CANADIAN CENTRE FOR
CYBER SECURITY

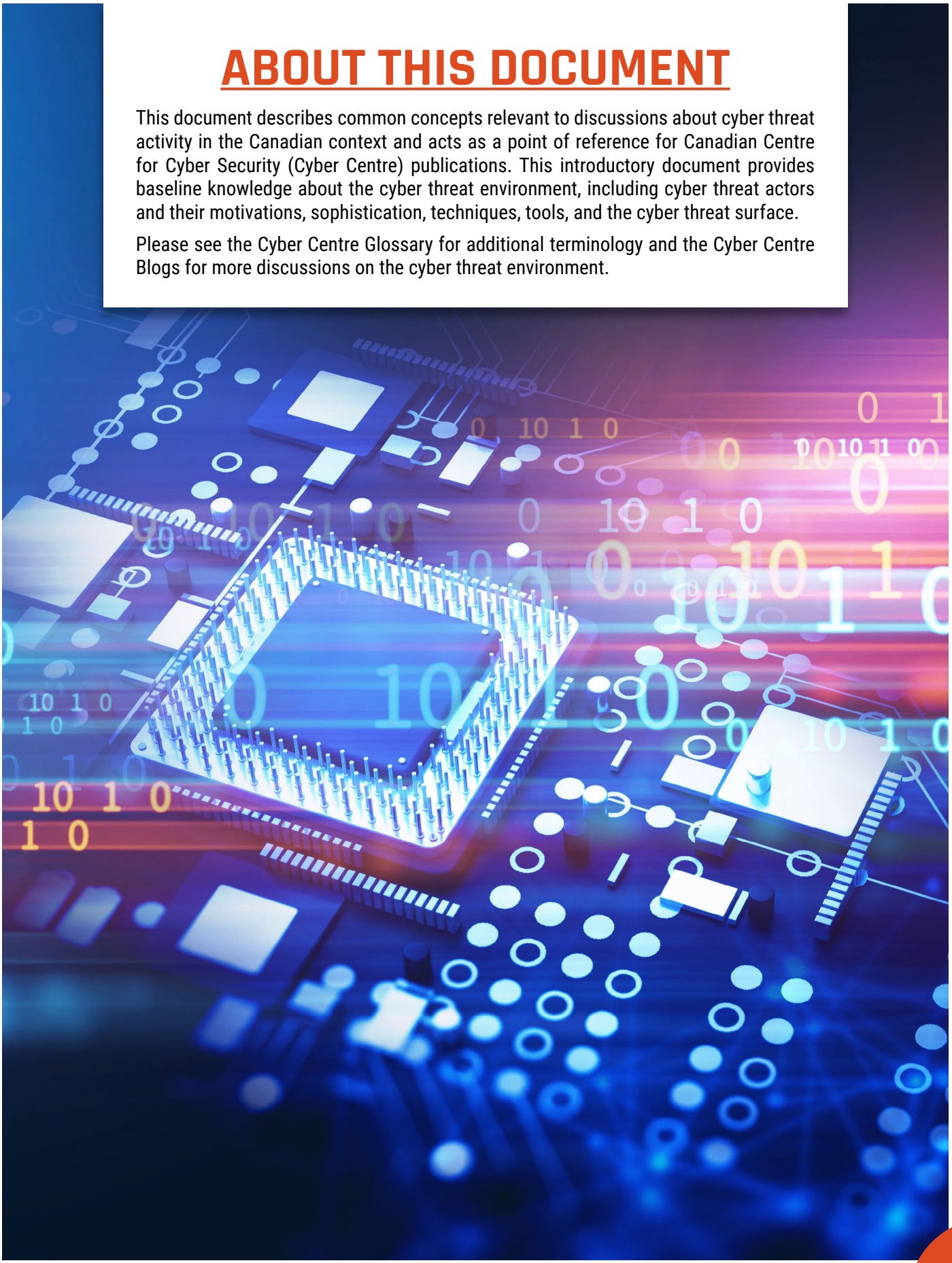
An Introduction to the Cyber Threat Environment

Communications Security Establishment
Centre de la sécurité des télécommunications
Canada

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 for additional terminology and the Cyber Centre Blogs for more discussions on the cyber threat environment.



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.

The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity.

CYBER THREAT ACTORS

Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.

MOTIVATIONS

Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation.

Figure 1: Cyber threat actors

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

SOPHISTICATION

Cyber threat actors are not equal in terms of capability and sophistication, and 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, even sophisticated actors use less sophisticated and readily available tools and techniques because these can still be effective for a given task and/ or make it difficult for defenders to attribute the activity.

Nation-states are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination.

Cybercriminals are generally understood to have moderate sophistication in comparison to nation-states. Nonetheless, they still have planning and support functions in addition to specialized technical capabilities that affect a large number of victims.

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

Hacktivists, **terrorist groups,** and **thrill-seekers** are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation.

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. Access is a key component for malicious threat actors and having privileged acess eliminates the need to employ other remote means. Insider threats may be associated with any of the other listed types of threat actors, but can also include disgruntled employees with motive.

CYBER THREAT ACTIVITIES

Cyber threat actors conduct malicious cyber threat activity by exploiting technical vulnerabilities, employing social engineering techniques, or by manipulating social media. A determined and capable adversary will often carefully select the technique most likely to result in successful exploitation after conducting reconnaissance against their target and may use a range of techniques to achieve their goal. The majority of threat actors, however, simply cast a wide net in hopes of exploiting any unsecure network or database.

Technical vulnerabilities are weaknesses or flaws in the design, implementation, operation, or management of an information technology system, device, or service that provides access to cyber threat actors. For example, a threat actor may attempt to install malicious software, called **malware**, or take advantage of existing flaws to exploit the targeted system. In addition to installing malware, threat actors also use tools that directly exploit specific technical vulnerabilities.

Exploitation methods that target human vulnerabilities, such as carelessness and trust, are collectively known as **social engineering**. Threat actors use social engineering to trick an individual into inadvertently allowing access to a system, network, or device. Phishing and spear-phishing are common social engineering techniques. (Please see *Annex A: The cyber threat toolbox* for more information).

Cyber threat actors can also manipulate social media in order to influence public discourse. 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 broader 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.

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 a number of reasons, including network defence, law enforcement, deterrence, and foreign relations. Cyber threat actors attempt to evade attribution through obfuscation.

Obfuscation refers to the tools and techniques that threat actors use to hide their identities, goals, techniques, and even their victims. In order to avoid leaving clues that defenders could use to attribute the activity, threat actors can use either common, readily available tools and techniques or custom-built tools that covertly send information over the Internet.

Sophisticated threat actors can also use **false flags**, 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.

The ability of cyber threat actors to successfully obfuscate their actions varies according to their level of sophistication and motivation. In general, more sophisticated actors, such as nation-states and competent cybercriminals, will be more adept at – and have more reasons for – obfuscation and will be more successful in avoiding attribution than less sophisticated threat actors.

CYBER THREAT SURFACE

The cyber threat surface refers to all the available endpoints that a threat actor may attempt to exploit in Internet-connected devices within the cyber threat environment. The many processes that produce, deliver, and rely on information systems connected to the Internet are also potential threat vectors and targets. Services, devices, and data can all be targeted to compromise production and delivery systems, such as supply chains and service management systems. As these processes continue to evolve, the threat surface will expand.

In addition, systems that connect physical entities with the Internet are increasingly common. For example, the smart grid, the Internet of Things, and industrial control systems all present a risk of cyber threat actors interfering with the physical environment of their victims.

Internet-connected devices and applications bring great benefits to individuals and to the global economy, but as more physical and information assets become accessible online or have a digital component, cyber threat actors will have more opportunities to conduct malicious cyber threat activity, to access information, disrupt operations, or even have a physical impact.

ANNEX A: THE CYBER THREAT TOOLBOX

It is beyond the scope of this document to present all cyber capabilities that threat actors could deploy. Below 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.

ADWARE

Adware is short for advertising software and its main objective is to generate revenue by delivering tailored online advertisements. As such, browser-based and application-based adware tracks and gathers user and device information, including location data. Adware can lead to exploitation of security settings, users, and systems. Malware, man-in-the-middle, and spyware are often associated with this tool.

BACKDOOR

A **backdoor** is a point of entry into a user's system or computer, bypassing authentication measures, encryption, or intrusion detection systems. Once threat actors have this remote access, they can steal information, install malware, or control the device's processes and procedures. Backdoors are often deliberately created for troubleshooting, software updates, or system maintenance. Threat actors can use these legitimate backdoors for malicious purposes.

BOTS AND BOTNETS

A **bot**, also known as a zombie, is an Internet-connected device (e.g., computers, mobile, and Internet of Things 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.

CODE INJECTION

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 stored for future use.
- 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.

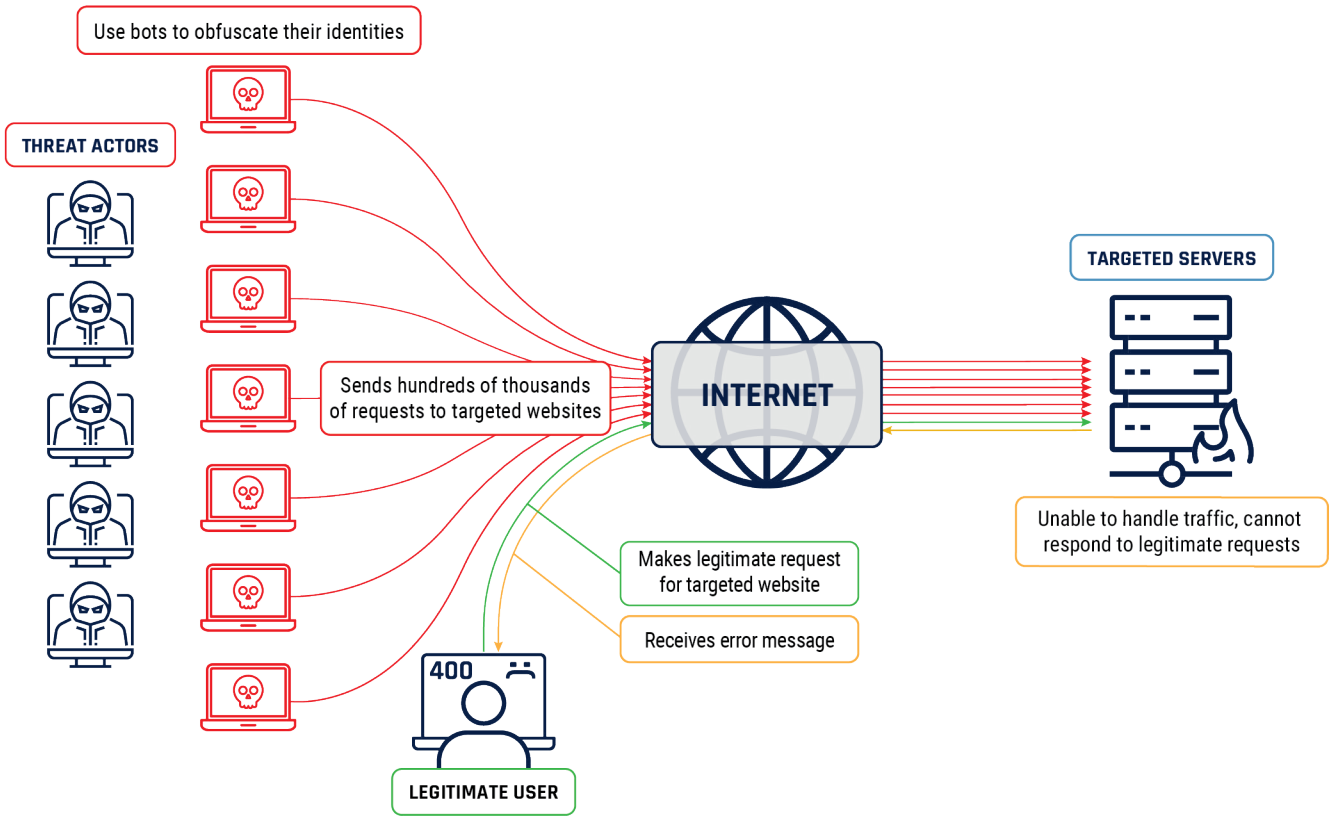
CRYPTOMINING

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. Cryptojacking is when a threat actor covertly exploits a victim's device (e.g., computers, mobile, and Internet of Things 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.

(DISTRIBUTED) DENIAL OF SERVICE

Denial of service (DoS) is a technique by which a threat actor makes an attempt at disrupting the normal activities of a specific host (e.g., website, server, network, Internet of Things device) by overwhelming it with Internet traffic, also known as requests. The overall objective is to render the host unavailable for legitimate requests from users and render the targeted system dysfunctional. **Distributed denial of service (DDoS)** adds a level of complexity by introducing traffic flooding from multiple sources (e.g., from a botnet). This larger-scale activity makes it much harder to stop and very difficult to distinguish legitimate user traffic from malicious traffic.

Figure 2: Distributed denial of service



DRIVE-BY EXPLOIT AND WATERING HOLE

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

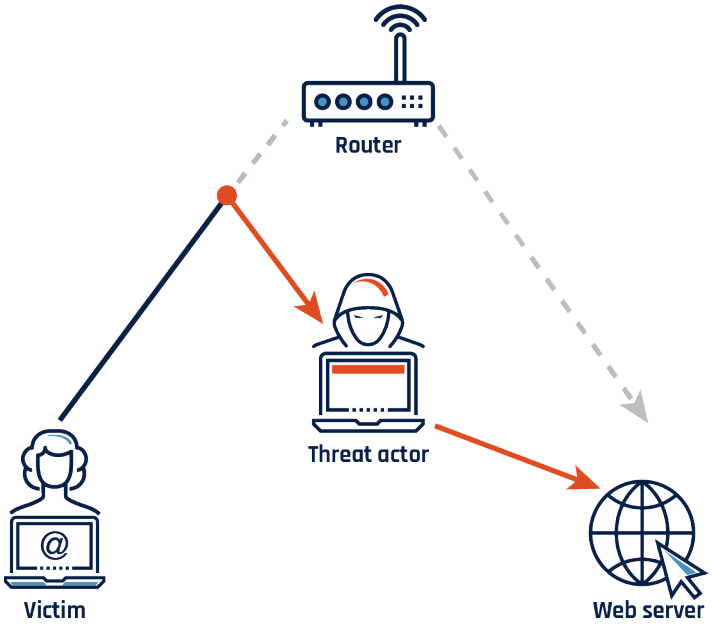
EXPLOITS AND EXPLOIT KITS

An **exploit** is malicious code that takes advantange 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.

MAN-IN-THE-MIDDLE

Man-in-the-middle (MITM) 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. MITM enables threat actors to monitor communications, reroute traffic, alter information, deliver malware, and acquire personally identifiable or other sensitive information. MITM can be achieved via several techniques such as phishing, pharming, typo-squatting, Wi-Fi eavesdropping, and SSL hijacking.

Figure 3: Man-in-the-middle



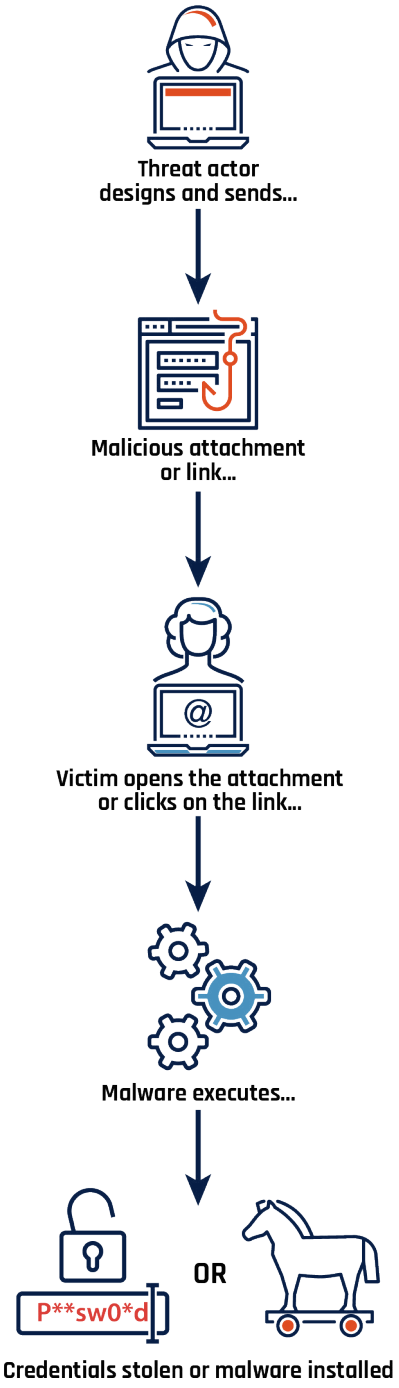
PASSWORD CRACKING

Password cracking is an attempt to directly access accounts. Two common forms of password cracking are **brute force** and **dictionary-based**. Brute force cracking uses an exhaustive number of randomly generated passwords to attempt to gain access, while dictionary-based cracking checks against a list of commonly used passwords.

PHARMING

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.

Figure 4: Phishing and spear-phishing



PHISHING, SPOOFING, SPEAR-PHISHING, AND WHALING

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.

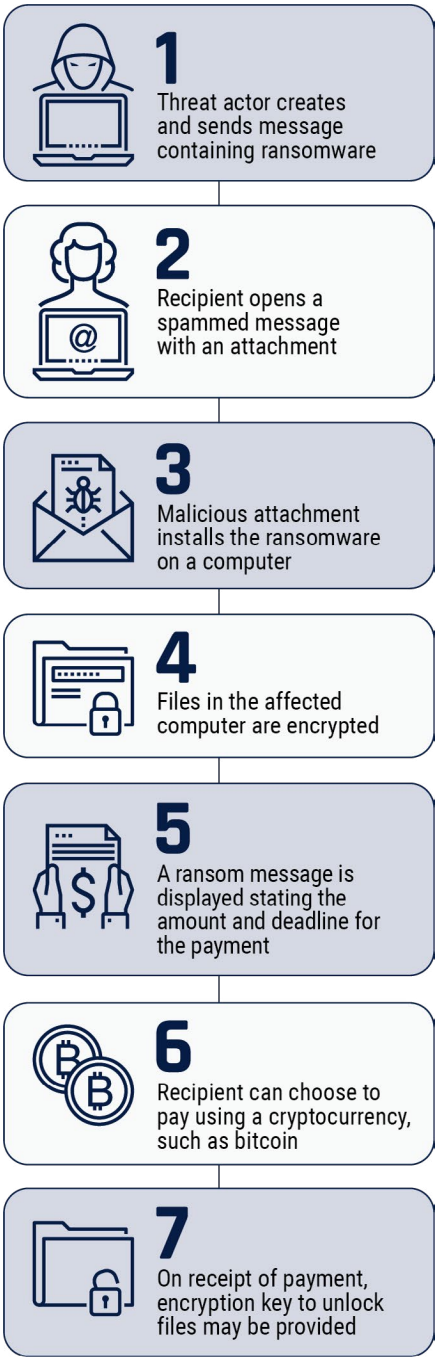
Spoofing is the act of masking or forging a website, email address, or phone number to appear as if it originates from a trusted source. After receiving a phishing message, the victim can be enticed into giving away personal, financial, or other sensitive information or clicking on a link or attachment,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

Spear-phishing 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.

RANSOMWARE

Ransomware is malicious software that, in many cases, restricts access to a computer or a device and its data by encrypting its content and demanding that a ransom be paid, usually via a cryptocurrency such as bitcoin, in order for the victim to regain access to systems and information. Ransomware can also lock systems in various ways without the use of encryption, disrupting device performance. Actors may threaten to expose sensitive, personal, or embarassing information unless a ransom is paid. Ransomware is typically installed using a trojan or a worm deployed via phishing or by visiting a compromised website.

Figure 5: Ransomware



ROOTKIT

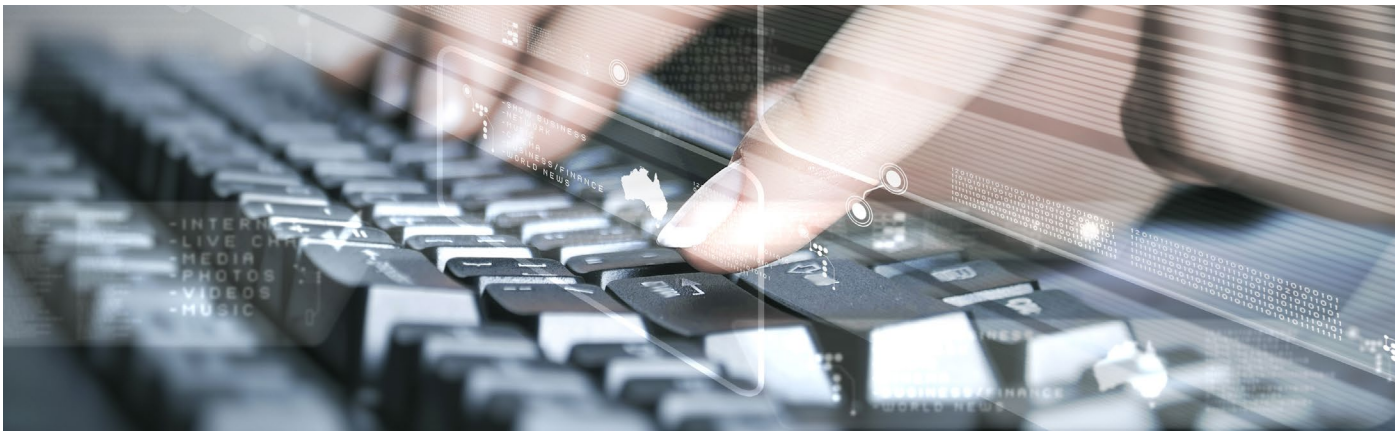
A **rootkit** is a malicious application that is designed to covertly provide a threat actor with "root" or administrative privileged access to software and systems on a user's device. A rootkit provides full control, including the ability to modify software used to detect malware. Rootkit installation can be achieved in many ways, including through password cracking, social engineering, and leveraging a bug or design flaw that can grant privileged access to a user's system or device.

SPYWARE

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.

SSL HIJACKING

Secure Sockets Layer (SSL) hijacking is a technique by which a threat actor is able to intercept and redirect 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 man-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.



TYPO-SQUATTING

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.

VIRUS, WORM, PAYLOAD, AND TROJAN

Malware is commonly delivered through the use of viruses, worms, and trojans with far-reaching consequences. 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). In its simplest state, a **worm** is a computer program meant to self-replicate and spread to other computers to drain a system's resources. Additionally, just like a virus, a worm has the ability to propagate code that can damage its host. Such code is referred to as a **payload** (e.g., the ability to encrypt files in ransomware and the installation of system backdoors that enable remote access). A **trojan** is a malicious program disguised as or embedded within legitimate software that has similar objectives to viruses and worms, but, unlike either of them, does not replicate or propagate on its own

WI-FI EAVESDROPPING

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 man-in-the-middle (MITM). Such activity allows a threat actor to monitor communications and to acquire personally identifiable or other sensitive information.

WIPER

A **wiper** is malware designed to completely wipe the hard drive of infected devices.

ZERO-DAY VULNERABILITIES AND ZERO-DAY EXPLOITS

Unmitigated vulnerabilities not in the public domain and known only to a few people are referred to as **zero-day vulnerabilities**. An exploit against a zero-day vulnerabilitiy is called a **zero-day exploit**.