A Common Cyber Threat Framework
Lexicon of concepts and definitions
July 17, 2018

The Cyber Threat Framework Lexicon is meant to be a flexible and open document. Our goal is to provide enough content and guidance to allow users to appropriately and repeatably categorize data without producing a massive document covering every conceivable possibility at the "Action" and "Indicator" level.
We solicit your comments and feedback on content, accuracy, and usability as a means to continually improve its content and utility.
Recommended changes must be unencumbered (e.g., non-proprietary or copyrighted) as they will be shared openly.

Terms				Definitions
Layer 1 Stages	layer 2 Objectives	Layer 3 Actions (Examplars)	Layer 4 Indicators	
stages				The progression of cyber threat actions over time to achieve objectives.
	objectives			The purpose of conducting an action or a series of actions.
		actions		Activity and associated resources used by a threat actor to satisfy an objective.
			indicators	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attempt to take or having taken an action, or to achieve an objective.

Preparation	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, timeline and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.			
	Plan activity			Steps taken by a threat actor before conducting malicious cyber activity to: define intent; establish policy limitations; identify funding; coordinate intended activities; establish initial objectives and parameters for measuring progress/success towards meeting them; and the steps taken to update plans, activities, and requirements based upon insights gained during the eventual victim engagement.
	Develop resources and capabilities			Steps taken by the threat actor to secure the requisite resources (funding, people), and acquire the capabilities (technology, processes, tools, infrastructure), and partnerships necessary for conducting the planned cyber threat activity, and for ascertaining its success/failure in achieving the desired objectives/outcomes.
	Acquire victim specific knowledge			Steps taken by the threat actor prior to gaining access to an intended victim's computer(s), information system(s), network(s), and/or data stores, but just prior to execution of the planned cyber activity, to gather through physical/electronic observation (i.e., port scanning) or social media surveys, the latest details on the activities, characteristics, resources and perceived vulnerabilities of the intended victim to validate/confirm final planning assumptions.
	Complete preparation			Warehousing malicious cyber capabilities in/on threat actor internally owned or externally acquired storage locations, whether as electronic media or physical hardware (i.e., removable media, bundled hardware/firmware/software corrupted through a cooperative supply chain) for future deployment, and issuing final instructions to those that will conduct the planned malicious activity.

Engagement	Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores.			
	Deploy capability			Steps taken to position malicious content for operational employment, e.g., place corrupted firmware in commercial products.
	Interact with intended victim			Contact between threat actor and intended victim in an attempt to establish an opportunity to or to gain direct access to victim's computer system/network.
	Exploit vulnerabilities			Steps taken to leverage deficiencies, vulnerabilities, gaps, and/or shortfalls (e.g., zero day exploits, malicious SQL injects, cross-site scripting) in the intended victim's computer(s), network(s), and/or information system(s) in an attempt to gain unauthorized access.
	Deliver malicious capability			Electronic or physical activities that expose malicious content to the intended victim that results in a physical or electronic presence but which does not activate the malicious content, e.g., send an email to intended victim with malicious attachment, distribute removable media containing Malware.

Presence	Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores.			
	Establish controlled access			Activities (automated or manual) intended to gain unauthorized control (violate the confidentiality) of the intended victim's computer(s), information system(s), and/or network(s) to allow the threat actor to direct or conduct enabling or malicious activity.
	Hide			Steps taken by a threat actor or Malware to avoid detection (e.g., obfuscation, masquerading, indicator manipulation, creation of unique libraries) on the victim's computer(s), information system(s), and/or network(s).

	Expand presence			Steps taken by a threat actor to broaden their initial footprint (measured in terms of authorizations and/or system capabilities) on the victim's computer(s), information system(s), and/or network(s), to support/conduct additional malicious activity.
	Refine focus of activity			Steps taken by the threat actor confirm the existence and validity of the intended victim's data, information, and/or system capabilities, and/or identify additional potential victims and their data, computer(s), and/or information system(s), and that the available malicious tools/processes will achieve the intended outcome/results.
	Establish persistence			Steps taken by the threat actor (electronically or physically) to preserve, obfuscate, or increase their footprint or capabilities on a victim's computer(s), information system(s), and/or network(s), e.g., additions to or modification of the existing operating system or enterprise capabilities (e.g., Windows software services, Master Boot Record), or the implant of additional malicious software.

Effect/Consequence	Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.			
	Enable other activities			Measurable cyber threat activities that indicate, identify and/or establish a foundation for (to include the conduct of effects assessments) subsequent actions against a victim's data, computer(s) and/or information systems, e.g., establish a command and control node or hop point, incorporates the victim's computer/information systems in a botnet, or exfiltrate user password and/or credentials. Analytic judgments or assessments are not included.
	Deny access			Steps taken by the threat actor to temporarily deny, degrade, disrupt, or destroy access to, or 'encrypt for ransom', (violate the availability) a victim's physical or virtual computer or information system(s), network(s), communications capabilities, and/or data stores.

	Extract data			Threat actor activities within the victim's resources to move data/data stores to an alternative location, either within the target's data stores, computers and/or systems, or external to them.
	Alter data and/or computer, network, and/or system behavior			Steps taken by the threat actor to change the behavior/outcomes/and interaction (violate the integrity) of the victim's computer(s), information system(s), and/or network(s).
	Destroy hardware/software/data			Permanently, completely and irreparably damage a victim's physical or virtual computer or information system(s), network(s), and/or data stores, e.g., system administrators discover permanent unexplained damage to portions of the information system, system users discover data/files have been inappropriately corrupted or deleted.