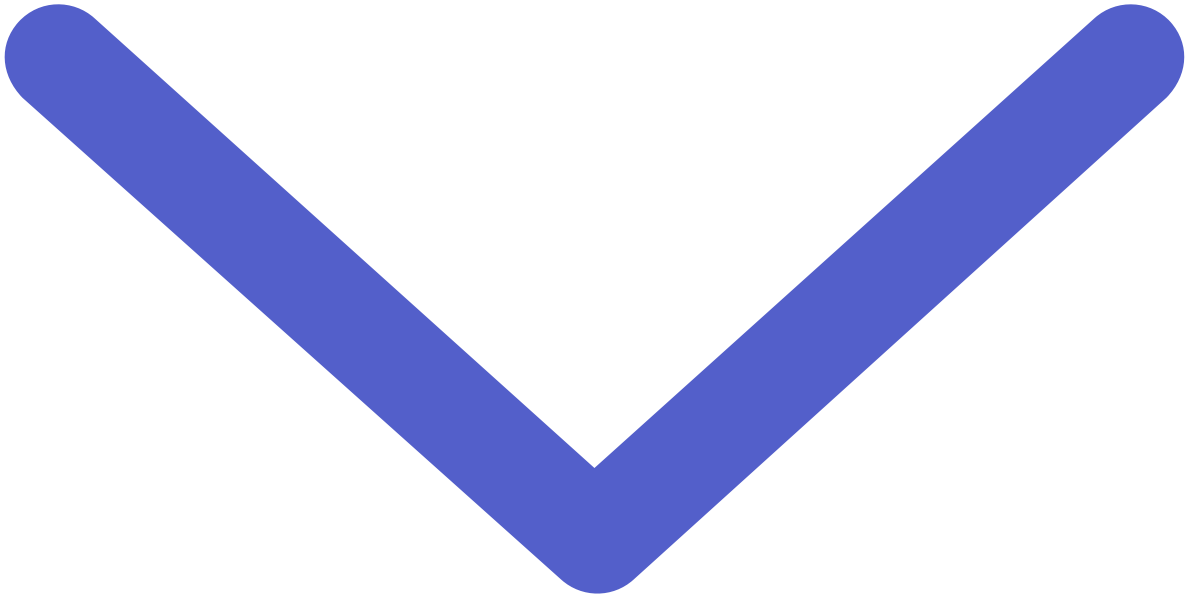
Intelligence 101

a



a

Alphabay

A darknet marketplace, originally launched in September 2014, that has been considered one of the most popular and comprehensive illicit marketplaces to exist. The original AlphaBay was taken down by law enforcement's "Operation Bayonet" in July 2017, and was relaunched by one of its original admins in August 2021. Its most popular offerings include drugs, fraud-related listings like credit cards and fullz, and guides and tutorials for fraud, hacking, and social engineering.

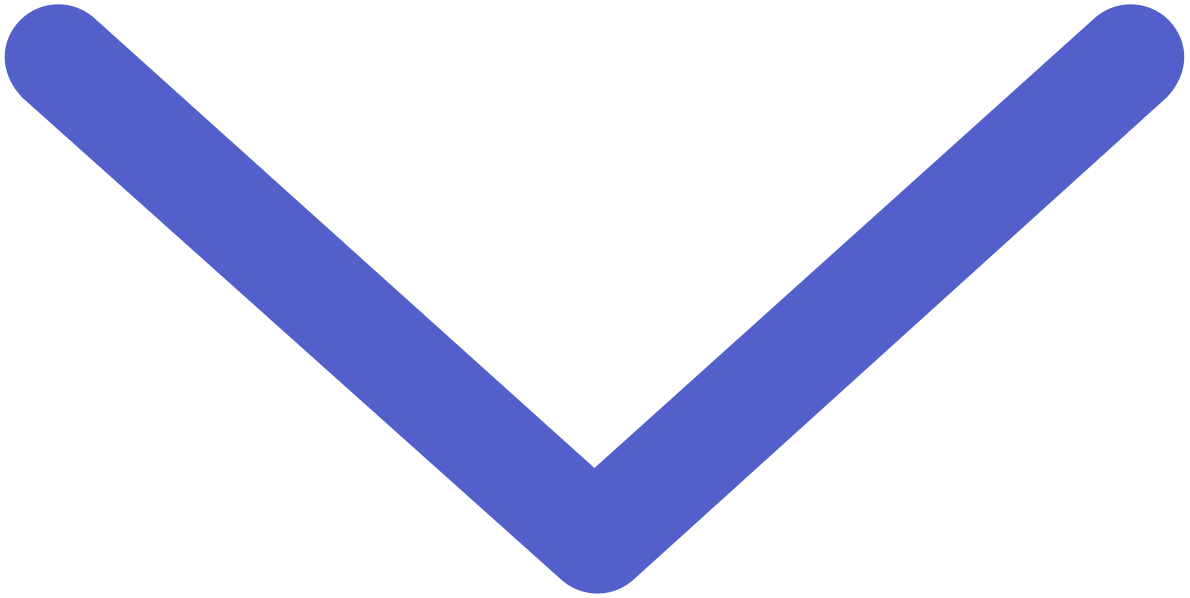
Anonymous

Anonymous is a globally recognized decentralized hacktivist collective, known for its widespread cyberattacks targeting numerous governments, government institutions, government agencies, and corporations. These actions have led to the arrest of numerous individuals involved in Anonymous cyberattacks across various countries, including the United States, the United Kingdom, Australia, the Netherlands, South Africa, Spain, India, and Turkey. Although Anonymous' media presence declined by 2018, the group resurfaced in 2020 to provide support for the George Floyd protests and other social causes. The decentralized structure of Anonymous enables different hackers in private chat rooms to contribute to different operations, while also allowing individuals who align with their mission to adopt the "Anonymous" label, regardless of formal group affiliation.

Attack surface

The attack surface refers to the sum of all the potential points of vulnerability in a system, application, or network that an attacker can exploit. It encompasses both the known and unknown vulnerabilities, including entry points, weak configurations, exposed services, and any other potential avenues for unauthorized access or compromise.

b



b

Bitcoin

A digital currency that uses cryptology to secure transactions and control the creation of additional currencies. Bitcoin is regarded as the first decentralized cryptocurrency and is the most widely used by cybercriminals. Its currency abbreviation is BTC.

Botnet

A network of computers controlled by malware and used for malicious purposes.

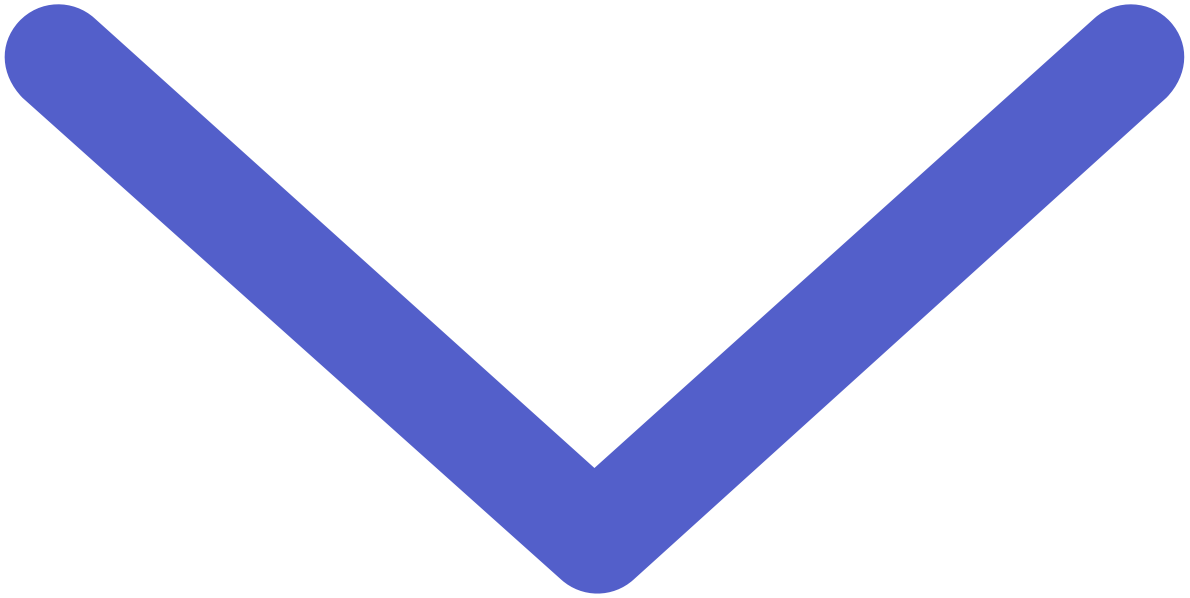
Brand impersonation

Brand impersonation refers to the act of creating fake online identities, websites, or social media accounts that mimic a legitimate brand or organization. The impersonators use these deceptive tactics to deceive and defraud individuals, often to gain access to sensitive information or to scam unsuspecting users.

Business email compromise

BEC—a type of email fraud that usually leads to payment fraud or the obtaining of sensitive corporate information.

c



C

Compromised credentials

Compromised credentials refer to login information (e.g., username and password) that has been illicitly obtained by unauthorized individuals or cyber attackers, potentially leading to unauthorized access and misuse of the associated online accounts or systems. This security breach can result from various methods, such as hacking, phishing, or malware attacks.

Corporate security

Corporate security refers to the strategies, protocols, and measures put in place by organizations to protect their physical assets, personnel, and sensitive information from internal and external threats. It encompasses a range of practices and disciplines aimed at maintaining a secure and safe environment for employees, visitors, and the organization as a whole.

Credential stuffing

Automatically entering a large number of credentials (usually obtained from data breaches) into websites until they are matched to an existing account. Used in account takeover attacks.

Crypting

Crypting is the process of encrypting or obfuscating malicious code to evade detection by security software and analysts.

CVE (Common Vulnerabilities and Exposures)

CVE stands for “Common Vulnerabilities and Exposures.” It is a system used by organizations and researchers to track and discuss publicly known vulnerabilities in various software and hardware products.

CVSS

The Common Vulnerability Scoring System (CVSS) is a standardized framework used to assess and quantify the severity of security vulnerabilities in computer systems or software. CVSS assigns scores based on various metrics to help organizations prioritize and address security risks effectively.

Cyber Threat Intelligence

Often referred to by the acronym CTI, Cyber Threat Intelligence refers to the information, data, and context that’s used to detect, assess, prioritize, and counter cyber threats in order to prevent potential attacks against an organization and reduce risk. Although the terms Cyber Threat intelligence and Threat Intelligence (CTI) are sometimes used interchangeably, they do have distinct nuances: Cyber Threat Intelligence specifically focuses on cyber threats, even those they may overlap with or manifest in the physical work, whereas Threat intelligence encompasses a broad spectrum of risks, including physical, geopolitical, and cyber threats.

Read More →

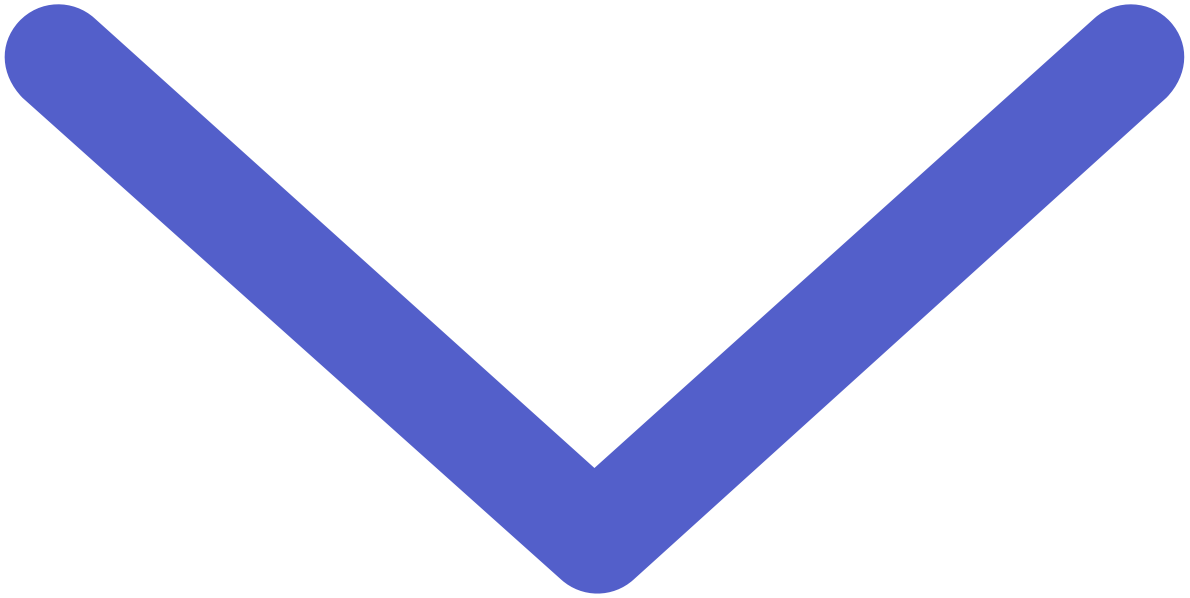
Cyberattack

A cyberattack is a deliberate and malicious act carried out by threat actors to compromise the confidentiality, integrity, or availability of computer systems, networks, or data. Cyberattacks encompass various techniques and tactics, such as exploiting vulnerabilities, ransomware, and DDoS attacks.

Cybersecurity

Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access, breaches, and attacks. It involves implementing measures, processes, and technologies to ensure the confidentiality, integrity, and availability of digital information, safeguarding against potential threats and vulnerabilities in the digital landscape.

d



d

Dark web

The part of the internet that is accessible only through special software, such as Tor, which includes security and obfuscation measures to preserve users' and website operators' anonymity.

Darknet

Also known as the dark web, the darknet is a hidden part of the internet that requires specific software, configurations, or authorization to access. It enables users to operate on encrypted networks, offering anonymity and privacy.

Data leak

A data leak occurs when sensitive or confidential information is unintentionally exposed or disclosed to unauthorized individuals or entities. Although used interchangeably with data breaches, data leaks are specifically limited to insider actions.

Deep web

The part of the internet not indexed by standard search engines, including password-protected or dynamic pages and encrypted networks. These sites are, however, accessible using common web browsers, if the URL and/or login credentials are known.

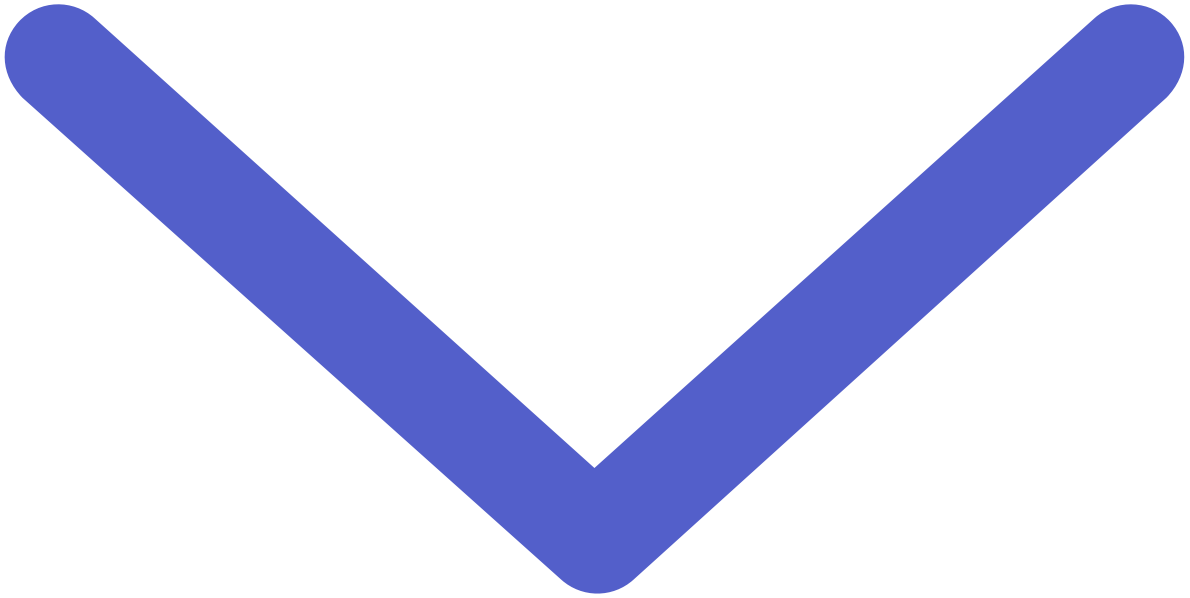
DevSecOps

An approach to software development that integrates security practices into every stage of the software development lifecycle.

Digital risk

Digital risk refers to the potential for negative consequences or harm that can arise from the use, adoption, or reliance on digital technologies and online platforms. This risk encompasses various factors, including cybersecurity threats, data breaches, privacy concerns, reputational damage, financial losses, and legal or regulatory issues associated with digital operations and interactions.

e



e

Eavesdropping

An attack in which a threat actor steals information as it is being transmitted.

Ethereum

A decentralized, programmable blockchain system and community that allows developers to build decentralized applications. Ethereum also has a currency, Ether (ETH).

Executable

A binary file that runs computer functions as designed by the programmer within the context of the operating system. In the context of malware, an executable is the part of the malware that runs the program's malicious functions and components.

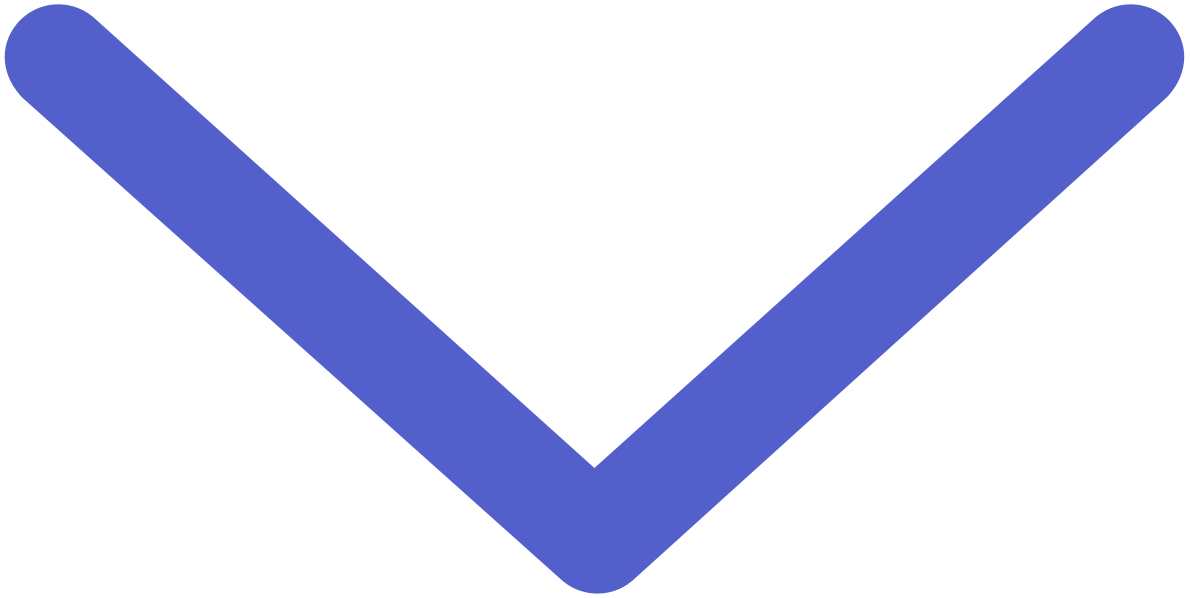
Exploit

A method of leveraging a vulnerability, usually for nefarious purposes.

External threat intelligence

External threat intelligence refers to information and insights about potential cybersecurity attacks and risks that come from sources outside an organization.

f



f

Fetty

A slang term used by threat actors to refer to Fentanyl.

Forum

An online discussion board in which members can exchange knowledge, ideas, or expertise. Many Deep and Dark Web (DDW) forums specialize in topics related to crime or extremist ideologies, which is why they utilize DDW anonymity measures.

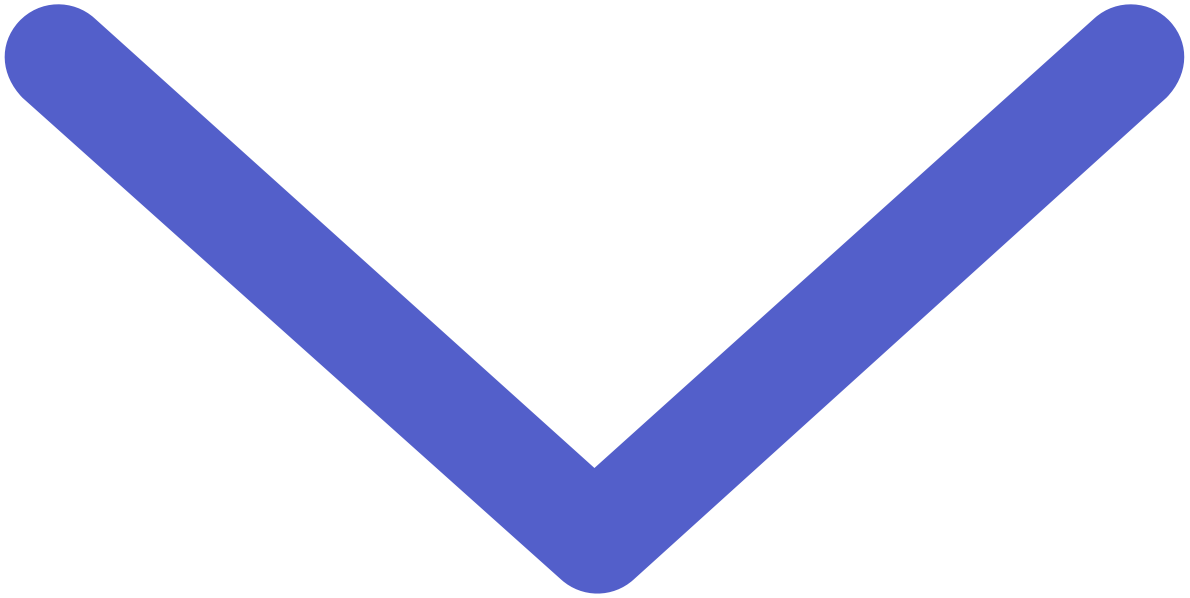
FUD

Fully undetectable, referring to malware that cannot be detected by antivirus software. Or, it can refer to Fear, Uncertainty, and Doubt, referring to the sensationalization of potential new threats.

Fullz

“Full packages” of individuals’ personally identifiable information (PII), such as social security numbers, addresses, or account numbers, sufficient for identity theft. Fullz can be sold to identity thieves to be leveraged in credit card and other fraud operations. The term is often used on Dark Web marketplaces.

h



h

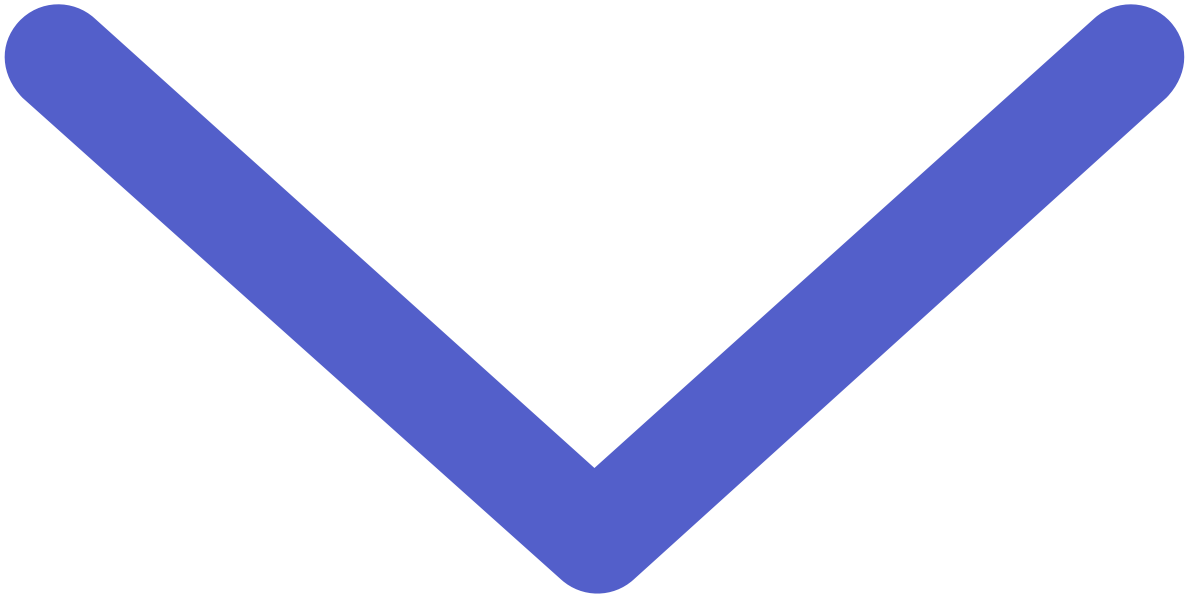
Hacktivism

Hacktivism refers to the use of cyberattacks to promote or advance a particular political or social cause. Hacktivist activities can range from website defacement, DDoS attacks, and data breaches.

High-fidelity intelligence

High-fidelity intelligence refers to detailed and accurate information that is rich in quality and enables a comprehensive understanding of a particular subject or situation. It allows organizations to act quickly and confidently to defend against potential attacks.

i



i

Impersonation

Impersonation refers to the act of creating fake identities or masquerading as a legitimate user, entity, or system to gain unauthorized access to networks, data, or resources to perform malicious activities.

Indicators of compromise

Known pieces of information associated with attacks. Indicators of compromise (IOCs) can include malware artifacts (such as file names and hashes), IP addresses to which the malware connects, and command and control (C2) domains and their resolutions.

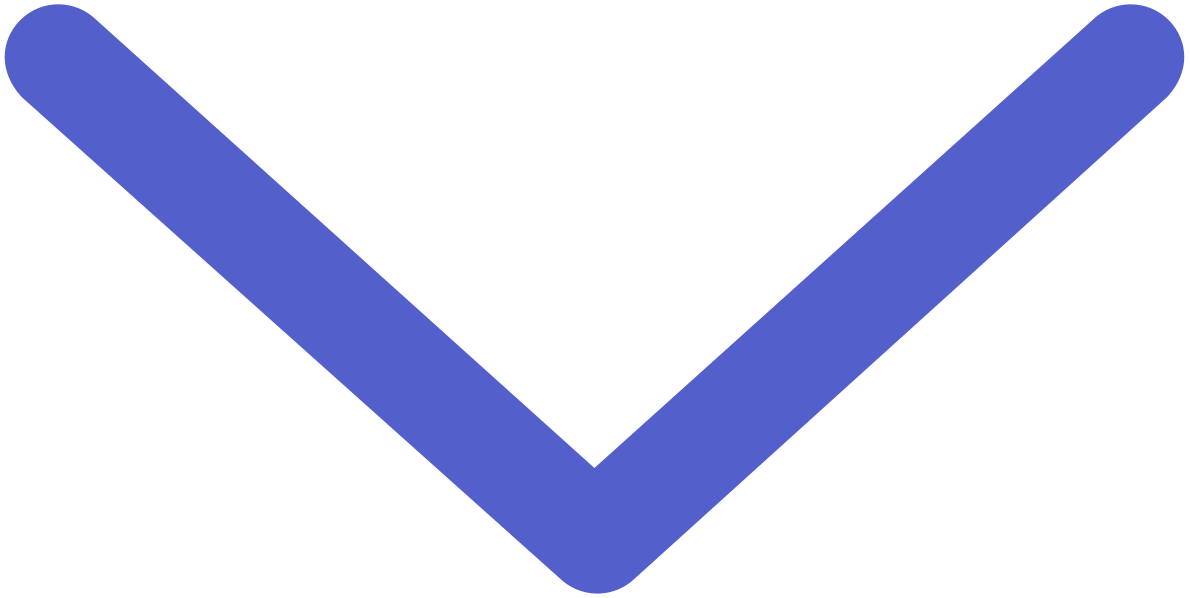
Intelligence

A discipline that uses information collection and analysis tools and techniques to provide guidance and direction to organizations' leaders in their decisions. The sole mission of any intelligence function is to support the decision-maker.

Internet of things

IoT—a network of everyday devices and complex machinery connected to the Internet. The IoT has enabled organizations to automate manual processes, streamline operations, and adapt to regulatory requirements through remote control of an existing network infrastructure.

j

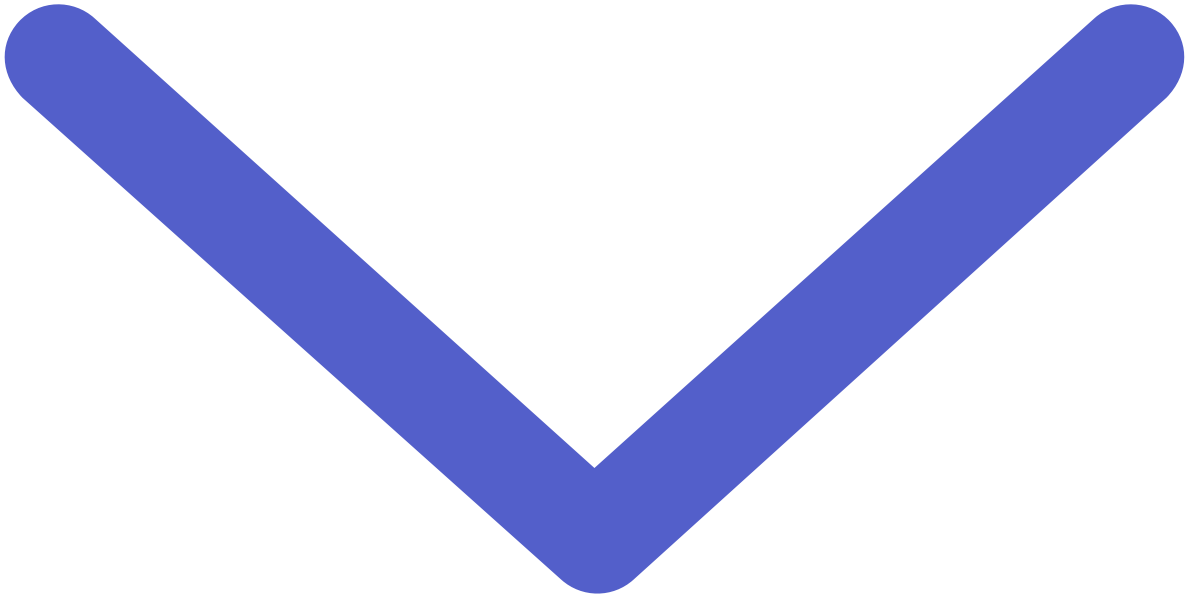


j

Joker’s Stash

First appearing in 2014, Joker’s Stash offered large volumes of uniquely and highly valid cards not available anywhere else online. It was one of the largest illicit payment card shops worldwide until its shutdown in 2021.

k



k

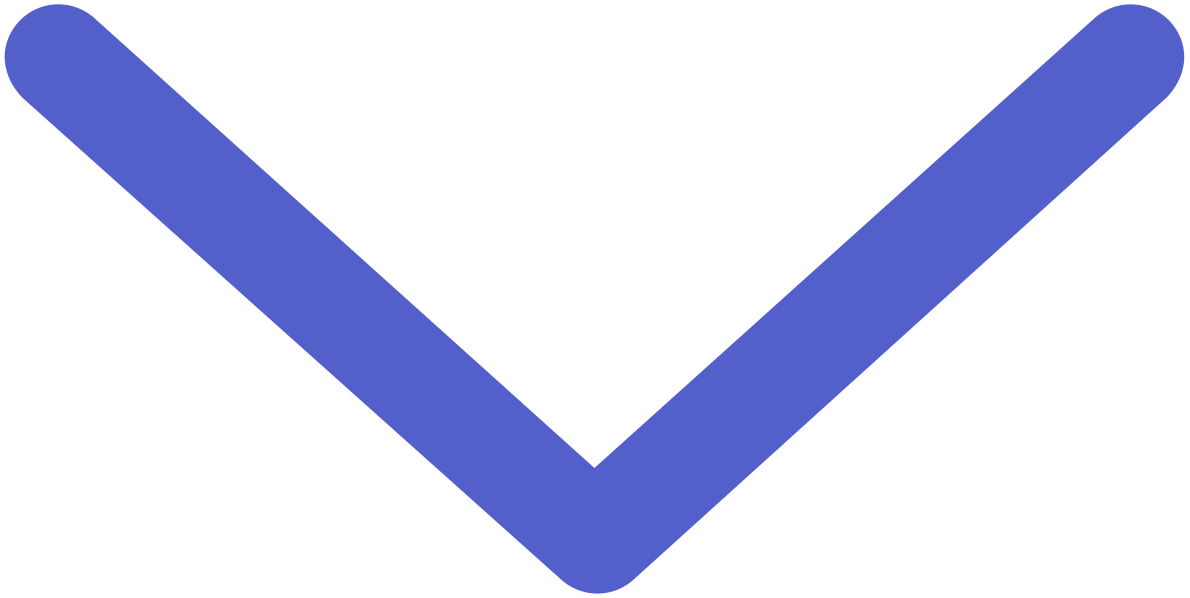
Kernal

The core of the Windows operating system. It provides interactions between hardware and software on Windows. It is always present within the system memory, and is the most crucial part of the operating system. To provide proper access to resources such as processor time, memory space, and external storage such as hard drives, the Windows kernel needs to run at the highest privilege context within the operating system.

Kill switch

A code found in malware that stops the malware's operation if the conditions of the code are satisfied. For example, a malware writer may design a code to prevent their malware from infecting machines in certain countries. When the malware encounters such a machine, the kill switch is activated.

l



l

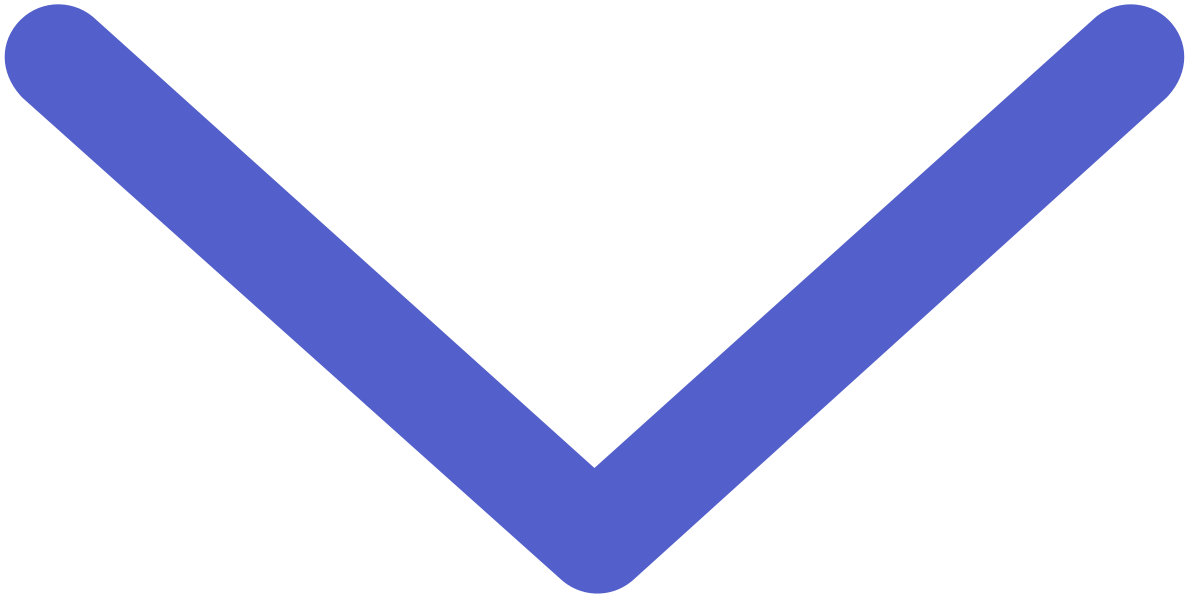
Litecoin

A cryptocurrency that utilizes blockchain technology. It was launched in 2011.

Logs

Login credentials—an umbrella term for any information that can be used to log in to an account. Logs frequently consist of a username and password pair. The term often refers to credentials obtained from botnets, but can also refer to login information obtained from dumps, leaks, or breaches.

m



m

Marketplace

An online forum that allows the exchange of goods or services. Different marketplaces specialize in various products, and many contain contraband and products that facilitate crime and fraud. Law enforcement agencies frequently target illicit marketplaces to track or shut down illegal exchanges.

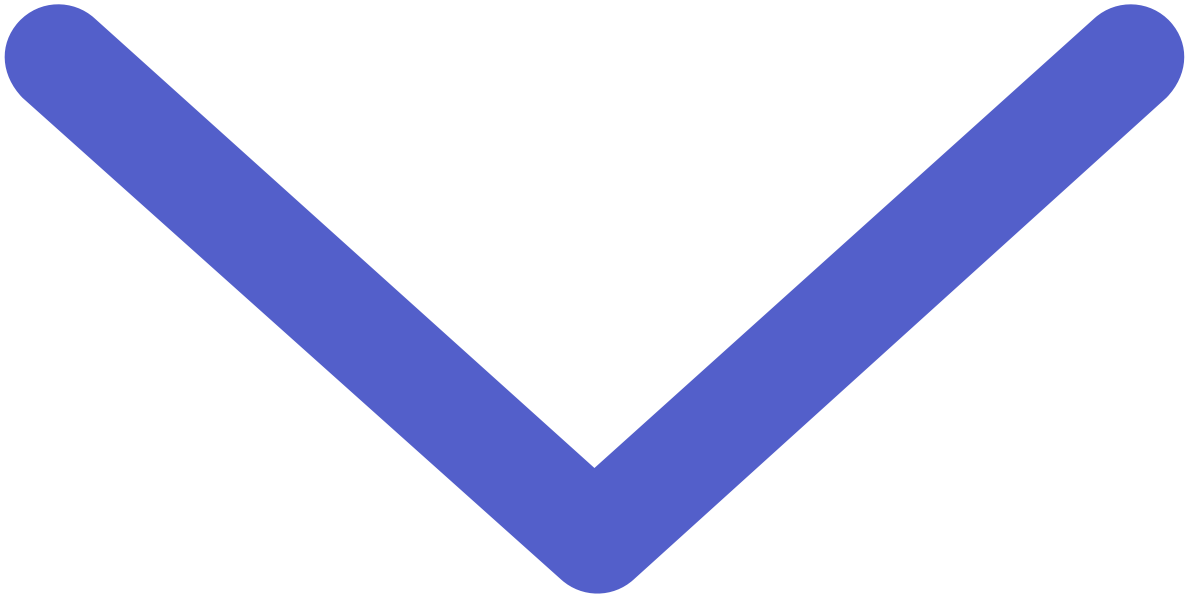
MITRE ATT&CK

A global knowledge base and framework for categorizing threat actor tactics and techniques. MITRE has categorized tactics (such as initial access) and subcategorized techniques (such as drive-by compromise or exploitation of a public-facing application). These techniques are identified by unique IDs.

Monero

A decentralized, privacy-focused cryptocurrency that obscures the identities of both parties involved in any transaction, as well as the transaction amount. Many threat actors in the DDW prefer Monero to other cryptocurrencies due to its privacy features.

n

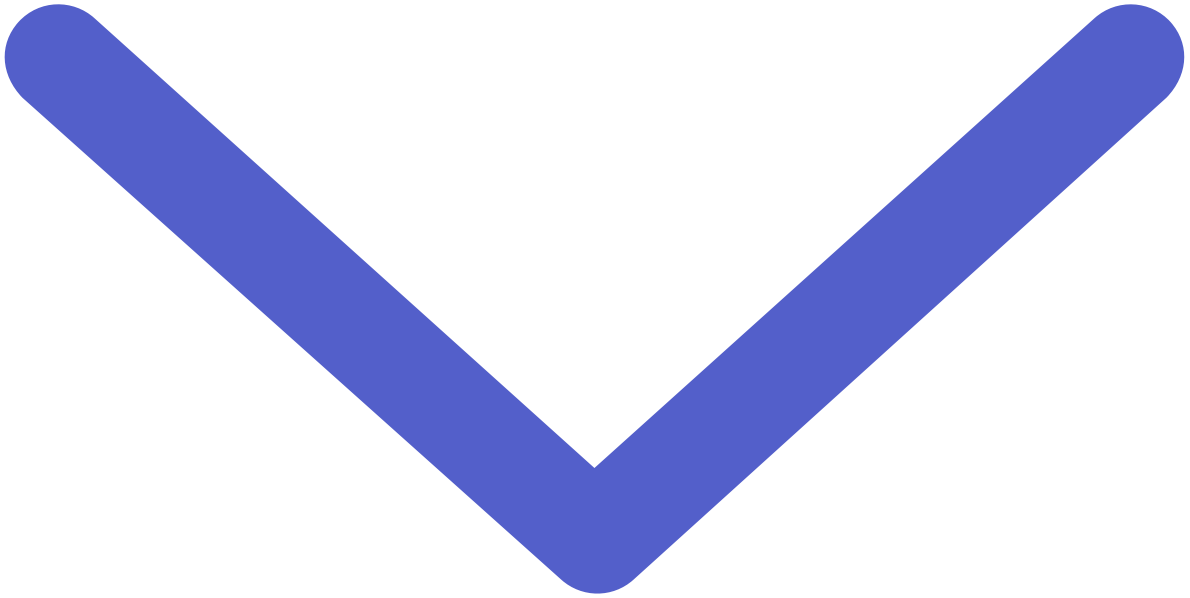


n

Neurolinguistic programming

A psychological manipulation technique that purportedly compels victims to act as directed. Neurolinguistic programming (NLP) was originally developed in the 1970s as a means of self-improvement related to hypnosis, and it has since been widely discredited. However, certain threat actors indicate high confidence in the technique. Fraud communities often refer to NLP as a social engineering method, while conspiracy theorist communities reference NLP as a form of population control.

o

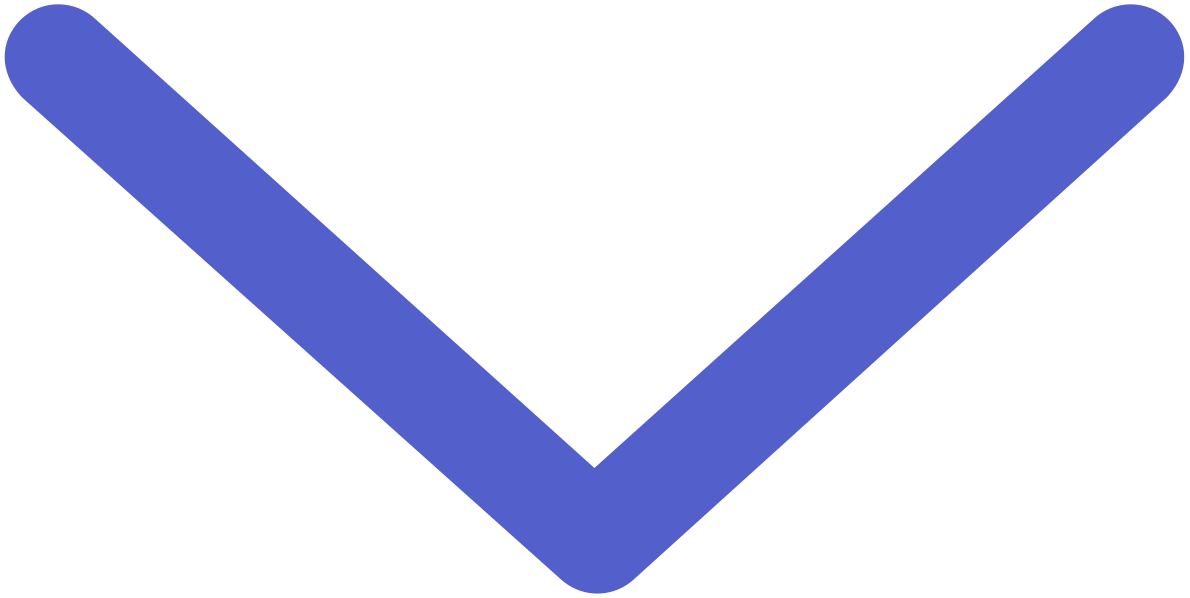


o

Operational security

Opsec—the process of protecting individual data items that could, when aggregrated, form a clearer idea of the identity of the actor(s) behind an alias or operation.

p



p

Pastebin

A website on which users can store information in plain text. It is popular among threat actors due to its ease of use for anonymously sharing information. Pastebin was created in 2002, and posts on the site are known as “pastes.”

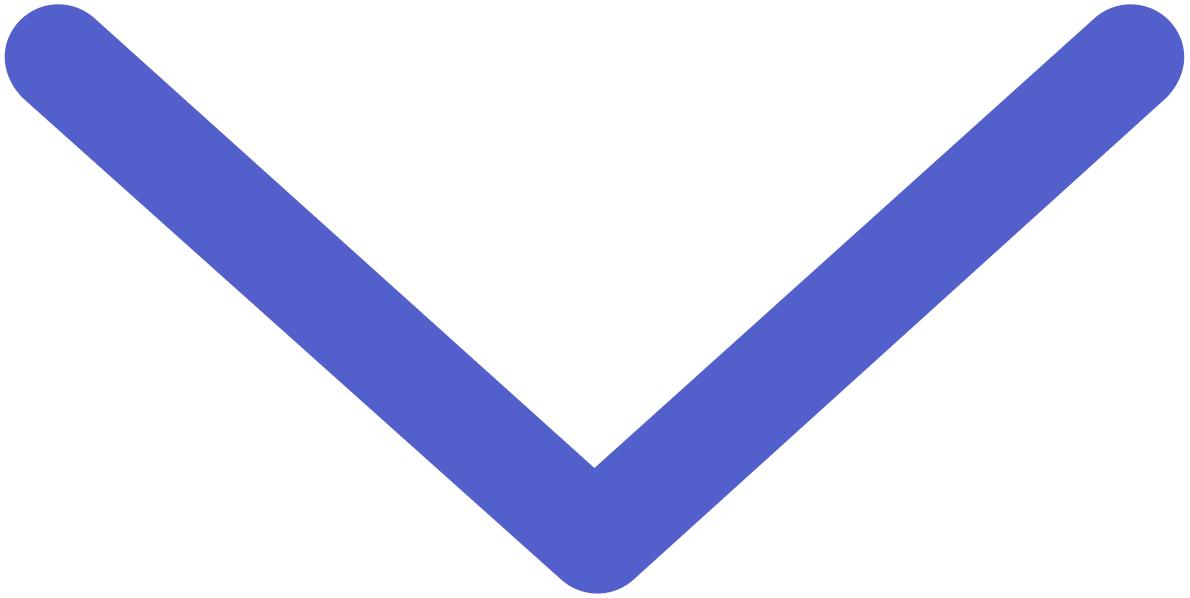
Patch Tuesday

Patch Tuesday is a recurring event that occurs on the second Tuesday of every month, when Microsoft publishes vulnerabilities affecting their software. However, multiple vendors have also copied this approach, resulting in hundreds of vulnerabilities being disclosed on the same day.

Primary Source Collection (PSC)

Primary Source Collection (PSC) is the ability to collect data directly from original sources, driven by an organization’s unique requirements, not a vendor’s fixed feed.

r



r

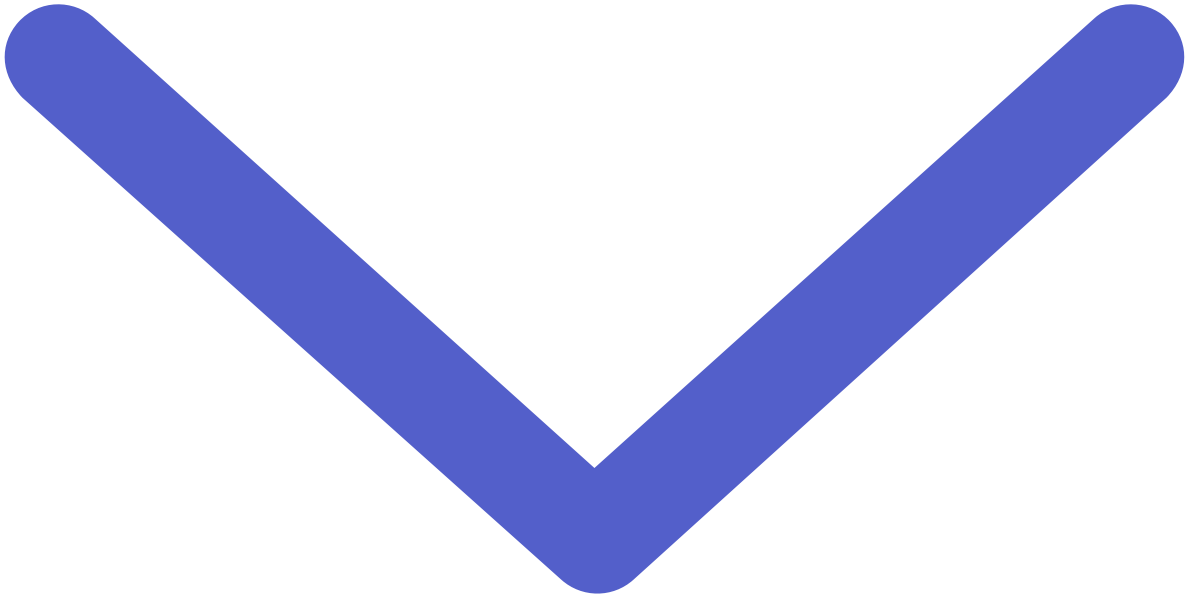
Remote Access Trojan

RAT—a piece of malware that provides a backdoor to establishing administrative control over an infected machine. By establishing administrative control, the malware operator is able to control the infected machine as if they had physical access.

Risk

The forecasting and evaluation of business risks together with the identification of procedures to avoid or minimize their impact.

s



S

Scammer

An individual who defrauds others by offering goods/services or payment for goods/services that they do not intend to follow through on.

SIM swap

The practice of having a phone number switched over to a different SIM card. Methods include social engineering customer service professionals at the carrier or working with an insider. The goal is usually to receive two-factor-authentication codes via SMS to aid in account takeover activities.

Social engineering

Techniques in which a threat actor uses social interactions or tailored content to manipulate a system or individual into improperly granting them permissions or benefits, or divulging protected information. For example, a threat actor may use social engineering to dupe a technology company employee into giving them password recovery information for an account that is not theirs, or they may convince a retail employee to grant them a refund for a delivery the threat actor actually received.

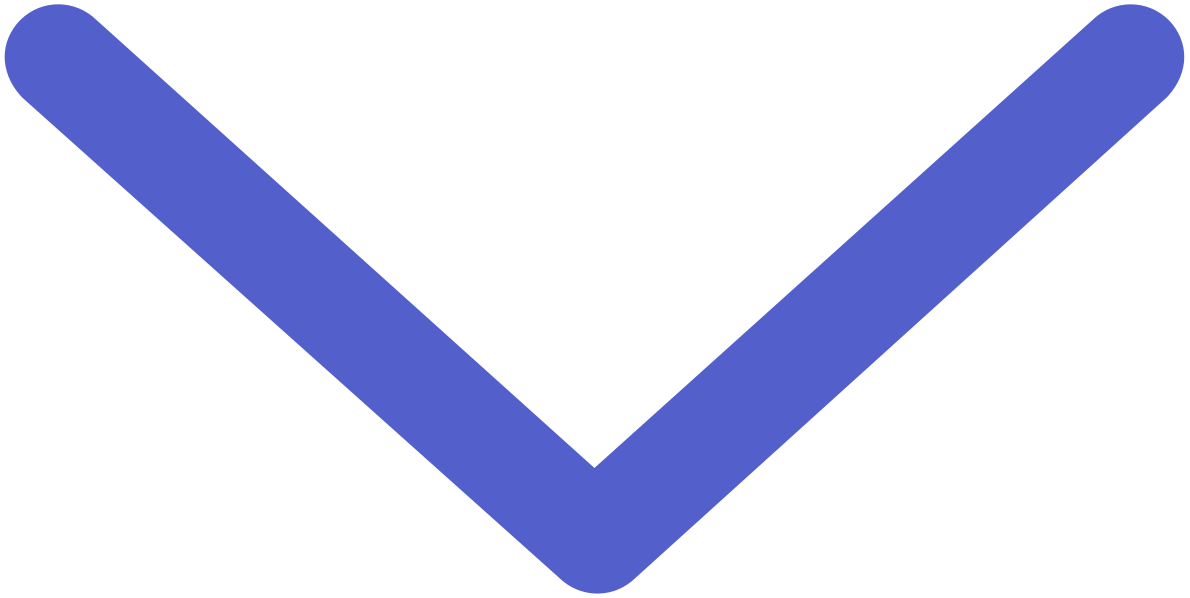
Spoofing

Spoofing refers to the act of falsifying or manipulating data to make it appear as if it comes from a trusted source when it does not. This deceptive technique is often used in various cyber attacks, such as email spoofing, IP address spoofing, or caller ID spoofing, to trick users or systems into believing that the information is legitimate, leading to potential security breaches, phishing attempts, or other malicious activities.

Stealer

A class of malware that steals data from a target user or a compromised system. The stolen data can include system data, user credentials, user files, or other data that the attacker can monetize or use in other attacks.

t



t

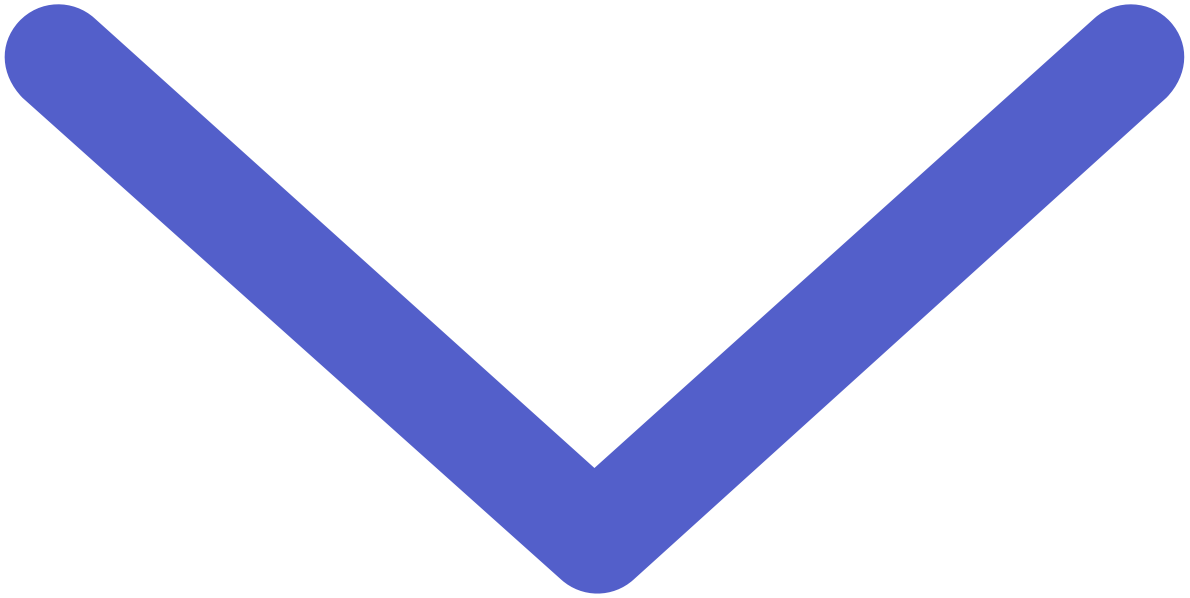
Tor

The Onion Router—a software bundle that enables users to communicate with the internet anonymously. Tor traffics encrypted communications through an overlay network consisting of thousands of relays, or nodes, and bounces information between these multiple relays from the user's computer to the internet and vice versa. Tor thus conceals a user's identity by wrapping traffic in encrypted layers, much like an onion. However, ISPs can tell when a user is using Tor. Tor was first proposed in 1995 by the Office of Naval Research (ONR) and later supported by DARPA in 1997. The Tor Project was founded in September 2004.

Typosquatting

A fraudulent domain that resembles a trusted URL, but with a small typo.

u



u

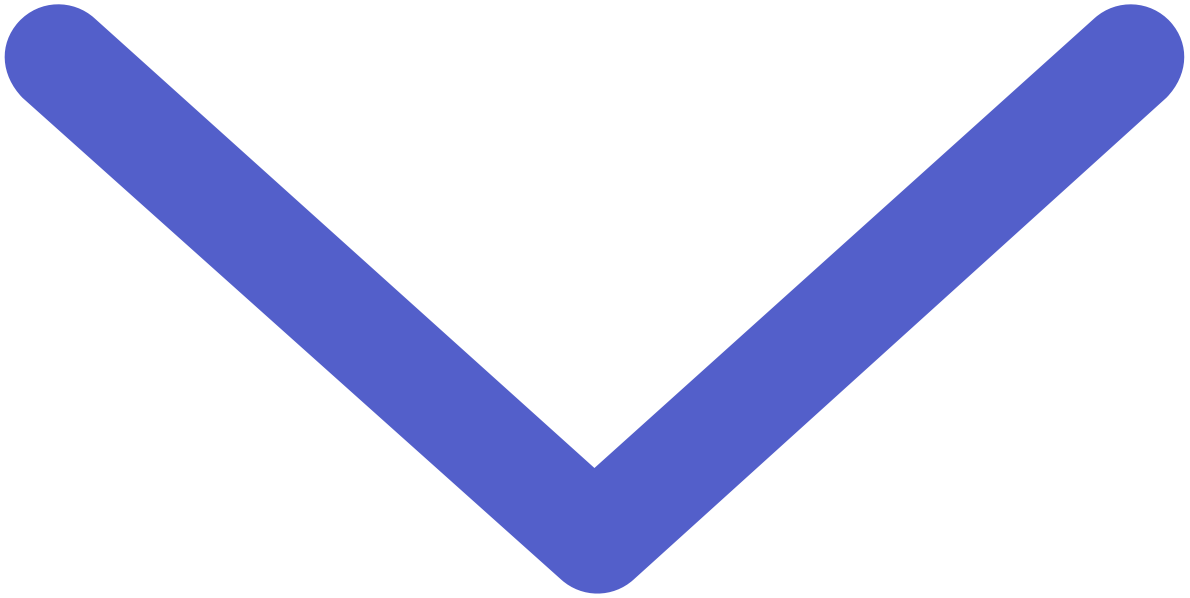
User agent

A software agent that represents or acts on behalf of a user. A user-agent string is information sent by a browser to a web resource to identify itself. The information contains the web browser being used, the operating system running the browser, the device type, and other useful information the web resource uses to identify the browser.

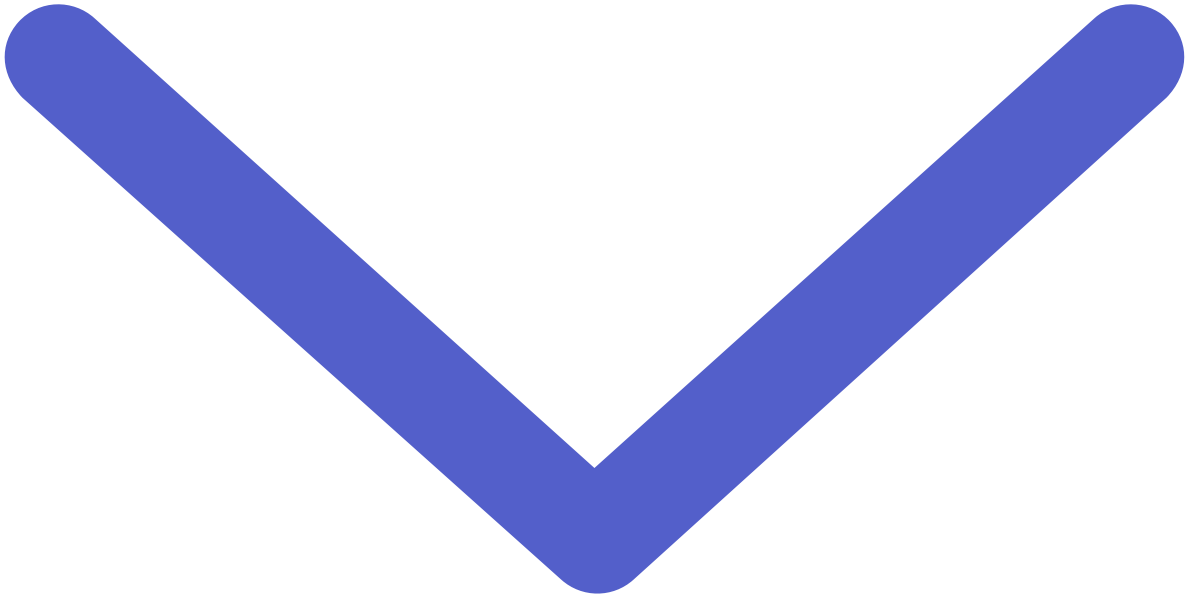
User datagram protocol

UDP—a protocol that provides a procedure for application programs to send messages to other programs with a minimum protocol mechanism. UDP is transaction-oriented, and delivery and duplicate protection are not guaranteed. This is a connectionless protocol that does not verify the source of the transmission.

v



w



W

Watering hole attack

An attack in which a threat actor compromises a specific website to access the confidential information of specific targeted victims. The threat actor generally chooses a site to target based on the victims who are most likely to access it—for example, the actor may target an academic website to compromise the credentials of experts in a given field. In some watering-hole attacks, victims are served malware when they access the compromised website; this malware may be tailored to target a specific IP address.

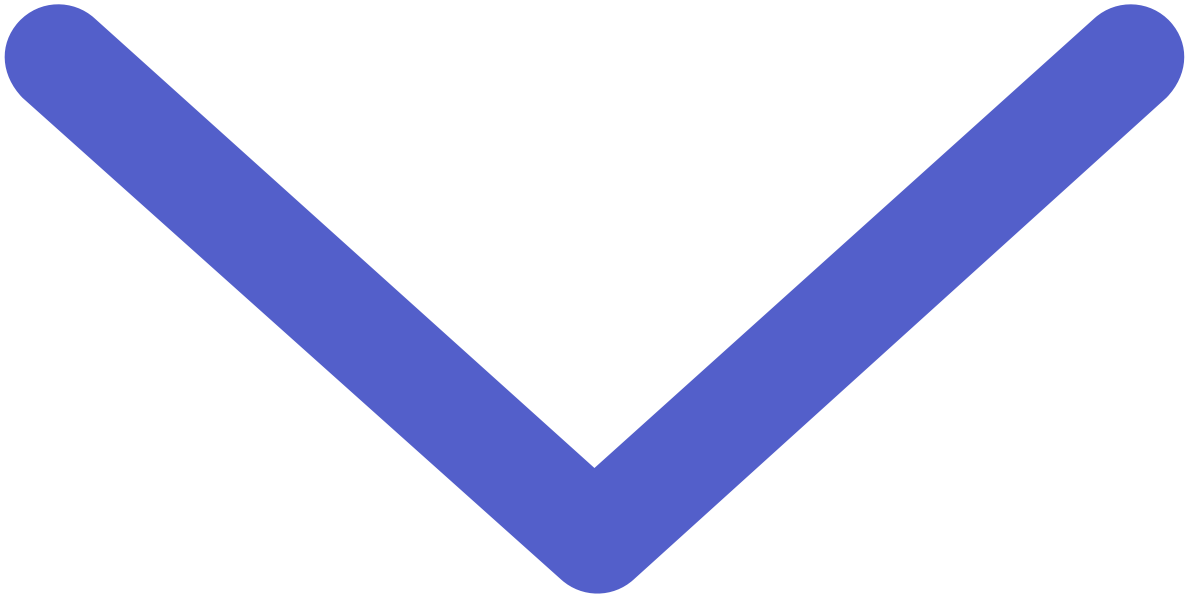
Web shell

A script in a web server that a threat actor uses to maintain persistence in a vulnerable or compromised system. Web shells may be used for other malicious functions by executing attacker input, or used simply as a backdoor. They can be installed on a system by exploiting vulnerabilities. They can be written in any scripting language as long as the web server supports it, though they are commonly written in web development languages such as PHP.

Worm

Malware that self-propagates and continually infects new machines while active on already-infected machines.

y



y

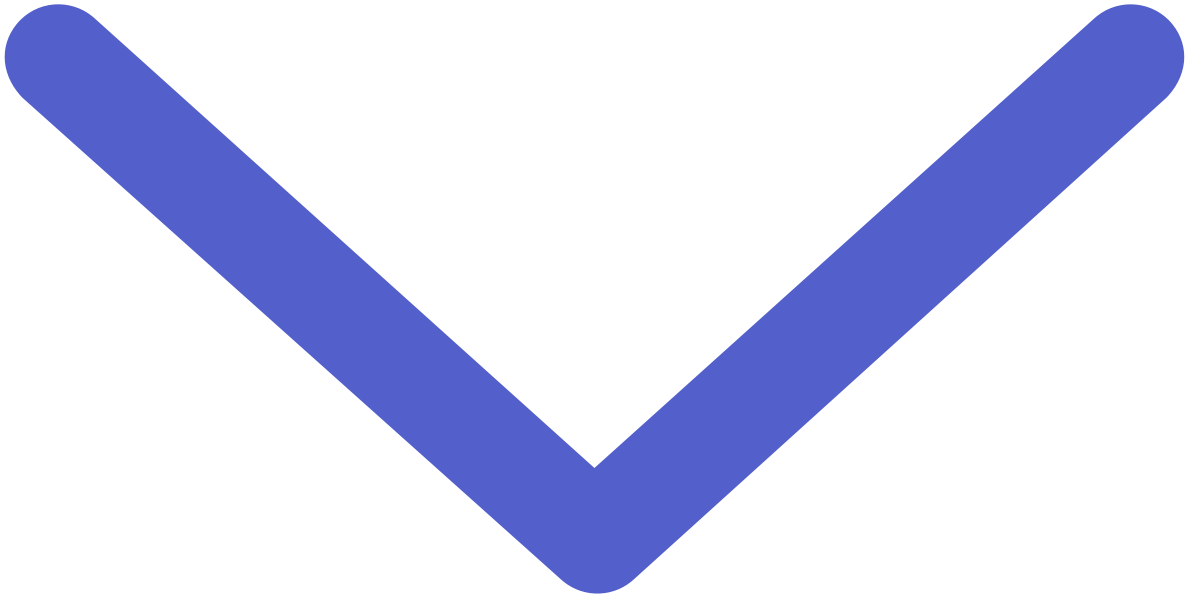
Yahoo Boys

Originally a group of Nigerian fraudsters known for conducting 419 scams; the term expanded to describe Nigerian fraudsters who engage in 419-related fraud schemes. Many Yahoo Boys are known for flaunting extravagant lifestyles.

Yandex

Russian internet services corporation that is best-known for its search engine, which is popular in Russian-speaking countries. The company also offers e-wallets for fund transfers to bank cards, Western Union, or bank accounts.

z



Z

Zero day

A previously unknown or undisclosed vulnerability that can be targeted and exploited. Advanced persistent threat (APT) groups may work to discover or develop them to target entities; cybercriminals who discover them may be able to sell them for hundreds of thousands of dollars.

Zero Trust

Zero Trust is a security framework and approach that assumes no implicit trust for users, devices, or network resources, regardless of their location. It emphasizes the need for continuous authentication, strict access controls, and comprehensive monitoring and logging to enhance security in today’s computing environments.
