies could make malicious content more resilient and censorship-resistant, creating new challenges for detection and takedown.[32]

In sum, blockchain-based domains illustrate the dual-edged nature of technological innovation. On one hand, they embody the promise of secure, censorship-resistant digital identities. On the other, they present a series of governance, interoperability, and enforcement gaps that can be exploited by organized crime. Their emergence underscores a critical point: as domain technologies evolve, so too do the methods by which malicious actors can manipulate these systems, reinforcing the need for anticipatory governance and international coordination.

AI-Enhanced Exploitation

AI is rapidly reshaping both the methods and scale of online exploitation. In the context of web infrastructure abuse, AI tools are enabling criminals to generate deceptive domains, polymorphic phishing URLs, and dynamic redirect chains with a level of automation and sophistication previously unattainable. Where earlier campaigns relied on static lures and fixed templates, AI now allows threat actors to tailor malicious pathways to individual targets, constantly mutating domains and links to evade detection. This accelerates not only the speed of attacks but also their resilience, as blacklisting and filtering become far less effective against constantly shifting identifiers.

The integration of AI with social engineering techniques compounds this risk. Attackers are using large language models (LLMs) to craft highly persuasive phishing messages, complete with contextual cues drawn from publicly available data. Phishing texts and scripts generated through generative AI incorporate the language and cultural nuances of intended victims, making campaigns far more effective. In fact, recent studies have shown that phishing messages produced by LLMs achieve significantly higher click-through rates than those written manually. The first malicious variants of LLMs, detected in 2023, have already been weaponized for this purpose, fuelling increasingly convincing phishing, malvertising,

[32] "Threat Spotlight: Cyber Criminal Adoption of IPFS for Phishing, Malware Campaigns", accessible at: https://blog.talosintelligence.com/ipfs-abuse/; and "A Survey on Content Retrieval on the Decentralised Web", accessible at: https://dl.acm.org/doi/10.1145/3649132.

and malspam campaigns.[33] These lures are typically embedded in URLs that mimic legitimate institutions, supported by typosquatted domains or cloaked subdomain structures. At the same time, deepfake content – voices, images, and videos – is being deployed to reinforce credibility, making phishing pages and fraudulent portals far more convincing than traditional templates.[34]

While these developments present clear risks, it is important to acknowledge AI's dual-use potential. As noted in its recent analyses, AI holds promise for strengthening the DNS ecosystem by enhancing anomaly detection, enabling faster identification of abuse patterns, and supporting the scalability of defensive measures. Yet, as with blockchain-based naming systems, governance gaps and interoperability challenges remain significant, particularly where AI-driven abuse falls outside the traditional DNS framework.[35]

[33] "Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025", accessible at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[34] "Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025", accessible at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[35] "Symbiotic Futures: ICANN's Interaction with Artificial Intelligence", accessible at: https://dn.org/symbiotic-futures-icanns-interaction-with-artificial-intelligence/.

FORTIFYING THE DIGITAL ECOSYSTEM: A MULTISTAKEHOLDER APPROACH

The stability and security of the global domain infrastructure are foundational to the safe and reliable functioning of the digital ecosystem. Yet, as this report demonstrates, that very infrastructure is increasingly exploited by serious and organized criminal actors. By capitalizing on technical vulnerabilities, regulatory inconsistencies, and gaps in cross-border cooperation, these actors construct and sustain complex cybercrime supply chains. In doing so, they transform digital trust pathways into instruments of fraud, malware distribution, and systemic abuse, eroding trust in the architecture designed to enable global connectivity and development.

Addressing this exploitation requires more than incremental technical remedies. It calls for a coordinated, multistakeholder strategy that unites governments, registries, private industry, and civil society. Legal frameworks must adapt to evolving patterns of abuse; verification and transparency in domain registration must be reinforced; and new models of international cooperation must emerge to disrupt the cross-jurisdictional ecosystems that underpin organized cybercrime. Protecting this infrastructure therefore demands a holistic approach – treating cybercrime not as a series of isolated incidents, but as a continuous, adaptive challenge requiring a sustained, collective response.

1. Technical Innovation

Enhancing the defence of domain infrastructure against abuse requires parallel investment in both technical innovation and human expertise. The volume and velocity of domain registrations and URL activities – often created and weaponized at automated speed – necessitate equally advanced detection and mitigation tools. Artificial intelligence, behavioural analytics, and large-scale pattern recognition systems are increasingly central to this effort, allowing analysts to assess hundreds of variables in real time and flag infrastructure associated with phishing, malware, or coordinated abuse campaigns. Continued innovation in these areas is critical to staying ahead of threat actors who themselves exploit automation to evade detection.

However, technology alone cannot address the evolving threat landscape. Effective monitoring and disruption require skilled professionals capable of designing, deploying, and refining these systems, as well as interpreting signals that fall outside algorithmic models. Expanding the pool of technical specialists – including data scientists, threat analysts, and domain infrastructure engineers – will be essential to ensure that innovation translates into operational resilience. Building this capacity requires investment not only in recruitment and training, but also in sustaining cross-sector knowledge exchange between the private sector, registries, law enforcement, and the technical community.

Together, the advancement of technical tools and the strengthening of the personnel who operate them represent mutually reinforcing pillars of a more resilient digital trust ecosystem. Without both, efforts to counter domain abuse will remain reactive and fragmented, leaving critical gaps for organized criminal actors to exploit.

2. Multistakeholder Collaboration

Cybercrime increasingly demonstrates the interconnectedness of technical and content-based abuses, underscoring the need for holistic approaches across the digital ecosystem. The fragmentation of actors – including core Internet governance and infrastructure entities, private sector stakeholders, public authorities, civil society, and end-users – at global, regional, and national levels complicates effective responses. Addressing this challenge requires structured collaboration that spans the entire digital trust pathway ecosystem.

Digital Trust Pathway Ecosystem

Category	Stakeholders
Internet Governance & Infrastructure	ICANN, Registries, Registrars, Resellers, Hosting Providers, DNS Operators, Certificate Authorities, Internet Engineering Task Force (IETF)
Private Sector / Commercial	Internet Service Providers (ISPs), Content Delivery Networks (CDNs), Advertising Networks, Payment Providers, Cybersecurity Firms, Domain Brokers, Social Media Platforms
Public Sector & Policy Actors	National Governments, Law Enforcement Agencies, Judicial Authorities, International Organisations (e.g., Europol, Interpol, UN bodies), Computer Emergency Response Teams (CERTs/CSIRTs)
Civil Society & End-Users	End-Users, Civil Society Organisations (CSOs), Academia
Cross-Cutting / Ecosystem Coordinators	Multistakeholder Forums, Industry Associations, Information-Sharing Platforms

Recognizing the limitations of prescriptive regulation alone and the need to foster partnership and shared responsibility, one promising model is the establishment of a global digital trust taskforce. In collaboration with existing governance structures such as ICANN, which focus primarily on technical coordination, this taskforce would convene multistakeholder expertise across technical, policy, and content domains to develop consensus-driven standards, guidance, and best practices. By enabling ongoing dialogue and coordinated action across these layers, the taskforce could enhance resilience against cybercrime while securing legitimacy and broad participation from a diverse range of stakeholders.

3. Globally Recognized Standards

The absence of harmonized regulation across jurisdictions creates structural vulnerabilities that organized criminal actors actively exploit. While some countries have introduced stronger legal frameworks – such as limits on bulk domain registrations, mandatory "Know Your Customer" (KYC) checks for registrants, clearer rules assigning content responsibility to domain owners and hosting providers, and proportionate powers to seize or transfer domains – these efforts remain uneven. The lack of global unity allows malicious actors to shift their operations to jurisdictions with weaker oversight, sustaining abuse at scale.

A coordinated solution lies in the development of globally recognized standards for top-level domain (TLD) registries. A shared charter – applicable to both generic (gTLDs) and country-code (ccTLDs) domains – could establish baseline, enforceable requirements. These would include rigorous verification of registrant identities, transparent data-sharing protocols, minimum security obligations for registrars and resellers, and harmonized rules for expedited cross-border takedowns.

Such a framework would not only close enforcement gaps but also reduce jurisdictional inconsistencies, creating a more predictable environment for both legitimate operators and regulators. By elevating safeguarding practices across the domain ecosystem, it would limit the ability of criminal networks to exploit regulatory fragmentation as a safe haven, while reinforcing trust in the global digital infrastructure.

4. Improved Information Sharing

Similarly, disruption of criminal infrastructure depends upon seamless information sharing and coordinated operational responses. Although much is being done across the environment to achieve progress, stakeholder opinion is that this effort has become fragmented. One central initiative, such as a cross-registry anonymized data layer (meta-RDAP), could enable authorized actors to trace abuse patterns across multiple registrars, revealing networks that currently remain opaque. Similarly, formalized public–private intelligence-sharing frameworks would ensure that early warnings regarding malicious domains or URLs are acted upon collectively, rather than in isolated silos.

One illustrative example of such multistakeholder initiatives is the Global Signal Exchange (GSE).[36] The GSE provides a centralized platform for sharing real-time threat intelligence among technology companies, financial institutions, and government agencies, enabling faster detection and disruption of online scams, fraud, and abuse. Its strengths include enhanced collaboration, AI-assisted threat analysis, and a growing, diverse data pool. Limitations include voluntary data sharing that may result in incomplete

[36] "Global Signal Exchange", accessible at: https://www.globalsignalexchange.org/.

coverage, privacy and legal compliance challenges across jurisdictions, and dependence on active participation to maintain effectiveness. Despite these constraints, the GSE exemplifies the type of collaborative frameworks necessary to strengthen global digital security.

5. Proactive Anticipation of Emerging Threats

Looking ahead, defenders must proactively anticipate and adapt to the impact of rapidly evolving technologies that present both opportunities for innovation and potent vectors for exploitation. Blockchain-based domain systems, with their decentralized, immutable, and cryptographically secured nature, offer enhanced resilience and user autonomy. However, the absence of robust governance and dispute resolution mechanisms in this nascent ecosystem creates fertile ground for malicious actors, who can exploit unchangeable registrations and namespace collisions for phishing and fraudulent schemes, largely outside the reach of traditional enforcement. Similarly, AI is profoundly reshaping the threat landscape. While AI tools promise significant advancements in defensive capabilities, such as enhanced anomaly detection and faster identification of abuse patterns, they simultaneously empower criminals to generate highly sophisticated deceptive domains, polymorphic phishing URLs, and dynamic redirect chains at unprecedented speed and scale. AI-driven social engineering, leveraging persuasive language models and deepfake content, further amplifies the challenge by creating highly convincing and adaptive lures. These emerging modalities, alongside potential future threats such as quantum computing, demand a strategic evolution in defensive models. Proactive measures must therefore include substantial investment in AI for advanced threat analytics, the development of governance frameworks for decentralized domain systems, and continuous adaptation of authentication protocols, representing critical forward-looking solutions to protect domain and URL integrity against an ever-mutating threat landscape.

6. Capacity Building for Policy Actors

Strengthening the ecosystem also means equipping those who govern and legislate for it. Many lawmakers and regulators lack comprehensive technical fluency in how domain infrastructure is abused, leading to significant blind spots in policy responses. Therefore, tailored training programmes for policymakers and judicial authorities are essential. These programmes must ensure a deep understanding of the mechanics of digital trust pathway exploitation, the limitations of current regulatory frameworks, and the ample opportunities for international cooperation. Parallel efforts should focus on embedding advanced training for investigators, Computer Emergency Response Teams (CERTs), and registrars. This approach aims to cultivate a well-informed and operationally precise workforce capable of effectively acting upon policy mandates.

7. Capacity Building for Users

Many of the most damaging exploitation campaigns succeed not because of technical ingenuity but because of social engineering, which convincingly persuades users to click, trust, and engage. Therefore, targeted training to recognize manipulated URLs, malicious redirects, and deceptive trust cues is a crucial first line of defence. When this user awareness is paired with advanced detection systems, strong legal frameworks, and a globally harmonised Top-Level Domain (TLD) Charter, a security-aware user base and policymaking community collectively become active barriers against the exploitation of digital trust pathways.

FINAL REFLECTIONS

The preceding analysis underscores a critical truth: digital trust pathways are the foundational layer upon which the integrity of the digital ecosystem rests. The pervasive manipulation of this infrastructure – from maliciously registered domains and strategically abused subdomains to dynamically generated URLs and stealthy traffic redirection – reveals that organized criminal actors are no longer relying on isolated incidents but are instead leveraging a deep understanding of human psychology to orchestrate large-scale, persistent, and evasive campaigns.

The consequences of this exploitation are profound, extending far beyond technical breaches to enable a spectrum of criminal outcomes, from identity theft and multifaceted fraud to ransomware deployment, child sexual abuse material distribution, human trafficking, violent extremist propaganda and intellectual property crime. These are traditional crimes amplified and anonymized by the digital medium, transforming trust pathways into vectors for exploitation.

Addressing this complex challenge demands a departure from fragmented responses. It necessitates a coordinated, multistakeholder strategy that integrates technical innovation, robust legal frameworks, and global collaboration. Strengthening standards, fostering seamless information sharing, and building capacity among policy actors and users are not optional but imperative. As emerging technologies like blockchain domains and AI continue to reshape the threat landscape, the need for anticipatory governance and proactive defence becomes even more critical.

Ultimately, safeguarding the digital ecosystem requires recognizing that digital trust pathways are not peripheral artefacts. Their exploitation is a core element of cybercrime and protecting them is a shared international responsibility, fundamental to preserving digital trust and ensuring an open, safe and secure Internet for all.