THOMSON REUTERS
PRACTICAL LAW™

Cybersecurity jargon buster

by Kelly Hagedorn and Hanna Hewitt, Orrick, Herrington & Sutcliffe (UK) LLP and Virginia Romero and Waithera Junghae, S-RM Intelligence and Risk Consulting Ltd

Status: **Maintained** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-031-1676**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

This note sets out a jargon buster to help you to understand some of the key terms used in the cybersecurity sphere and to explain common types of cybersecurity incidents, attack techniques and forensic terms.

Scope of this note

This note sets out a jargon buster to help you understand some of the key terms used in the cybersecurity sphere and to explain common types of cyber incidents, attack techniques and forensic terms. It may serve as a document to aid lawyers when dealing with cyber incidents and the forensic reports that arise out of them.

Terms are organised in alphabetical order within four categories:

- Day-to-day operations.
- Cyber incidents.
- Attacker techniques and modus operandi.
- Forensic investigation-related terms.

Links to defined terms used within the definition of another term are included for ease of use.

The jargon buster is not exhaustive and is not intended to provide a list of all terms relevant to cybersecurity.

Day-to-day operations

A-D

Active directory

A centralised database that stores information about users, computers, groups and network objects within a Windows domain environment.

Advisory

A document explaining a vulnerability and the risks it presents for customers and users of a product, device or service. Generally, it contains as a minimum:

- A standardised name and unique identifier (such as a common vulnerabilities and exposures (CVE) ID).
- An explanation of:
  - the vulnerability;
  - affected products, including versions;
  - the risks presented;
  - whether remediation is currently available; and
  - if applicable, the remediation offered, for example, patching details.
- A standardised severity rating and discussion of any known or active exploits.
- Revision history or other historical information (for example, when the organisation updates or reissues the advisory).
- A means of authenticating or otherwise verifying the vulnerability report.
- Crediting information or other finder recognition.
- Any references or pointers to further information or contacts.

For more information, see Practice note, Bug bounty and vulnerability disclosure programmes (UK): Advisories and patches.

Antivirus

An umbrella term for software designed to prevent, scan, detect and remove malware from individual computer devices, networks and IT systems.

Asset management

The process of identifying and recording an organisation's IT hardware and software infrastructure including

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

Thomson Reuters™

computers, servers, routers, software applications, data resources and personnel.

Black hat

A malicious actor who hacks or gains unauthorised access to a network to release malware that destroys and/or encrypts files or steal passwords and other personal information.

Bring your own device (BYOD)

A policy that governs whether and how employees may use their personal devices (such as smartphones, computers or removable storage devices) for work purposes. BYOD can reduce employer control and oversight of device protections and settings, potentially increasing the risk of unauthorised access to a computer system or data. For an example of a BYOD policy, see Standard document, Bring your own device to work (BYOD) policy.

Bug bounty

A reward or recognition offered to an individual who identifies and reports a bug, vulnerability or software exploit. For more information, see Practice note, Bug bounty and vulnerability disclosure programmes (UK).

Business continuity planning (BCP)

BCP helps companies to continue operations in the event of business as usual interrupting events, such as a cyber incident. Such plans involve:

- Identifying, analysing and defining various risks.
- Developing mitigation, response and recovery strategies and incorporating these in the organisation's risk management strategy.

For a specimen business continuity agreement, see Standard document, Business continuity agreement (pro-supplier).

Cipher

Cryptographic algorithms used as part of data encryption and data *decryption*. They convert original plaintext to an encrypted text (ciphertext), where arbitrary symbols represent the original text.

Cloud computing

The delivery of computing services (such as servers, storage, software and networking) over the internet. This usually operates on a subscription basis and can reduce organisations' IT expenditure by enabling faster innovation, flexible resources and economies of scale. For more information, see Practice note, Cloud services: overview.

Coding languages

Commands to create instructions for a computer so that it can perform certain tasks. PHP, Python and Java are extensively used examples of such languages.

Cold storage

Storing data that is infrequently accessed on lower-performing and cheaper storage environments. Cold storage also relates to data that is stored securely without a connection to a network.

Common vulnerabilities and exposures (CVE)

A system for referencing and cataloguing publicly disclosed computer security flaws (including as part of an Active directory). Each security vulnerability or exposure is assigned a CVE ID, which can facilitate the tracking and information-sharing of cybersecurity issues to aid the prevention of a cyber-attack.

Component-driven risk management

A category of cybersecurity risk management which focuses on the technical components of a network and information system and the threats they face. Component-driven risk management can be contrasted with system-driven risk management, which analyses the system as a whole. For more information, see Practice note, Cybersecurity risk assessments and reporting (UK): Choosing the most appropriate risk assessment method (or combination).

Computer network defence (CND)

Controls and actions to defend computer networks against unauthorised access and activity, including cyber-attack. CND includes monitoring, detecting, analysing and responding to suspicious activity on the network. Examples include firewall, antivirus and virtual private network (VPN).

Consumer connected devices

Network-connectable devices and their associated services that are made available primarily to consumers.

Content delivery network

A network of distributed servers that work together to deliver content (such as web pages, images, videos) to users based on their geographic location, ensuring faster load times and better performance.

Data at rest

All data in storage that is not being actively used or transferred. It can be considered the opposite of data in transit. An email being sent is an example of data in

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

transit; however, when it arrives in the recipient's inbox, it would become data at rest.

Data integrity

The overall accuracy, completeness and consistency of data during its lifecycle. It is the assurance that data has been protected against unauthorised modification, destruction or loss. Data integrity is a core principle of the EU GDPR and UK GDPR (*Article 5(f)*). For more information on the UK GDPR, see Practice note, Overview of UK GDPR.

Data in transit

A stream of data moving through any kind of network. It can be considered the opposite of data at rest as it represents data which is being transferred, while data at rest is data which is static. An email being sent is an example of data in transit; however, when it arrives in the recipient's inbox, it would become data at rest.

Data loss prevention (DLP)

Measures and technologies that detect and prevent data breaches, data exfiltration or unwanted destruction of data on computer systems. Such measures may include:

- The monitoring and control of endpoints.
- Data stream filtration on corporate networks.
- Monitoring of data transfers to removable devices.
- Monitoring data in the cloud to protect data at rest and data in transit.

Decryption

The process of returning encryption data to its original plaintext form, for which a decryption key is used.

Defence-in-depth

A strategy which protects the confidentiality, integrity and availability of network and information systems and the data within them. It might include defences (such as careful network segmentation, strong access controls and continuous monitoring). It is beneficial to adopt this strategy because it:

- Ensures network security is redundant, preventing any single point of failure.
- Significantly increases the time and complexity required to successfully compromise a network.
- Provides many hurdles a threat actor must overcome. Most cyber-attacks are opportunistic, meaning threat actors take the path of least resistance. Unless a particular organisation is the specific target, attackers will move on to less mature organisations that have not implemented a defence-in-depth strategy.

For more information, see Practice note, Vulnerability management (UK): Glossary.

Demilitarised zone (DMZ)

A publicly exposed subnetwork at the perimeter of an organisation's wider network that contains external-facing services and resources, such as web servers. The primary function of a DMZ is to limit access to an organisation's private network, providing additional protection to those areas of its internal network where its most valuable and critical resources or assets are stored.

Distinct enterprise-connected device (distinct ECD)

Enterprise-connected device (ECD) that is primarily designed for use in an enterprise setting. While it may be available to purchase by a consumer, it usually requires some form of additional infrastructure or has limited use by the public.

Domain (in the context of networking)

An administrative grouping of multiple users, workstations, servers and devices within the same networked architecture. Access to resources within a domain is typically administered under a common security policy.

Domain controller

A domain controller is a server responsible for authenticating users and enforcing policies on a Microsoft Windows domain.

Domain name

The text-based address for a particular location or website on the internet. Examples include google.com or facebook.com. For more information, see Practice note, Domain names explained.

Domain name system (DNS)

The hierarchical system by which an internet domain name is located and translated into a numerical Internet Protocol (IP) address. This allows a user to enter a web address or domain name, which is easier to remember, into their web browser, rather than a numerical IP address. For more information, see Practice note, Domain names explained: Allocation of IP addresses.

Domain trust group

The relationship between domains, which allows authentication traffic to flow between them through a system of referrals. This means that users in one domain can access resources in the other domain using their own credentials without having to log in separately to the other domain.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

E-H

Encryption

The transformation of data from a readable format (plaintext) to an encoded format (ciphertext) using an encryption key.

Endpoints

End-user devices (such as workstations, laptops and mobile phones) but can also include servers, printers, appliances and Internet of things (IoT) devices. Endpoints may also be referred to as, or include, an enterprise-connected device (ECD).

Endpoint detection and response (EDR) solutions

Emerging security systems that detect and investigate suspicious activities on endpoints, employing a high degree of automation to enable security teams to quickly identify and respond to threats.

The primary functions of an EDR security system are to:

- Monitor and collect activity data from end-user devices that could indicate a threat.
- Analyse this data to identify threat patterns.
- Automatically respond to identified threats to remove or contain them and notify security personnel.
- Implement forensics and analysis tools to research identified threats and search for suspicious activities.

Endpoint security

Endpoint security serves to secure endpoints against cybersecurity threats. It is important to secure such endpoints as they tend to be easier to infiltrate and more susceptible to cyber-attack, including since they are not protected within the network's on-site security measures.

Endpoint security ranges from multi-factor authentication (MFA) tools and active directory software to more sophisticated tools, such as Enterprise-connected device (ECD).

Enterprise-connected device (ECD)

An ECD is defined by the National Cyber Security Centre (see Practice note, Cybersecurity in regulated sectors, cybersecurity guidance and standards: National Cyber Security Centre) as any device which interacts with, holds or processes an organisation's data. ECDs can encompass wide categories of device depending on their use and can cross over to multiple device classes, including:

- End-user devices, such as laptops and smartphones. Although these are devices designed for both consumers and organisations, if used in the context outlined above, they are classed as ECDs. If a personal device is also used for work purposes (for example, bring your own device (BYOD)) or is able to interact with organisation data, for example by being able to connect to an enterprise network, it is viewed as an ECD.
- Internet of things (IoT) devices.
- Distinct enterprise-connected device (distinct ECD).

File system

A file system determines where and how data is stored on a hard drive (also responsible for handling deleted data). Used as an index for the operating system to quickly find files.

Firewall

A firewall scans incoming and outgoing network traffic and permits or blocks access or data transfer, depending on a predetermined set of security rules (such as "allow internet access for only one computer in the local network and block access for all others"). It thereby protects the private internal network and prevents unauthorised access from the internet.

Group Policy Object (GPO)

The GPO is an inbuilt administrative mechanism which can be used to automatically push out policy or software changes to all devices across a Microsoft Windows Active Directory domain.

Hashed password

A hashed password is a password that has been transformed into a string of characters using a hash function. This differs from a plaintext password, which is stored exactly as it is entered and can be read without any decryption.

Hashing

A one-way cryptographic function, whereby a mathematical algorithm is used to convert an input of variable length and contents into a fixed length output, typically an alphanumeric string. As a one-way function, it is practically impossible to reverse reliable hashing algorithms to obtain the original input data from any hash. However, various techniques are available to decode some hashes.

Honeypot

A honeypot mimics a legitimate target and is used as a decoy to attract a threat actor. This can help detract from legitimate targets or to gain insights into how threat actors operate.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

Hypervisor

A hypervisor is software that enables the simultaneous operation of multiple virtual servers on a single physical machine.

I-L

Identity and management controls (IAM)

A set of processes, policies and technologies for defining and managing the roles and access rights of users and devices to various resources, including applications, devices or data. This includes, for example, multi-factor authentication (MFA) and single sign-on (SSO) systems.

Incident response plan (IRP)

An internal document that helps an organisation navigate a cyber incident, setting out steps that should be taken by an organisation before, during and after an incident (including any reporting obligations an organisation might be under). For an example of an IRP, see Standard document, Cyber incident response plan (IRP) UK.

Information security policy (ISP)

An ISP sets out the rules, policies and processes for end-users and networks within an organisation to follow to meet the organisation's IT and data protection security requirements. For more information, see Practice note, Information security risk: how to assess the inherent and residual risk in your business: Policies and guidance.

Internet Protocol (IP) address

A unique numerical address that identifies a device on the internet or a local network. For more information, see Practice note, Domain names explained: IP addresses.

Internet of things (IoT) devices

A network of interconnected smart devices, vehicles, buildings and other everyday objects that contain sensors, processors and wireless communication components that enable them to communicate with computers, servers and one another and to collect, use, analyse, store and share data. Devices that connect to the IoT are different from conventional devices because they can be programmed to perform functions and take actions on command, on their own or in conjunction with other connected devices.

Intrusion detection system (IDS)

A tool to monitor networks or computer systems for information security policy (ISP) violations or malicious activity.

Intrusion prevention system (IPS)

An IPS adds preventive functions to an Internet Protocol (IP) address, such as blocking threats discovered by an IDS.

Local area network

A network that connects computers and devices within a limited geographical area.

M-P

Managed security service provider (MSSP)

A third-party IT and network security provider. Common services include the provision of:

- Managed firewalls.
- Internet Protocol (IP) address.
- Intrusion prevention system (IPS).
- Virtual private network (VPN).
- Vulnerability assessment systems (VASs), including continuous monitoring.
- Antivirus software.

Mobile device management (MDM)

A software that allows administrators to control and enforce policies on mobile endpoints, such as work phones and laptops used by employees, to ensure networks are secure. Common MDM features include:

- Device inventory and tracking.
- Remote wiping.
- Password enforcement.
- App whitelisting and blacklisting.
- Data encryption enforcement.

Multi-factor authentication (MFA)

MFA is an authentication method that requires a user to satisfy two or more methods of verification to access a resource, such as an application or online account. Implementing types of MFA are, in some circumstances and sectors, becoming legislative requirements. For example, the revised Payment Services Directive ((EU) 2015/2366) (PSD2) introduced a package of reforms referred to as strong customer authentication (SCA) for authenticating e-commerce card-based payment transactions. SCA requires authentication to use at least two of the following three elements:

- Something the customer knows (for example, a password or PIN).
- Something the customer has (for example, a phone or hardware token).

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

- Something about the customer that is physiologically unique to them (for example, a fingerprint or facial recognition).

The breach of one element does not compromise the reliability of the others. SCA is designed in such a way as to protect the confidentiality of the authentication data. For more information, see Sector note, Strong customer authentication under PSD2.

Patching

The process followed to update software to remediate a known software vulnerability. Some software packages, especially consumer-oriented products, provide automated update features that regularly receive and install patches with little or no user intervention. For more information, see Practice note, Bug bounty and vulnerability disclosure programmes (UK): Advisories and patches.

Penetration testing (pen testing)

A simulated cyber-attack against a computer system to identify security weaknesses, vulnerabilities and areas where an organisation's cybersecurity could be improved. For more information, see Practice note, Cybersecurity risk assessments and reporting (UK): Penetration tests.

Proxy server

A router that acts as an intermediary between end-users and the internet. The proxy server creates its own Internet Protocol (IP) address and therefore the end-user's IP address remains hidden, making it more difficult to trace and enhancing anonymity online. In addition, proxy servers also improve security and privacy of the user, protect networks from malware and can grant access to restricted content.

Q-T

Remote Desktop Protocol

A proprietary protocol developed by Microsoft that allows users to remotely access and control a computer over a network connection.

Responsible disclosure policy

A policy that provides individuals with clear guidelines for reporting a security vulnerability to an organisation. For more information, see Practice note, Bug bounty and vulnerability disclosure programmes (UK). For a specimen vulnerability disclosure process, see Standard document, Cyber vulnerability handling process (VHP) (UK).

Salting

Salting involves attaching a string of random data to an input before it is hashed (see hashing). Salts are typically used to further secure hashed passwords against being decoded.

Sandbox

An isolated testing environment on a network that mimics end-user operating environments. This enables users to run suspicious programs or open files without risking harm to the device or network.

Secure Sockets Layer (SSL)

A type of encryption method for the internet to ensure privacy, authentication and data integrity in internet communication. Websites that display "HTTPS" in the URL deploy SSL for security.

Security by design

An approach to software and hardware development that seeks to make systems as free from any vulnerability and as resistant to attack as possible through multiple measures which may include careful network segmentation, strong access controls, continuous monitoring, authentication safeguards such as multi-factor authentication (MFA) and adherence to best programming practices.

Security perimeter

A security perimeter is a physical or logical boundary for a particular computer system or network, within which a particular security policy or security architecture can be applied.

Single sign-on (SSO)

An authentication mechanism that enables users to securely authenticate and access multiple resources or applications with a single set of credentials. For example, with SSO in place, an authenticated SSO account may automatically have access to all linked applications, systems, data sets and environments the authenticated user is provisioned for.

Software as a Service (SaaS)

A cloud computing-based software licencing and distribution model where a cloud provider hosts software applications and makes them available to users over the internet. The cloud provider is fully responsible for managing and maintaining the software. For more information, see Practice note, Cloud services: overview.

System-driven risk management

A category of cybersecurity risk management which analyses a system as a whole (which in this context refers to something which aims to achieve a specified function; this function could be achieved by

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

technology, but equally a system could be a group of people, a building or a naturally occurring pattern of weather). It can be contrasted with component-driven risk management, which tends to focus on the individual components of a system. System-driven risk management can be useful when analysing large and complex systems. In particular, it can help an organisation to explore interaction failures. These occur when individual components within the system are working precisely as they should, but there is some flaw in the way in which these components interact with one another which makes it possible for a security breach to occur. For more information, see Practice note, Cybersecurity risk assessments and reporting (UK): Choosing the most appropriate risk assessment method (or combination).

Tabletop

A simulated cyber incident against an organisation's computer system carried out with key personnel of an organisation. The purpose of a tabletop is to put an organisation's incident response plan (IRP) to the test and to identify any areas of an organisation's incident response plan that could be improved.

Threat actor

An individual, organisation or other actor that presents a cybersecurity threat. This may include:

- Negligent or malicious employees who create internal threats.
- Nation state actors, hackers or criminals who create external threats.

Token

A short piece of code which allows the performance of an operation, for example, an access token relates to access control operations.

U-Z

Virtual local area network (VLAN)

A network segmentation technique that enables the creation of multiple logically separate networks within a single physical network infrastructure. VLANs are commonly used to enhance network security, improve performance, and simplify network management by dividing a large network into smaller, isolated segments.

Virtual private network (VPN)

A VPN creates a secure, encrypted connection to the internet, providing a private tunnel for data while using public networks.

Whitelisting

A mechanism which allows certain identified entities, users or programs to access a particular service or privilege, or perform a particular function.

White hat

A white hat, otherwise known as an ethical hacker, is an individual permitted to hack a system to identify a security vulnerability and make recommendations for improvement.

Cyber incidents

A-M

Bot

In the context of computing, a bot (robot) refers to software that performs automated tasks, usually in a manner that impersonates a human. Malicious bots perform automated tasks that enable a threat actor to take control of devices.

Botnet

A botnet (robot network) is a network of compromised computing devices, which are under the control of a remote threat actor. Botnets can be used to launch various co-ordinated attacks, such as a distributed denial of service (DDoS) attack.

Big game hunting

A type of cyber-attack that leverages malware to target large, high-value organisations or high-profile entities.

Brute force attack

A method of systematically cycling through numerous passwords until the correct one is found, giving a threat actor access to a user account or network.

Bug

A colloquial reference to any unexpected problem experienced by software or hardware.

Card skimming

A generic term for the use of an illegal device to collect information from a credit or debit card. A related term is "digital skimming" in which a threat actor steals payment card data from existing input fields in online payment forms or trick users by sending them to fake checkout pages.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

Clickjacking

The process where an individual is tricked into clicking on one object on a web page when they want to click on another.

Credential stuffing

Credential stuffing attacks involve using large databases of stolen usernames and passwords (obtained from data breaches) to automatically log in to online accounts, exploiting the fact that many users reuse passwords across multiple accounts.

Cryptojacking

The unauthorised use of computing devices (computers, smartphones, tablets or even servers) by cybercriminals to mine for cryptocurrency. The motive for cryptojacking is profit and it is intended to remain completely hidden from the victim.

Cyber-attack

A malicious, unauthorised or criminal act in relation to a computer network or system. The intention of such an act is to disable, disrupt, destroy or control computer systems, or to manipulate or steal data held in these systems.

Cyber incident

The breach of a system's security policy that affects its integrity or availability, or unauthorised access or attempted access to a system or systems. This can be the result of a cyber-attack but it can also refer to other accidental or unintended activities by individuals with detrimental consequences.

Deepfake

Deepfake is a type of synthetic media generated through deep learning techniques intended to manipulate, alter or create fake images, videos, audio recordings and texts. Threat actors have been known to use deepfake technology to facilitate various types of cybercrime.

Dictionary attack

A type of brute force attack in which a threat actor runs through a set of commonly used words and phrases to guess passwords.

Distributed denial of service (DDoS) attack

A DDoS attack seeks to disrupt the normal delivery of a service (for example, access to a website, server or network) by overwhelming the target with internet traffic to prevent it from working properly. Botnets are often used to stage DDoS attacks.

Domain name squatting

The act of registering, trafficking in or using a domain name with bad faith to profit from the goodwill of a trade mark belonging to someone else. Also known as domain name piracy or cybersquatting. For more information, see Practice note, Domain names: disputes.

Doxing / Doxxing

Where an unauthorised third-party shares personally identifiable information about an individual, usually online, without consent.

Drive-by download attack

A drive-by download attack involves the unintentional download of malicious programs to a network or device without the user's consent. This can either be authorised without knowing the full implications or unauthorised with no notification of the download.

Leakware

Ransomware that is deployed to a machine, which displays a message threatening to distribute sensitive information (whether personal data or confidential information) and requesting payment to prevent the "leak" of sensitive information online.

Malicious loader

A malicious loader is a program or script designed to download or install additional malware. In some cases, further malicious software can be stored within the loader, rather than downloaded from another external source, to avoid detection.

Malware

Malicious software designed to perform unauthorised processes that steal data or compromise, damage or disrupt a computer system or network (or both). Examples include a virus, worm, ransomware and trojan horse (Trojan).

Man-in-the-middle attack (MitM)

In an MitM attack, a threat actor positions themselves between a user and the destination of the user's communications, allowing the threat actor to intercept the user's communication before it reaches its destination.

N-Z

Open redirect

An open redirect is a vulnerability in a website that allows manipulation of the URL and redirects users to

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

another site. This vulnerability is exploited by threat actors in phishing attacks to conceal the destination of a link.

Phishing

Phishing involves tricking a user through social engineering to reveal personal or confidential information, which can be used illicitly. Most often this is an email sent by a threat actor impersonating a legitimate source.

Phishing-as-a-service (PhaaS)

Refers to a service where criminals offer phishing tools, resources, and infrastructure as a paid service to other malicious actors.

Ransomware

A type of malware designed to perform encryption and prevent access to a computer system or the data stored on it. A threat actor typically demands a sum of money or a ransom in exchange for a *decryption* key that a victim can use to regain access, see Practice note, Cyber threats: ransomware (UK).

Ransomware as a service (RaaS)

Ransomware that is hosted, deployed and otherwise managed (including collecting payment from and organisation and if relevant, restoring access to data) by a threat actor.

Remote access trojan (RAT)

A RAT is a form of trojan horse (Trojan) that provides a threat actor with remote access to a device or network.

Scareware

A type of malware deployed to a machine that claims to have detected a virus. The malware often pushes through multiple pop-up screens to flood a user's device, prompting a user for payment, or locks a user's device.

Social engineering

A manipulation technique to exploit human error, to gain access to personal or sensitive data.

Spam

Unsolicited communications (such as emails, text messages or internet postings) that are typically sent to a large number of recipients or posted across various locations on the internet. These can be harmless (such as advertising) or malicious (such as phishing emails).

Spear phishing

A more targeted type of phishing that is addressed to a specific person or group in an organisation.

Spoofing

Spoofing involves tricking a user into believing that communication is from a trusted source. There are different types of spoofing including call ID spoofing, and IP address spoofing that a threat actor will use to trick its intended target.

Spyware

A type of malware that allows access and insight into a user's activities and transmits this information back to a threat actor without the user's knowledge or consent.

Structured Query Language (SQL) injection

An SQL injection exploits an input validation vulnerability in SQL-based applications (such as websites) by introducing malicious codes in SQL statements (standard query language used to perform tasks such as updating data on a database or retrieving data from a database). A threat actor can use this to manipulate a vulnerable SQL database to gain unauthorised access to sensitive data that is not typically expected to be accessible. SQL injection attacks are used to retrieve, manipulate, and/or delete content in SQL databases.

Supply chain attack

Where a threat actor exploits vulnerabilities or weaknesses in third-party entities to gain unauthorised access to the target organisation's systems, data, or infrastructure.

Trojan horse (Trojan)

A type of malware that appears legitimate but has a hidden and malicious function that often evades security mechanisms.

Virus

A type of malware that can replicate itself and infect computers without the permission or knowledge of the user.

Watering hole attacks

When a threat actor compromises a website frequented by a specific group of users, such as employees of a particular organisation, to distribute malware and infect systems.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

Whaling

A phishing attack targeted at senior or high-profile personnel of an organisation.

Worm

A type of malware that can replicate itself and spread across a computer network without external intervention.

Zero-day attack

An attack that exploits a potentially serious software security vulnerability that the vendor or developer may be unaware of, or has recently discovered.

Zero-day vulnerability

A vulnerability that is only learnt about after an attacker has already exploited it, so that victims, law enforcement or other incident responders retrospectively identify the vulnerability as the attack's cause.

Attacker techniques and modus operandi

A-M

Credential access

Credential access is conducted by a threat actor after they have gained initial access to a system to steal credentials such as account names and passwords.

Collection

Collection refers to the techniques a threat actor uses to gather information on the target system before data exfiltration.

Command and control

A technique used by a threat actor to interact with and send commands to a system that has been compromised by malware. This will often be done in a way that mimics legitimate network traffic to avoid detection.

Data exfiltration

The unauthorised copying, transfer or retrieval of data from a computer or server. This can be conducted manually through physical access to a computer or via programs over a network.

Defence evasion

Defence evasion occurs when a threat actor takes actions to avoid detection once in the network such as uninstalling or disabling security software or deleting event logs.

Discovery

Discovery occurs when a threat actor takes actions after initial access to learn more about the target system and its broader environment.

Encryption

Typically occurs in ransomware attacks, when an attacker deliberately alters data from a readable format to an encoded format using an encryption key, to prevent a victim from accessing their information.

Double extortion ransomware

A type of cyber-attack where a threat actor firstly exfiltrates an organisation's data, before encrypting the data on the organisation's systems. This technique is often used by a threat actor as leverage to encourage an organisation to pay a ransom.

Execution

Execution occurs when a threat actor takes action to run a malware payload such as ransomware to encrypt files on a target system.

Extortion

Extortion in ransomware cases refers to the act of demanding payment from victims in exchange for restoring access to their encrypted data or systems.

Horizontal privilege escalation

In horizonal privilege escalation, a threat actor gains access to additional accounts with similar privileges to their existing access which broaden the threat actor's access across the compromised systems or networks.

Lateral movement

Lateral movement is conducted by a threat actor after they have gained initial access to a system through an entry point and then move onto other portions of the network.

Multi-extortion ransomware / Multifaceted extortion

A type of cyber-attack where a threat actor uses two or more attack methods to encourage an organisation to pay a ransom. This could include exfiltrating files, encrypting files, distributed denial of service (DDoS) attacks or extending ransom demands to third-parties (often clients, suppliers and so on of the organisation).

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

N-Z

Privilege escalation

Privilege escalation occurs when a user or threat actor takes actions to increase their permissions, privileges, rights or access on a computer or network. Escalating privileges allows a threat actor to perform functions they would not have been able to perform with their initial access.

There are two types of privilege escalation: horizontal privilege escalation and vertical privilege escalation.

Rootkit

A type of malware used by a threat actor to gain access to and control of a remote computer or network.

Vertical privilege escalation

Instances where a threat actor obtains access to additional accounts with higher privileges than their existing access. This often allows them to access more sensitive data and perform certain tasks that require increased privileges.

Web shell

A malicious script that enables a threat actor to compromise devices exposed to the internet and launch additional attacks. After gaining initial entry, threat actors use a web shell for remote administration and lateral movement.

Forensic investigation-related terms

A-M

Advanced persistent threat (APT)

A sophisticated threat actor that gains unauthorised access to a system or network and remains undetected in that system for an extended period.

Artefact

A piece of data that may or may not be relevant to an investigation into a cyber incident. Examples include registry keys and files.

Attack surface

The number of all possible points or attack vectors where an unauthorised user or threat actor can access a system and commit data exfiltration .

Authentication bypass vulnerabilities

A form of vulnerability which allows a threat actor to avoid authentication requirements and gain access to accounts or networks.

Computer Emergency Response Team (CERT)

A group of information security experts responsible for protection against, detection of and response to an organisation's cyber incident.

Continuous monitoring

Continuous monitoring programs deploy software, such as vulnerability assessment systems (VASs) to perform vulnerability monitoring on a continuous basis to:

- Monitor security controls.
- Identify a vulnerability.
- Verify hardware and software configurations.
- Flag suspicious activities.

The tools that support continuous monitoring automatically correlate and present results to IT and other technical operations staff for further action. Some continuous monitoring tools include automated update features to close gaps (such as blocking suspicious network traffic), software patching or changing configurations.

Data carving

An analytical process that attempts to extract fragmented or deleted data from storage devices, file systems, or disk images by searching for file signatures, headers, footers, and other patterns to recover deleted files or remnants of data.

Data mining

An analytical process that attempts to find correlations or patterns in large data sets. For more information, see Practice note, Legal aspects of managing data: Text and data mining.

Digital forensics

A subdivision of forensic science that focuses on the identification, recovery and analysis of digital material on electronic devices that can be used in a court of law.

Disk imaging

The process of creating a forensic copy or image of a storage device to preserve the original data and facilitate analysis without altering or damaging the original evidence.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2024. All Rights Reserved.

Exploit

A program or piece of code that finds and takes advantage of a security flaw or vulnerability in an application or computer system.

Indicators of compromise (IOCs)

Forensic evidence of potential intrusions on a network or device. Examples include unknown files, applications and processes on a network.

File hashing

The process of generating a unique digital fingerprint or hash value for a file using cryptographic algorithms (such as MD5, SHA-1, or SHA-256) to verify its integrity and authenticity.

Log analysis

An examination of system logs, event logs and other records generated by systems and network devices.

Memory forensics

A process of analysing volatile memory (RAM) to extract and analyse artefacts such as running processes or open network connections.

Malware analysis

The process of analysing malware to understand its behaviour, functionality, propagation methods, and impact on systems in order to develop countermeasures, detect infections, and attribute attacks to a specific threat actor.

N-Z

Network forensics

The investigation and analysis of network traffic, protocols, logs, and devices (such as routers, switches, and firewalls) to identify security incidents, intrusions, unauthorised access, and data exfiltration.

Payload

The component of a cyber-attack that causes harm to the victim.

Public key infrastructure (PKI)

A system for digital signatures and public-key encryption. It is designed to secure the transfer of information over insecure networks.

Remote code vulnerabilities

A form of vulnerability that allows a threat actor to remotely execute commands on a vulnerable device.

Vulnerability

A weakness or flaw in a software, system or process that an attacker may seek to exploit. Based on the nature of the vulnerability, these can be subdivided into various categories, such as authentication bypass vulnerabilities and remote code vulnerabilities.

Vulnerability assessment systems (VASs)

(Also known as vulnerability scanners.) Commercial and open source tools which provide off-the-shelf Vulnerability assessment systems (VASs) capabilities for organisations, including continuous monitoring. For example, vulnerability scans can identify:

- Outdated software or missed patching.
- Insecure hardware or software configurations or settings.
- Unexpected or unnecessary files or services.

Vulnerability management programmes

Vulnerability management programmes:

- Define a formal process for:
  - timely identification of any applicable vulnerability;
  - closing the security gaps that vulnerabilities create by remediating or at least mitigating their effects; and
  - tracking and documenting an organisation's efforts.
- Prioritise often limited IT and other resources. Organisations must focus on vulnerabilities according to their level of risk, particularly considering the sheer volume of changes that diligent vulnerability management can demand.
- Continuously monitor and evaluate an organisation's IT and other environments to ensure compliance and avoid reintroduction of known vulnerabilities.
- Minimise Cyber-attack risks by decreasing the organisation's attack surface.

A vulnerability management programme can be differentiated from patching because applying patches is only one means of managing some vulnerabilities.

Vulnerability monitoring

The process whereby, typically, automated tools (such as Vulnerability assessment systems (VASs)) are used to determine whether particular computers or other IT or operational technology assets are subject to any known vulnerability, especially those that a threat actor can easily exploit.

Legal solutions from Thomson Reuters

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. For more information, visit www.thomsonreuters.com

Thomson Reuters™