ISBN 978-0-660-45950-9
CAT D96-9/2022E-PDF

CANADIAN CENTRE FOR
CYBER SECURITY

An Introduction to the **Cyber Threat** Environment

2023
2024

Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada

Communications Security Establishment
1929 Ogilvie Road
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISBN 978-0-660-45952-3
CAT D96-9/2022

About this document

This document describes common concepts relevant to discussions about cyber threat activity in the Canadian context and acts as a point of reference for Canadian Centre for Cyber Security (Cyber Centre) publications. This introductory document provides baseline knowledge about the cyber threat environment, including cyber threat actors and their motivations, sophistication, techniques, tools, and the cyber threat surface.

Please see the Cyber Centre Glossary[1] for additional terminology and the Cyber Centre guidance page[2] for more discussions on the cyber threat environment.

[1] https://cyber.gc.ca/en/glossary

[2] https://cyber.gc.ca/en/guidance/

Cyber threat

A **cyber threat** is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains, or to disrupt digital life in general.

The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity. It includes the networks, devices, and processes that are connected to the Internet and can be targeted by cyber threat actors, as well as the methods threat actors use to target those systems.

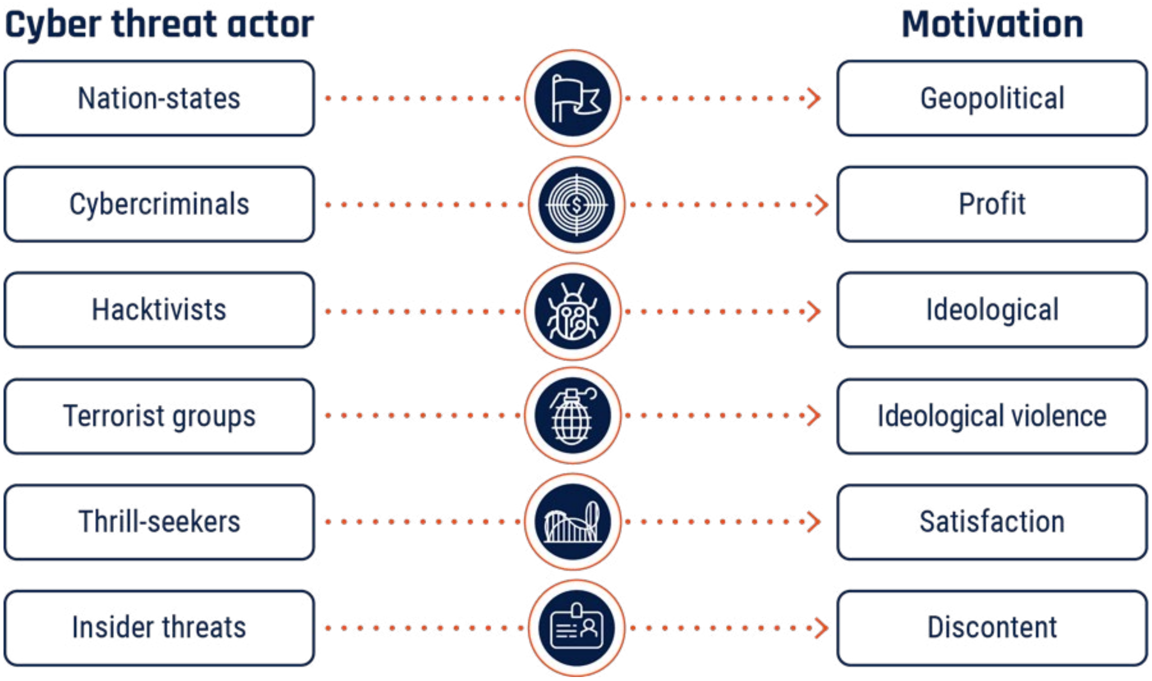
Cyber threat actors

Cyber threat actors are groups or individuals who, with malicious intent, aim to exploit weaknesses in an information system or exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks, including the authenticity of the information that flows to and from them. The globalized nature of the Internet allows threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.

Types of cyber threat actors and their motivations

Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices and networks for different reasons, such as siphoning processing power, exfiltrating or manipulating information, degrading the network's performance and extorting the owner. Some threat actors conduct threat activity against specific individuals or organizations, while others opportunistically target vulnerable systems. In general, each category of cyber threat actor has a primary motivation.

Figure 1: Cyber threat actors



Sophistication

Cyber threat actors are not equal in terms of capability and sophistication. They have a range of resources, training, and support for their activities. Cyber threat actors may operate on their own or as part of a larger organization (i.e., a nation-state intelligence program or organized crime group). Sometimes, sophisticated actors use readily available tools and techniques because they can still be effective for a given task and/or make it difficult for defenders to attribute the activity—for example, by leveraging the commercial security tools used by security researchers.

Advanced persistent threats (APT) refer to threat actors in the top tier of sophistication and skill. APTs are capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their goals. This designator is usually reserved for nation-states or very proficient organized crime groups.

State-sponsored cyber threat actors operating on behalf of nation-states primarily use cyber threat activity to advance their geopolitical objectives. They are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination. Nation-states without developed cyber programs can use commercial cyber tools and the growing global pool of talent to enable sophisticated cyber threat activity. Some nation-states also have operational relationships with private sector entities and organized criminals.

The activities of state-sponsored cyber threat actors may include espionage against governments, organizations, and individuals; prepositioning on or disrupting critical systems; influencing and shaping public discourse; or building networks of compromised devices to enable further cyber threat activity. State-sponsored cyber threat actors may also pursue financially motivated threat activity.

Cybercriminals are primarily financially motivated and vary widely in sophistication. Organized crime groups often have planning and support functions in addition to specialized technical capabilities that can affect a large number of victims. Illegal online markets for cyber tools and services have made cybercrime more accessible and allowed cybercriminals to conduct more complex and sophisticated campaigns.

Hacktivists carry out ideologically motivated cyber threat activity and are generally lower sophistication than state-sponsored cyber threat actors or organized cybercriminals. These actors, alongside terrorist groups and thrill-seekers, often rely on widely available tools that require little technical skill to deploy. Their actions often have no lasting effect on their targets beyond reputation, however, at times these actors have been able to inflict physical and financial damages on their targets.

Insider threats are individuals working within their organization who are particularly dangerous because of their access to internal networks that are protected by security perimeters. Insider threats are often disgruntled employees, and may be associated with any of the other listed types of threat actors.

COMMERCIAL CYBER TOOLS

Commercial cyber providers sell tools and services that allow clients to deliver malware, intercept communications, and steal information from target devices. Commercial cyber tools are often advertised as being for law enforcement, but not all providers discriminate in who they sell to. Cyber threat actors may leverage commercial cyber tools to increase the sophistication of their threat activity.

Cyber threat surface

The **cyber threat surface** refers to all information systems and services a cyber threat actor may exploit in trying to compromise an individual, organization, or network. It includes all Internet-exposed endpoints, including networks, personal computers, mobile devices, Internet of Things (IoT) devices, and servers, in addition to processes that communicate with or rely on information systems connected to the Internet. Individual threat surface is also informed by the amount of personal information shared with online vendors and services; the broader an individual shares their personal and financial details, the more vulnerable their information becomes to theft or exposure via a data breach. The larger the cyber threat surface of an individual, organization, or network, the more difficult it is to secure.

The number of endpoints connected to the Internet increases significantly every year, driven by increased deployment of IoT and industrial IoT (IIoT) devices.[3] Connected consumer and medical devices such as home security systems, cars, and pacemakers are becoming more common, as is connected operational technology (OT), the hardware and software integrated into devices used to monitor and cause changes in the physical world.

Services, devices, and data can all be targeted by cyber threat actors to gain initial access into an environment. Supply chains increasingly include digital information transfer in addition to the movement of physical goods. Since 2020, more organizations have adopted technologies such as cloud-based software, infrastructure, and platform "as-a-service" products to increase their efficiency in a hybrid work environment, with some employees working from home and others on site. Managed service arrangements often include elevated access for suppliers into their clients' networks. The trust and information flow between organizations provides threat actors an indirect means of compromising their intended targets by first compromising a third-party.

Figure 2: Endpoints

An endpoint is any device connected to a network, including personal computers, mobile devices, IoT devices, servers, and more.

[3] https://www.statista.com/topics/2637/internet-of-things/#dossierKeyfigures

Cyber threat targets, impacts, and activities

The targets of cyber threat activity

Cyber threat actors conduct malicious activity against anything connected to or residing on the Internet, including devices, information, financial resources, opinions, and reputations:

- **Devices** include connected technology such as personal cell phones or computers, servers, and the operational technology that controls industrial processes. Once compromised, devices can be used to facilitate further cyber threat activity.
- **Information** includes intellectual property, other sensitive business information, and personal information. This could also include valuable financial information such as banking details or logins.
- **Financial resources** include assets such as fiat currency and digital assets, including cryptocurrency. Cyber threat actors often target Canadian individuals with fraud and scams aimed at convincing victims to send money to a threat actor to avoid a punishment or receive a fictional reward. Cyber threat activity aimed at financial institutions and systems may intend to steal much larger sums.
- **Opinions** can be influenced and **reputations** damaged through online influence activities using misinformation, disinformation, or malinformation. Threat actors can target individuals or social discourse more broadly, by influencing specific events such as elections or conducting persistent influence campaigns to promote narratives favourable to their geopolitical objectives.

The impacts of cyber threat activity

Impacts to Canadians' privacy

Canadians put significant amounts of personal information online and depend on Internet-connected devices for communication, finances, entertainment, comfort, and safety. As this information moves online, it becomes vulnerable to cyber threat actors. Cyber threat actors also steal financial, medical, and other personal information to sell online or use in cybercrimes. Large corporate data breaches impact millions of customers and reveal personal information that can be used in follow-on crimes.

Impacts to Canadians' financial security

When threat actors obtain Canadians' login credentials, credit card details, and other personal information they can use this information to steal money, commit fraud, or sell it on cybercrime marketplaces. Cyber threat actors also target point-of-sale (POS) systems used by businesses by installing malware that can steal customer information, interfere with business operations, make fraudulent purchases, manipulate pricing, and cause other forms of disruption.

Canadians are targeted by online fraud schemes. Cyber threat actors keep scams relevant and appealing by associating their cyber fraud operations with current events. Elections, tax season, and trending news stories have all been used as a backdrop for cybercrime.

Impacts to Canada's economic health

Cyber threat activity results in unwanted expenses for organizations, including the costs of ransoms or stolen funds, losses due to the disruption of operations, the price of securing and insuring networks, reputational damage and related loss of customers, and theft of intellectual property or sensitive information. These costs are a drain on organizations' finite resources and decrease their competitiveness. Taken together, they are also a drain on the Canadian economy.

Cyber threat actors target Canadian businesses with the intent of stealing valuable business information. The theft of this information can have both short- and long-term financial consequences for the victims, including impacts to global competitiveness and reputational damage.

Impacts to Canadians' trust

By spreading false and potentially harmful information, cyber threat actors pollute the online information space making it difficult for Canadians to separate truth from falsehoods. This can influence civil discourse, influence policymakers' choices, and impact the reputations of politicians and leaders.

Cyber threat actors exploit trusted relationships between organizations by targeting online and in-person payment systems, supply chain vulnerabilities, or by taking advantage of the privileged access held by managed service providers—companies that provide information technology (IT) services and maintain the networks of their clients.

Impacts to Canadians' safety and security

When cyber threat actors target physical processes in industry, or critical services connected to the Internet such as those in healthcare or transportation, disruptions can result in impacts to Canadians' safety and security. For individuals, there is a risk that cyber threat activity against home and personal IoT devices, including medical devices such as pacemakers, can impact physical safety.

Stalkers and abusive partners can take advantage of vulnerabilities in personal IoT devices to steal information collected by fitness trackers and smart home technologies to identify and locate victims, or overtly control a victim's devices to intimidate them.

How cyber threat actors operate

Cyber threat actors pursue their objectives by exploiting technical vulnerabilities, using social engineering, and by creating, disseminating, or amplifying false or misleading content online to influence individuals' behaviour and beliefs.

Vulnerability exploitation involves taking advantage of weaknesses or flaws in the design, implementation, operation, or management of an IT system, device, or service, collectively referred to as **vulnerabilities**. Threat actors use **exploits** to take advantage of vulnerabilities, and deploy **payloads** that allow them to access, control, destroy, or enable further malicious activity on a victim's system. Threat actors can use tools that directly exploit specific technical vulnerabilities, and sophisticated actors may invest resources in attempting to discover new, previously unknown vulnerabilities, referred to as zero-days, in target systems. While **zero-days** have the advantage of being unknown to the owner of the IT system or software, cyber threat actors target known vulnerabilities as well, taking advantage of weak security protocols and unpatched systems.

Social engineering involves taking advantage of the people using the IT by exploiting human traits such as carelessness and trust. Threat actors use social engineering to trick individuals into providing sensitive information or inadvertently allowing access to a system, network, or device. Social engineering is an extremely common tactic in cyber threat activity today. For example, business email compromise (BEC) is a common and costly social engineering scheme, where threat actors impersonate executives or trusted third parties to trick victims into directly transferring funds. Social engineering is also often used in combination with vulnerability exploitation. For example, threat actors will create phishing and spear-phishing emails with malicious links or attachments – when people interact with those links and attachments, it activates exploits that provide the threat actor access into the victim's system.

Foreign cyber threat actors can also manipulate social media and legitimate advertising and information-sharing tools to conduct **online foreign influence** campaigns that seek to impact domestic events such as elections, censuses, or public health campaigns, as well as public discourse more broadly. Online foreign influence occurs when foreign cyber threat actors covertly create, disseminate, or amplify misinformation, disinformation, or malinformation to influence the beliefs or behaviours of the citizens of another state. With a thorough understanding of how traditional media and social media work—and how individuals consume information—cyber threat actors can promote their message to broad target audiences at a relatively low cost. They can do this by masquerading as legitimate information providers, hijacking social media accounts, or creating websites and new accounts. Threat actors can also leverage technology to create synthetic content including text, images, or videos, to promote their messages or create distrust.

Identifying cyber threat activity

Attribution is the act of accurately determining the threat actor responsible for a particular set of activities. Successful attribution of a cyber threat actor is important for several reasons, including network defence, law enforcement, deterrence, and foreign relations. However, attribution can be difficult as many cyber threat actors attempt to evade attribution through obfuscating their activities.

Obfuscation refers to the tools and techniques that threat actors use to hide their identities, goals, techniques, and even their victims. To avoid leaving clues that defenders could use to attribute the activity, threat actors can use tools and techniques that covertly send information over the Internet.

Sophisticated threat actors may also conduct **false flag operations**, whereby an actor mimics the known activities of other actors with the hope of causing defenders to falsely attribute the activity to someone else. For example, a nation-state could use a tool believed to be used extensively by cybercriminals or other nation-states in the hopes that it will be attributed to them.

The ability of cyber threat actors to successfully obfuscate their actions varies according to their level of sophistication and motivation. In general, nation-states and competent cybercriminals are more adept at obfuscation than other threat actors.

Appendix: Glossary

The following is a non-exhaustive list of common tools and techniques that are used by threat actors. For simplicity, they are listed alphabetically and are not ranked according to frequency or impact.

Backdoor (Porte dérobée)

A **backdoor** is a point of entry into a user's system or computer that bypasses traditional access and authentication measures. Once threat actors have this remote access, they can steal information, install malware, or control the device's processes and procedures. Backdoors can be a product of malware or other malicious cyber activity, but are also often deliberately and non-maliciously created for troubleshooting, software updates, or system maintenance. Threat actors can use these legitimate backdoors for malicious purposes.

Bots and botnets (Ordinateurs zombies et réseaux de zombies)

A **bot**, also known as a zombie, is an Internet-connected device (e.g., computers, mobile, and IoT devices) that is infected with malware without the owner's awareness and is remotely controlled by a threat actor to perform a specific malicious task. A **botnet** is a grouping of these compromised devices that are coordinated by a threat actor. Botnets typically expand by scanning the online environment and finding vulnerable devices that can provide computing power and additional capacity. Botnets are used for a multitude of purposes, such as to conduct distributed denial of service (DDoS), spread ransomware and malware, conduct ad fraud campaigns, send spam, divert traffic, steal data, and manipulate, amplify, and/or suppress social media and web platform content in order to impact public discourse.

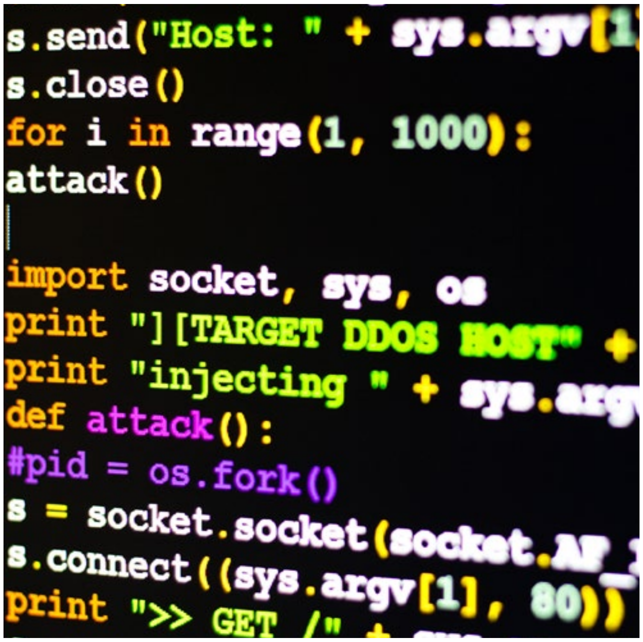
(Distributed) Denial of service

(Déni de service [distribué])

Denial of service (DoS) refers to any activity that makes a service (e.g., website, server, network, IoT device) unavailable for use by legitimate users, or that delays system operations and functions.

Flooding attacks (Attaque par inondation)

Flooding attacks are the most common form of DoS, where the threat actor repeatedly sends requests to connect to the target server but does not complete the connections. These incomplete connections occupy and consume all available server resources. As a result, the server cannot respond to legitimate traffic and connection attempts.



```
s.send("Host: " + sys.argv[1
s.close()
for i in range(1, 1000):
attack()

import socket, sys, os
print "][TARGET DDOS HOST" +
print "injecting " + sys.arg
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_
s.connect((sys.argv[1], 80))
print ">> GET /" +
```

Crash attacks (Attaque par arrêt de service)

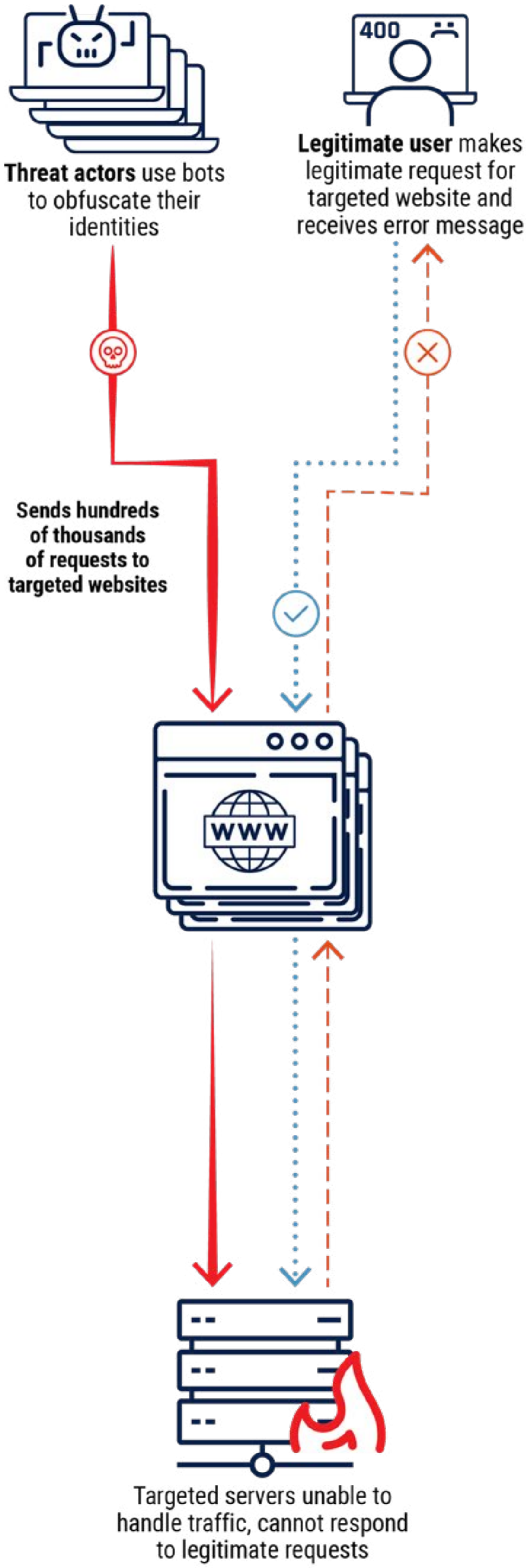
Crash attacks are less common than flooding attacks, and refer to when threat actors exploit a vulnerability to crash a system, thus denying access to it.

Distributed denial of service (DDoS)

(Déni de service distribué)

A **distributed denial of service attack, or DDoS**, is a DoS attack that originates from several machines at once. These machines can be controlled by a group of threat actors working together or be part of a botnet acting under the direction of a single threat actor. DDoS are more powerful and make it more difficult to identify the true source of the attack.

Figure 3: Distributed denial of service



400
Threat actors use bots to obfuscate their identities
Legitimate user makes legitimate request for targeted website and receives error message
Sends hundreds of thousands of requests to targeted websites
WWW
Targeted servers unable to handle traffic, cannot respond to legitimate requests

Exploits and exploit kits (Exploits et trousses d'exloit)

An **exploit** is malicious code that takes advantage of an unpatched vulnerability. An **exploit kit** is a collection of multiple exploits that affect unsecure software applications. Each exploit kit is customized to search for specific vulnerabilities and execute the corresponding exploit for the vulnerability it finds. If a user visits a website hosting an exploit kit, the exploit kit will test its repository of exploits against the software applications on the user's device and deploy the exploit that fits the user's vulnerability.

Code injection (Injection de code)

Code injection is when threat actors introduce malicious code into a computer program by taking advantage of a flaw in a program's functionality instructions or in the way it interprets data input. Two common code injection techniques are **cross-site scripting (XSS)** and **Structured Query Language (SQL) injection**.

- **XSS** is a code injection method whereby a threat actor injects and executes malicious code within a web application by bypassing the mechanisms that validate input. The malicious code is executed in the browser of users accessing the exploited web application. Code injected by XSS may either be a one-time execution or used to enable further malicious activity.
- **SQL injection** retrieves or modifies the contents of an SQL database by entering code into web forms that are meant to receive input for or query SQL databases. These databases may hold personally identifiable or other sensitive information.

Zero-day exploits (Attaques du jour zéro)

A **zero-day vulnerability** is a vulnerability that is not yet known by the vendor, and therefore has not been mitigated by a patch. A **zero-day exploit** is an attack directed at a zero-day vulnerability. Once a patch is developed, the vulnerability is no longer considered a zero-day.

Living off the land (Attaque hors sol)

Living-off-the-land is when threat actors use only the tools available through the victim systems' legitimate processes to conduct malicious cyber activity, rather than deploying malware. Cyber threat actors use pre-existing system tools to blend into the normal operations of a victims' device or network and avoid detection.

Malware (Maliciel)

Malware, short for "malicious software", refers to any software or code designed to infiltrate or damage a computer system. "Payload" refers to the actions malicious software takes once inside a victim's system or network (e.g., ransomware encrypting files or the installation of system backdoors that enable remote access).

Adware (Logiciel publicitaire ou publiciel)

Adware is short for "advertising software". Adware may infect a computer by being downloaded as part of another program or through web-based drive-by exploits. Its main objective is to generate revenue by delivering tailored online advertisements. Browser-based and application-based adware tracks and gathers user and device information, including location data and browsing history. Adware can lead to exploitation of security settings, users, and systems.

Beacon (Balise)

Beacons are signals sent by malware that attempt to connect to a cyber threat actor's command and control infrastructure once it has successfully infiltrated the target environment. Beacons let the threat actor know that they have successfully compromised the system and allows them to send additional commands to the malware.

Cryptojacker (Minage clandestin)

Cryptojacking is when a threat actor covertly exploits a victim's device (e.g., computers, mobile, and IoT devices) for the unauthorized mining of cryptocurrency. In order to increase efficiency (e.g., revenue) a threat actor can leverage a botnet of compromised devices. Such malware is typically delivered by visiting a compromised website, installing an application, or through phishing. Cryptomining or cryptocurrency mining is when software programs leverage computing resources to generate or "mine" a cryptocurrency, an activity that rewards the miner with a small fraction of the mined cryptocurrency as a fee for the mining service.

Ransomware (Rançongiel)

Ransomware is malicious software that restricts access to or operation of a computer or device, restoring it following payment. Threat actors often accomplish this through encryption, although they may also employ any number of methods of extortion, such as DDoS, threatening partners and clients, and/or threatening to release sensitive information. Ransomware is typically installed using a trojan or a worm deployed via phishing or by visiting a compromised website.

Some cybercriminals engage in **big game hunting (BGH)** ransomware campaigns, where they focus their activities against large organizations like critical infrastructure providers, governments, and large enterprises, that cannot tolerate sustained disruptions to their networks and are willing to pay large ransoms to quickly restore their operations.

Rootkit (Dissimulateur d'activité)

A **rootkit** is a malicious application designed to provide a threat actor with "root" or administrative privileged access to software and systems on a user's device. A rootkit provides full control, including the ability to modify software used to detect malware.

Spyware (Logiciels espions ou espiogiciels)

Spyware is malicious software used to track a user's digital actions and information with or without the user's knowledge or consent. Spyware can be used for many activities, including keystroke logging, accessing the microphone and webcam, monitoring user activity and surfing habits, and capturing usernames and passwords. Spyware used to facilitate intimate partner violence, abuse, or harassment is referred to as **stalkerware**.

Trojan (Cheval de troie)

A **trojan** is a malicious program disguised as or embedded within legitimate software.

Virus (Virus)

A **virus** is an executable and replicable program that inserts its own code into legitimate programs with the objective of damaging the host computer (i.e., deleting files and programs, corrupting storage and operating systems).

Wiper (Effaceurs)

A **wiper** is malware designed to completely wipe the hard drive of infected devices. Wipers may pose as ransomware to obfuscate the intent of the malware and make attribution more difficult.

Worm (Ver)

A **worm** is a computer program that independently self-replicates and spreads to other computers to drain a system's resources. Just like a virus, a worm can propagate code that can damage its host (e.g. deleting files, sending documents via email, or taking up bandwidth).

Online foreign influence activities (Activité d'influence étrangère en ligne)

Online foreign influence activities (OFIA) are a common tool for adversaries to further their core interests, including national security, economic prosperity, and ideological goals. Online influence campaigns can try to impact civil discourse, influence policy makers' choices, exacerbate friction in democratic societies, and damage the reputation of public figures such as politicians. OFIA often exploits **misinformation**, **disinformation**, and **malinformation**.

Misinformation (Mésinformation)

Misinformation refers to unintentionally false information that is not intended to cause harm.

Disinformation (Désinformation)

Disinformation refers to intentionally false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction.

Malinformation (Malinformation)

Malinformation refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.

Password cracking (Perçage de mots de passe)

Password cracking refers to techniques that allow cyber threat actors to directly access an account by guessing or decrypting the password.

Brute force (Force brute)

Brute force cracking uses an exhaustive number of randomly generated passwords to attempt to guess the correct password and obtain access to the account. Brute force password cracking is the least efficient method, especially against complex passwords.

Credential stuffing (Bourrage d'identifiants)

Credential stuffing is when lists of compromised username and password pairs are used to gain unauthorized access to online accounts. Cyber threat actors use these lists to conduct large-scale automated login requests, hoping that one of the compromised pairs will match an existing account on the site and give them access.

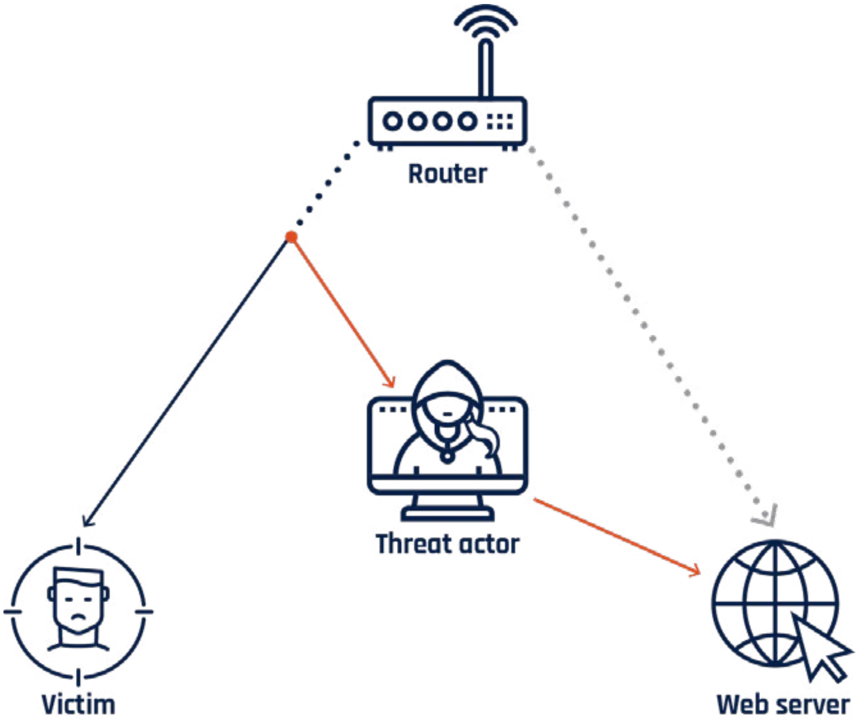
Dictionary attack (Attaque par dictionnaire)

Dictionary attacks take advantage of comprehensive lists of words and commonly used passwords, often including common misspelling of words and various permutations that account for password complexity requirements.

Person-in-the-middle (Attaque de l'intercepteur)

Person-in-the-middle (PITM) is a technique by which a threat actor intercepts a communication between two parties, such as a victim and a web server, without the victim's knowledge. The victim is under the illusion that they are communicating directly and securely with a website. PITM enables threat actors to monitor communications, reroute traffic, alter information, deliver malware, and acquire personally identifiable or other sensitive information. PITM can be achieved via several techniques such as phishing, pharming, typo-squatting, Wi-Fi eavesdropping, and SSL hijacking.

Figure 4: Person-in-the-middle



SSL hijacking (Détournement SSL)

Secure Sockets Layer (SSL) hijacking is a technique by which a threat actor intercepts and redirects an unsecure connection between a victim and a server trying to establish a secure connection. The threat actor is then able to provide a secure connection instead of the intended website, which enables them to intercept and compromise the communication without the victim's knowledge (see person-in-the-middle above). SSL hijacking is not about breaking the security provided by SSL, but rather, it inserts a compromised bridge between the non-encrypted and encrypted part of a communication.

Wi-Fi eavesdropping (Écoute électronique par réseau wi-fi)

Wi-Fi eavesdropping is when a threat actor installs what looks like a legitimate Wi-Fi access point in a public area. Once users connect to such an access point, often referred to as a malicious hotspot or a rogue access point, they fall victim to person-in-the-middle (PITM). Alternatively, threat actors may be able to intercept unencrypted web traffic on unsecured public Wi-Fi networks. Such activity allows a threat actor to monitor communications and to acquire personally identifiable or other sensitive information.

Reconnaissance (Reconnaissance)

Reconnaissance, or **recon**, refers to activities conducted by a threat actor to obtain information and identify vulnerabilities to facilitate future compromise(s). Opportunistic threat actors may scan the Internet for hosts with unsecured vulnerabilities and target them. When a target is selected, the threat actor may conduct additional research on their target including open-source searches on their business, employees, and infrastructure. More direct techniques include probing the target with malicious Internet traffic or using social engineering to extract information.

Social engineering (Piratage psychologique)

Social engineering is the practice of obtaining sensitive information by manipulating legitimate users, often using the telephone or Internet. Social engineering techniques may attempt to deceive the target into sending payment to an account controlled by the threat actor or collect information to enable further threat activity.

Phishing (Hameçonnage)

Phishing is a common method by which threat actors disguise themselves as a trustworthy entity with the intent to lure a large number of recipients into providing information, such as login credentials, banking information, and other personally identifiable information. Phishing is an example of a social engineering technique and is mainly conducted through email spoofing and text messages. Users become victims when they open malicious attachments or click on embedded links.

Spoofing (Mystification)

Spoofing is the act of masking or forging a website, email address, or phone number to appear as if it originates from a trusted source. After receiving a phishing message, the victim can be enticed into giving away personal, financial, or other sensitive information or clicking on a link or attachment, which can infect a device with malware.

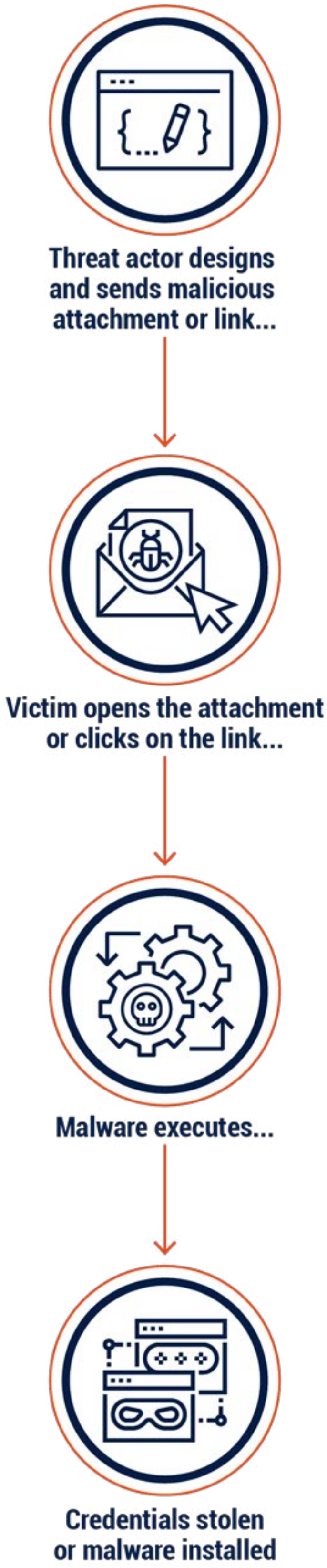
Spear-phishing (Harponnage)

Spear-phishing occurs when a cyber threat actor sends a personally tailored phishing message to a more precisely selected set of recipients or even a single recipient. Spear-phishing relies on social engineering, using details that are believable to the victim as originating from a trusted source. Whaling refers to spear-phishing targeted at senior executives or other high-profile recipients with privileged access and authorities.

Business email compromise (BEC) (Compromission de courriel d'affaires)

Business email compromise (BEC) is one of the most common and costly social engineering schemes targeting organizations. BEC involves emails designed to trick an employee in the target organization into directly transferring funds to cyber threat actors. To achieve this, cyber threat actors often impersonate high-level executives or trusted third parties.

Figure 5: Phishing & spear-phishing


Threat actor designs and sends malicious attachment or link...
Victim opens the attachment or clicks on the link...
Malware executes...
Credentials stolen or malware installed

Web-based exploits (Exploit sur le Web)

Web-based exploits aim to compromise users when they browse, or attempt to browse, to specific webpages. They function by compromising or impersonating a website that victims wish to visit, compromising the victim themselves, or exploiting vulnerabilities in the systems that direct users to the correct webpage.

Drive-by exploit (Attaque par téléchargement furtif)

A drive-by exploit refers to malicious code that a cyber threat actor has placed on a website without the website host's knowledge; the malicious code attempts to compromise the devices of any user who visits the website.

Formjacking (Détournement de formulaire)

Formjacking is when cybercriminals inject malicious code into a webpage form, such as a payment page, to compromise it and steal credit card details and other information that is entered by users on these pages.

Pharming (Détournement de domaine)

Pharming is a technique used to redirect traffic from a legitimate website to a malicious one. This deception can be achieved by modifying the user's system settings or by exploiting vulnerabilities in the domain name system (DNS) server software, which is responsible for resolving URLs into IP addresses. Contrary to typo-squatting (see below), where a user mistypes a website address and is redirected to an illegitimate website, pharming can redirect a user who properly types the URL. At a quick glance, the illegitimate website may appear to be the legitimate website and can be used to deliver malware and acquire personally identifiable or other sensitive information.

Typo-squatting (Typosquattage)

Typo-squatting is a technique by which a threat actor registers domain names that have very similar spelling to and can be easily confused with a legitimate domain address. Typo-squatting is also known as URL hijacking and enables a threat actor to redirect a user who incorrectly typed a website address to an alternative look-alike domain under the actor's control. The new domain can then deliver malware and acquire personally identifiable or other sensitive information. Luring a victim to a hijacked URL can also be achieved through phishing techniques.

Watering hole (Attaque par embuscade)

A **watering hole** is a website compromised with an exploit and frequented by individuals specifically targeted by a cyber threat actor.