Glossary of Terms

Abbreviations

Abbreviation	Meaning	Remarks
AAA	Ask an Analyst	A feature allowing you to get in touch with the Skurio intelligence analyst team.
API	Application Programming Interface	An interface that defines interactions between multiple applications.
APK	Android Package	The file format used by the Android Operating System for mobile apps.
BA	BreachAlert	The application by Skurio that lets you monitor open-source information for a wide range of risks and threats to your business.
BEC	Business Email Compromise	A type of attack which uses email fraud to attack an organisation, resulting with a negative impact on the target organisation.
BIN	Bank identification number	The first 4 to 6 digits on the long number of a payment card. These numbers identify the financial institution that issues the card. See also, IIN.
CTI	Cyber threat intelligence	The process of collecting, processing and analysing data to understand a threat actor's tactics, techniques and procedures within the cyber realm.
DLP	Data Loss Prevention	Technology that performs content inspection and contextual analysis of data passing over a network, as well as data at rest, and tries to prevent the leakage of sensitive information.
DOS	Denial of Service	An attack whereby a service, such as a website, is rendered inaccessible due to a flood of requests. Typically mitigated against by the implementation of network load balancers.
DDOS	Distributed Denial of Service	Similar to a DOS, but more versatile. A DDOS attack utilises multiple computers so that load balancers can't detect the flood due to the differing IP addresses in use. The users of the computers used to perform this type of attach are often unaware that their machines are being utilised; these machines are called *Zombies*, or *BotNets* and may consist of thousands of computers.
DRP	Digital Risk Protection	The primary objective of Skurio's platform, DRP can be broadly defined as the combination of intelligence, detection and response, utilised together to mitigate attacks across the external threat landscape.
DNS	Domain Name Service	The networking protocol that connects URLs with IP addresses. DNS is effectively a directory whereby plaintext domain names (e.g. https://skurio.com/) are referenced against their

		corresponding IP address. Without the DNS protocol searching the web would be similar to using a telephone directory, and users would be required to memorise specific numbers.
GDPR	General Data Protection Regulation	A regulation under EU law whose aim is to give individuals control over their personal data. The law applies to all businesses that operate within the EU, even if they are not based there.
HIBP	Have I Been Pwned?	A website whereby users can check to see if their personal data has been listed in any known data breaches.
HTTP	Hypertext Transfer Protocol	An application layer protocol that is used to delivery websites to end users. It translates HTML data and displays the output within a web browser.
HTTPS	Hypertext Transfer Protocol Secure	An encrypted version of HTTP, whereby a 'tunnel' is created between the web server and the client offering end-to-end data encryption.
ICMP	Internet Control Message Protocol	A basic networking protocol typically used to send time-to-live requests, ping requests, or error messages across a network.
IIN	Issuer Identification Number	Can be used interchangeably with BIN. Dependent upon the region a payment card provider sits in IIN may be referred to. See BIN.
IOC	Indicator of Compromise	In computing, an IOC refers to any piece of forensic data that identifies malicious activity on a system or a network. For example, a partially redacted password or hash-string appearing on a dumpsite would indicate that a breach has occurred, albeit not all data has been released.
IRC	Internet Relay Chat	An application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. Whilst outdated, this form of communication is popular among amateur hackers/hacktivists.
ITSM	Information Technology Service Management	Aset of policies, processes and procedures for managing the implementation, improvement and support of customer-oriented IT services.
MFA	Multi-factor Authentication	A method of signing into an application using multiple unique identifiers in order to prove authenticity. This method circumvents the threat of a single identifying piece of information being used to fraudulently log into a system. MFA must include 2 of the following: something you are, something you have, something you know, somewhere you are, something you are, something you do.
MITM	Man-in-the-Middle	A type of attack whereby an adversary taps into a communication and 'listens' to traffic. Types of MITM attack include ARP poisoning, DNS poisoning and Relay Attacks.

NAC	Network Access Control	A network security solution that enforces a Group Policy on endpoints. A set of rules that certain devices are forced to adhere to when communicating across a network or subnets.
NDA	Non-disclosure Agreement	A contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.
OSINT	Open-source Intelligence	The collection, analysis and dissemination of information gathered from publicly available records.
PCI DSS	Payment Card Industry Data Security Standard	An information security standard that applies to any organisation that handles payment card data.
PGP	Pretty Good Privacy	Applied to email traffic, a program that provides cryptographic privacy for data communication.
PHI	Personal Health Information	Any private medical information.
PII	Personally Identifiable Information	Any data that may be used to identify a person. This may include, first name, surname, national insurance number, passport number, email addresses, driving license number and more.
PKI	Public Key Infrastructure	A mechanism whereby digital certificates are shared and public-key encryption is managed.
PPP	Point-to-Point Protocol	A direct link between two routers, without any hosts or any other networking in-between.
PSK	Pre-shared Key	A cryptographic term that refers to a secret key that is shared between two parties ahead of being used for the first time.
RSS	Really Simple Syndication	A web feed that allows both users and applications to access updates to websites in a computer-readable format.
SaaS	Software as a Service	A delivery model whereby applications are provided via the internet, as a service, such as Skurio’s BreachAlert platform.
SAML	Security Assertions Markup Language	A transitive trust mechanism, whereby different platforms can pass authentication of users between one another. Similar to SSO, but utilises different protocols.
SIEM	Security Information and Event Management	An event log that generates security alerts in a single centralized platform.
SLA	Service Level Agreement	An agreement between a service provider and a client, outlining expectations in terms of delivery of goods or services.
SSO	Single Sign-on	An authentication mechanism that allows users to sign in to multiple systems or types of software with a single username and password.
TOR	The Onion Router	The Web Browser used to access sites on the Dark Web, otherwise known as *.onion* domains.
TLD	Top-Level Domain	The highest-level DNS affixation. For example, .com, .ru, .org. net
URL	Universal Resource Locator	Colloquially known as a web address.
VK	VKontakte	A Russian social media platform, mainly used by Russian-speakers, but available in multiple

		languages. Often referred to as the Russian equivalent of Facebook.
VoIP	Voice over Internet Protocol	Also called IP Telephony, a method for making voice communications over the internet.
VPN	Virtual Private Network	The process whereby a private 'tunnelled' network is established via public network. Allows traffic to remain hidden and prevents sniffing.
WAF	Web Application Firewall	A form of firewall that filters, monitors and blocks HTTP traffic to and from a web application.

Terminology

Term	Meaning
Approximate string matching	The technique of finding strings that match a pattern approximately. See also, Fuzzy Matching.
Brandjacking	The act of acquiring or otherwise assuming the online identity of another entity for the purposes of acquiring that person's or business's brand equity.
Carding	The unauthorized use of credit and debit card account information to fraudulently purchase goods and services.
Credential Stuffing	The automated injection of breached username/password pairs in order to fraudulently gain access to user accounts.
Curated Sources	A variety of pages from across the clear and Dark Web that have been added individually by a Skurio Analyst.
Cybersquatting	Registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trade mark belonging to someone else
Dark Web	A hidden collective of internet sites only accessible by a specialized web browser.
Derived Sources	Pastes on bins sites that are not directly searchable.
Domain Name Squatting	See Cybersquatting
Doxxing	The practice of publishing private information about an individual or organisation to allow others to conduct various attacks against them.
Dumpsite	A collection of breached data from multiple online sources.
Fuzzy Matching	A computer-aided translation of a keyword that enables inaccurate search results to be returned. Used to create close-matches to a domain name when performing Typosquatting alerts. See Typosquatting
Onion Browser	A Web Browser that anonymizes your web traffic; for searching the Dark Web.
Pastebin	A Web Application where users may upload and share 'dumps' of text online. Commonly used for application source code sharing, but can also be used to share credentials following data breaches.
Phishing	Any attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a malicious website. Typically sent via email, however, other types of distribution are also common, such as SMS (Smishing), phone calls (Vishing), and targeted (Spear Fishing). The term Whaling is also used when a Phishing attack is focused upon high-profile victims, such as a CEO.
Scraping	Also referred to as 'web scraping;' the process of extracting large quantities of data from a website.
Skimming	Referring to any method whereby payment card information is stolen by way of deception. Methods can include physical devices, such as magstripe readers and RFID scanners, or via various website hacking techniques, such as cross-site scripting or SQL injections.

Typosquatting	An act that targets Internet users who incorrectly type a website address into their web browser or an attempt to mislead users into visiting a domain that they believe to be legitimate. See also, Cybersquatting, Brandjacking, Domain Name Squatting.
Zero-day/0day	Any computer-software vulnerability that is publicly unknown and has no-known patch or mitigation technique available.