## GCTI – FOR578 INDEX



# Aa

**Actions on Objectives** *[b2/p25]* Everything that happens after the adversary has operational control of a system.

**Activity Group** *[b1/p58]* Clustering of intrusions by vertices on the diamond model. Mathematical formulas are used to define and expose value to an analyst.

**Activity Group Creation** *[b4/p82]* Six distinct steps. See book for steps.

**Adversary**  *[b2/p31]* Individual or group behind an event. Two categories: Operator & Customer

**Adversary Registered Domain** *[b3/p39]* Adversary registered domains run a risk but allow control. Money trail can be created.

**Analysis Defined**  *[b1/p26]* Detailed examination of elements or structure of something, breaking something down into parts to understand its operation.

**Analysis of Competing Hypothesis**  *[b4/p39]* Structured method to identify all potential hypotheses, collect all evidence, compare evidence w/ hypothesisF, and then rank/identify the best choice.

**Anchoring/Focusing** *[b4/p28]* Beginning with an assumption then adjusting ones assessment as new information becomes available instead of taking the information as a whole.

**Anecdotal Fallacy** *[b4/p23]* Personal experience is used over compelling evidence.

**Appeal to Probability**  *[b4/p23]* Making a determination based on what's most likely the cause.

**Appeal to the Stone** *[b4/p24]* Identification of a claim as absurd without any proof to dismiss it.

**Argument from Repetition**  *[b4/p24]* Arguing so much that eventually people accept the conclusion to end it.

**Argument from Silence** *[b4/p24]* Accepting a conclusion due to lack of evidence against it.

**Assessment equation** *[b5/p76]* confidence + analysis + evidence + sources = assessment

**Attribution (Four Approaches)**  *[b5/p100 ]* Adversary Admission, Leaks, Direct Access, Intrusion Analysis.

**Attribution (Use Cases)** *[b5/p103]* Criminal prosecution, State Tools, Strategic org changes.

**Attribution Requirements** *[b5/p98]* Costly intel requirement. List at this location in the book.

**Autonomous System Number (ASN)** *[b3/p45]* ASN represent the routable ip addresses for an entity connected to the internet. Broadcast via BGP.

**Axiom** *[b5/p8]* Multi company team focused on unraveling of complex espionage program attributed to China.

# Bb

**Bit9** *[b5/p7]* Security vendor hit by Hikit via initial use of sql injection.

**Brainstorming** *[b1/p42]* Capture and sort info quickly supports collaboration and sharing of ideas.

**Burden of Proof** *[b4/p25]* Requiring someone to disprove someone else's claim instead of requiring proof.

**Business Case for Security** *[b5/p64]* Identify Technical needs and match + Translate into audience language = understood, appreciated, and supported security efforts.

# Cc

**Campaign** *[b1/p60]* Mission focus of the adversary across multiple intrusions.

**Capability/TTP**  *[b2/p33]* Tools and tradecraft employed by the adversary during an event.

**Carbanak** *[b1/p108]* Carberp based malware that was heavily modified and used to target the financial sector by APTs.

**Carberp** *[b1/p107]* Cybercrime toolkit appearing in Fall 2010.

**Causation**  *[b4/p34]* Causation IS correlation

**CoA (Courses of Action)** *[b2/p38]* Actions to take as the defender in response to intelligence. 7 D's of Action.

**Code Reuse** *[b3/p8]* Reuse of code in malware used in intrusions. Can be good for detection purposes as code persists through samples.

**Code Reuse** *[b3/p14]* Code reuse can help reveal links in the Adversary portion of the diamond model.

**Cognitive Bias** *[b4/p26]* Constraints on how we as analysts think that influence incorrect decisions and assessments.

**Collection Management Framework (CMF)** *[b1/p115]* Plan for how you collect data, where you collect it form and what type of data you collect.

**Collective Intelligence Framework** *[b3/p72]* Management system to make threat feeds useful to organizations.

**Command & Control (C2)** *[b2/p22]* Ways communication is established between the victim/target system and the adversary.

**Compile Time** *[b3/p6]* Time malware or files are compiled for use. Can be used to make links between intrusions.

**Conceptually Driven Analysis** *[b1/p28]* Used frequently due to lack of precision or data accuracy. Does not always lead to a consensus but a greater understanding.

**Confidence Assessments**  *[b5/p75]* High, Medium, Low. Sliding scale of confidence this is not the only route to display confidence.

**Configuration Data** *[b3/p16]* Details to the malware on how to perform its necessary functions.

**Confirmation Bias** *[b4/p29]* Tendency to include or reject evidence based on its alignment to a preferred hypothesis.

**Congruence Bias** *[b4/p30]* Failure to adequately present and test alternative competing hypoth. and instead find different ways to present data that tests an existing hypoth.

**Correlating Clusters** *[b4/p75]* Use of the ACH process w/ Killchain/Diamond model and the rule of 2.

**Correlation** *[b4/p34]* Often ISNT causation.

**Counterintelligence**  *[b1/p21]* Identification, assessment, and neutralization of adversary intelligence activities.

**CVE-2014-1761** *[b3/p100]* Remote code execution in Microsoft Word.

# Dd

**DanBot** *[b3/p6]* Malware used by HEXANE but not attributable to them is off the shelf/commodity.

**Data Analysis** *[b4/p55]* Cleaning, transforming, and modeling of data, for the purposes of revealing patterns and new insights.

**Data Driven Analysis**  *[b1 /p28]* Pre-existing/developed analytic models based on assumptions data and the model used are accurate and applicable.

**Data Pivoting** *[b3/p32]* Taking a data point/indicator then culling data sources to identify what info. we can find related to the starting point.

**Data vs. Intelligence**  *[b1/p41]* Relationship of Data, information, and intelligence graphic.

**Datasploit** *[b3/p74]* Identified credentials, API, keys, subdomains, domain history, etc.

**DC3 Malware Config Parser** *[b3/p23]* A framework for parsing configuration information from malware.

**Decomposition**  *[b1/p37]* Breaking down a problem into its components

**Delivery**  *[b2/p14]* Tools and infra used to pass weaponized object to the target/victim.

**Diagnostics**  *[b4/p43]* Assess the degree to which each piece of evidence is diagnostic in determining the relative likelihood of the hypotheses.

**Diamond Model (Meta Features)** *[b4/p81]* timestamps, phase, result, direction, methodology, and resources.

**Diamond Model Axioms**  *[b2/p29]* Accepted assumptions about the diamond model. 7 in total.

**Diamond Model Overview** *[b2/p28]* Model/Lens to conduct analysis of repeating patterns through multiple intrusions. 4 facets: Infra, Adversary, TTP/Capability/Victim

**Discover (Tool)** *[b3/p74]* Preforms reconnaissance and scanning on domains, IPs, or target lists.

**Disk Forensics**  *[b2/p97]* Use of imaging software to pull details related to files and processes on disk.

**Domains (Collection Source)** *[b3/p31]* Domains used as collection to attribute intrusions and conduct analysis/pivoting.

**DomainTools** *[b3/p53]* Passive DNS collection and analysis tool.

**Doppelpaymer Ransomware** *[b4/p7]* Good example of nuance between ttps and tradecraft.

**Dynamic DNS Domains (DDNS)** *[b3/p40]* DDNS records have a short TTL to expedite propagation. Used by the adversary to rotate ip addresses of domains.

# Ee

**Elections**  *[b1/p33]* Ransomware targeting elections causing confirmation bias in the media and surrounding reporting.

**Enumerate Hypothesis** *[b4/p41]* Analyzing competing hypotheses is to develop the hypotheses thems3elves based on the available intelligence.

**Epic Turla** *[b3/p51]* Snake/Uroboros is a threat group attributed to Russia. Uses sophisticated C2 protocols in intrusions.

**Estimative Language**  *[b5/p70]* Likely might seem and such are estimative language.

**Evidentiary Dependence** *[b4/p46]* What evidence is most significant in the prioritization?

**Exploitation**  *[b2/p17]* Action of using weaponized object against the victim/target. Human/computer/vulnerability.

**External Intrusion Reports** *[b4/p80]* Complementary to filling knowledge gaps. DO NOT merge with your data.

# Ff

**False Flags**  *[b5/p117]* Specific type of operation where purpose is to redirect the blame of an attack onto a third party.

**Field of View Bias** *[b1/p40]* Each person and org has a limited view into threats.

**FireHOL** *[b3/p71]* List of threat feeds that is well maintained.

**Forensic Images** *[b2/p112]* Two types mem and disk. volatile vs non volatile

**Four Types: Threat Detection** *[b1/p88]* Environmental: (Modeling/Configuration Analyst) Threat: (Threat Behaviors/Indicators)

# Gg

**Generation vs Consumption**  *[b1/p80]* Generating and consuming intelligence are two fundamental parts of a program.

**GlassRAT** *[b3/p62]* Campaign tied to plugx campaign. Undetected trojan targeting Chinese nationals.

**GUID** *[b3/p7]* Globally Unique ID.

# Hh

**Hacking Team** *[b5/p30]* Italian security firm specialized in providing surveillance and exploitation services for gov and law enforcement.

**Header Metadata** *[b3/p13]* PDB paths, compiler versions and other artifacts that are left in the code. Sometimes OPSEC mistakes.

**Heatmap** *[b5/p51]* Heatmap visualization for metrics on CTI.

**HEXANE** *[b3/p5]* Activity group targeting oil and gas in the middle east.

**Hikit** *[b5/p6]* Malware that doesn't connect directly to c2, but waits for the adversary to interact with it.

**Hinderances**  *[b1/p32]* Bias, Simplification of process causing misses, etc.

**Hindsight Bias** *[b4/p31]* Tendency to see an unpredictable event as an obvious result of a set of conditions or parameters.

**HRTest Server** *[b1/p13]* Proxy server monitored by the FBI used by Moonlight Maze actors.

**Hub and Spoke**  *[b5/p43]* Hub acts as a clearing house for all information. Push/pull actions available.

**Human Finger Print Locations** *[b3/p12]* Header metadata, code reuse, configuration data.

**Human Fingerprints** *[b2/p32]* Using malware as a source of adversary capability intelligence. Humans make marks and follow patterns when using malware.

**Human Operated Ransomware**  *[b4/p5]* Class of ransomware attacks where the adversary penetrates the network and tailors their operation to the victim.

# Ii

**Identify Milestones** *[b4/p48]* Analytical conclusions should always be regarded as tentative. Changes cause re-evaluation.

**Illusory Correlation**  *[b4/p32]* Tendency to observe a correlation between two observations when no such correlation exists.

**Indicator Fatigue** *[b1/p73]* Value of rate of indicator creation and the use of intelligence over the SIEM and other automated processes.

**Indicator Life Cycle** *[b2/p77]* Revealed -> Mature -> Utilized

**Indicators**  *[b1/p66]* Data + Context = Indicator

**InfoGo** *[b3/p74]* Identifies registration info, subdomains, and emails based off of a domain or email address.

**Infrastructure** *[b2/p34]* Physical and logical mechanisms used to employ a capability is infra.

**Injecting New Analysis Approaches**  *[b4/p51]* Analysts all respond differently to different types methods of analysis.

**Installation**  *[b2/p19]* Where persistence is initially established on the victim/target machine. How files are placed, processes invocation, etc.

**Intel Gain/Loss**  *[b2/p49]* Feasibility of gaining intelligence or taking action against an adversary. risk/reward

**Intelligence Definition**  *[b1/p18]* Intelligence is the collection, processing, and analysis of information. Intelligence is both a product and a process.

**Intelligence Requirements** *[b1/p56]* A request to satisfy a knowledge gap about the threat or the operational environment.

**Intelligence Sources**  *[b1/p20]* HUMIT, GEOINT, MASINT, SIGINT, OSINT

**Intelligence-Driven Hypothesis** *[b4/p64]* Utilization of intelligence to drive the creation of hypothesis to include internal/external reporting & collection.

**Intent** *[b5/p109]* Impact != Intent. your analysis will give you a perception of intent but not the actual.

**Intrusions**  *[b1/p57]* Any attempt, successful or failed, that the adversary makes to comp0romise or attack systems.

**ISACs** *[b5/p39]* Information Sharing and Analysis Centers - sharing of threat info among civ and gov sectors.

**ISAOs** *[b5/p39]* Non-gov orgs to encourage private community sharing.

# Jj

**Judgment** *[b1/p27]* Analytical judgment is made to meet a specific intelligence requirement and has multiple factors.

# Kk

**Key Indicators** *[b1/p70]* Criteria for important indicators for an incident.

**Kill Chain Overview** *[b2/p6]* CTI model created by Lockheed martin has 7 stages.

**Know the Audience**  *[b5/p12]* This is the key to sharing threat intelligence - know your audience.

**Know Thy Team** *[b4/p51]* Learn your team members analysis types. Play to the teams strengths.

**Know Thyself**  *[b4/p51]* Everyone has a favorite type of analysis for given situations.

# Ll

**Legitimate Compromise Domains** *[b3/p43]* Likely to bypass network/human sensors. Modification or additions of new dns records.

**Life Cycle**  *[b1/p38]* Model used to structure intelligence efforts in a repeatable and scientific manner.

**Life Cycle (Indicators)** *[b1/p67]* How indicators beget indicators.

**Link Analysis** *[b4/p52]* Analysis of relationships between data points.

**Link Analysis Tools**  *[b4/p53]* Maltego/CaseFile, IBM Analyst Notebook, Palantir, Centrifuge, Gephi, Neo4J, Titan, Linkurious, Keylines.

**Logical Fallacies** *[b4/p23]* A flaw in reason including anecdotal fallacy/appeal to probability. These occur when arguments do not logically make sense.

**Logrotate**  *[b2/p61]* Service included in Linux for managing retention of system logs without interrupting processes writing to files.

# Mm

**Maltego**  *[b3/p107]* Link analysis tool that allows analysts to establish and define relationships between "nodes".

**Malware (Collection Source)** *[b3/p11]* Malware is the adversary's tool to operate in the environment and achieve their objectives.

**Malware Information Sharing Platform (MISP)** *[b4/p15]* Open source intelligence sharing platform that has a focus on automation.

**Mental Models** *[b1/p35]* Experience based assumptions and expectations on how the world operates.

**Metrics** *[b5/p49]* 2 Types: Organizational (Operational efficiency, Workload) & Risk (Threat)

**Middle Ground** *[b4/p25]* Making a compromise between two points an accepted truth.

**Mindmup** *[b1/p43]* Tool to brainstorm and build maps and relationship connections.

**Mirror Image** *[b4/p27]* Fooling ourselves into believing that the entity we are analyzing would behave in a way to what we would expect.

**Mitigation Scorecard** *[b5/p55]* Includes passive courses of action, mitigation capabilities and arch decisions, proposed changes, new tech, etc.

**MITRE ATT&CK** *[b2/p50 ]* Documentation of tactics and techniques.

**Moonlight Maze**  *[b1/p11]* Russian intrusion campaign targeting us military and gov networks starting in 1996.

# Nn

**Naming (Campaigns)** *[b4/p69]* DO: uses names inspired by incidents, obscure name inspiration, use humor. DONT: name after tools, use attribution, name after the incident.

**National-Level Government Info** *[b5/p38]* Sources: Criminal Investigations, Public/Private Partnerships, Foreign Intelligence

**Neodymium** *[b1/p75]* Activity group targeting specific individuals in Turkey.

**Network Flow Data** *[b2/p67]* Collection of the flow of packets across a network with applied schemes depending on tool use.

# Oo

**Observation vs Interpretations**  *[b5/p68]* Clearly separate facts, observables, evidence from interpretations and conclusions.

**One-to-One Mapping** *[b4/p73]* Intrusions are unique to organizations using other definitions and reporting without naming yourself is a mistake.

**Open-source Intelligence**  *[b3/p66]* Data exclusively from publicly available information.

**Operation Aurora** *[b1/p46]* Campaign targeting google in 2010. Links between separate campaigns were detected due to reuse of indicators and behaviors.

**Operation Bodyguard** *[b1/p22]* Passive/Active counterintelligence operation by the allies to counter German intelligence efforts on D-Day.

**Operational Threat Intelligence**  *[b5/p35]* Operational threat intel is the focus for operational level audience members. Usually surrounds what the "defender" needs.

**Opportunity** *[b5/p113]* Availability of means to accomplish objectives. May be technical political or logistical.

# Pp

**Panama Papers**  *[b4/p59]* Largest information leak in history of orgs avoiding taxes, sanctions, laundering money, and making shady deals.

**Passive DNS** *[b3/p47]* Collection of DNS domain query responses passively. Better vantage point = more verbose information.

**Pattern Recognition**  *[b1/p30]* Matching of information for external sources to long term memory.

**Peer to Peer (TAXI)** *[b5/p43]* Multiple orgs can produce data and multiple orgs can consume data.

**Penguin Turla**  *[b1/p14]* Toolkit spawned from LOKI2 that has overlap with Moonlight Maze

**Perception** *[b1/p29]* Not a passive process but something we can train a strive to be aware of when conducting analysis.

**Pivoting** *[b2/p76]* Using indicators to beget other indicators by process of analysis.

**PlugX** *[b5/p5]* Chinese based malware that propagated to multiple threat groups.

**Poison Hurricane** *[b3/p44]* Campaign where legitimate services were popped and DNS records changed for use in intrusions.

**Prioritize the Hypothesis**  *[b4/p45]* Hypothesis in the matrix are considered for its relative likelihood based on the evidence presented.

**Priority Intelligence Requirements (PIR)** *[b1/p95]* Requirements that are key to the mission of the organization. Paramount to mission success.

**Promethium**  *[b1/p75]* Activity group targeting specific individuals in Turkey.

**Prototype Matching** *[b1/p30]* Not exact matching but an average of similar templates to provide flexibility and a wider net during analysis.

**Proxy Logs** *[b2/p70]* Log format called squid is used to extend capabilities beyond caching and http optimization. 80/443 traffic capture and filtering.

**Publicity**  *[b1/p15]* Publicity degrades visibility in ongoing investigations vs. publicity increases visibility in historic investigations

**Pyramid of Pain**  *[b1/p90]* Model by David Bianco showing how much pain is caused to the adversary by burning intel.

# Rr

**Recon & Precursors**  *[b2/p8]* Preparatory steps to an intrusion including tasking, acquisition, identification, and research.

**Refine the Matrix** *[b4/p44]* Remove non-diagnostic evidence, add overlooked evidence now applicable, include formulation of new hypothesis, document evidence excluded.

**Report Conclusions**  *[b4/p47]* Hypotheses considered, key evidence, proper estimative language.

**Retiring Clusters** *[b4/p91]* States of Campaigns: Active, Inactive, Dormant. Keep all info for clusters indefinitely.

**Richard J. Heuer Jr.** *[b1/p25]* Veteran, CIA, Author of "Psychology of Intelligence Analysis", Overcoming bias.

**Rosetta Stone** *[b4/p72]* Mapping of known attribution, campaign names, and malware used by Groups. Loose correlation due to 1:1 mapping.

**Rule of 2** *[b4/p89]* Looking for overlaps between two vertices in intrusions or campaigns.

**Ryuk** *[b4/p8]* Trickbot -> emotet -> ryuk ransomware. Use of open-source tools is prevalent in this attack chain.

# Ss

**Scale of Cybersecurity**  *[b1/p81]* Framework developed to track impact to cost for levels of security function in an organization.

**School of Thought** *[b1/p8]* A perspective of a group with common opinions and disciplines.

**Sharing Best Practices** *[b5/p46]* Ensure auth/logging, references/appendixes, strip out unneeded data, use standards, interface.

**Sherman Kent**  *[b1 /p23]* Yale professor, Cold war CIA agent, Father of intel analysis, Author of "Strategic Intelligence for American World Policy"

**Sherman Kent Analytic Doctrine** *[b1/p24]* Ten step process kent created to structure intelligence efforts for communication/judgment.

**Sorting**  *[b1/p42]* Capture of data to sort and view in different ways usually leads to pivot points.

**Source/Subscriber (TAXI)** *[b5/p43]* Source determines what is available to the subscribers.

**STIX** *[b5/p41]* Describes threat info including IOCs and provides a common format for sharing across orgs.

**STIX Objects**  *[b5/p44]* Examples: Indictor, Tool, Note, Course of Action, etc.

**Storage Best Practices**  *[b4/p18]* Make a common format, make the method scalable, make the method secure, make the method shareable.

**Storage of Intelligence** *[b4/p13]* Ability to store collected information in an environment while making it available historically and adhoc for analysis.

**Storage Platforms**  *[b4/p14]* Pro/Cons of both open source and closed source storage platforms.

**Strategic Threat Intelligence** *[b5/p62]* Audience is strategic level decision makers. Usually the most polished data and focused on policy outcomes.

**Structured Analytic Techniques (SAT)** *[b1/p37]* Approaches to better evaluate information while reducing the impact of bias. 6 families 8 techniques

**Structured Models** *[b1/p36]* Lockheed Killchain, MITRE Attack, Diamond Model - puts things in buckets to allow communication between intel and others.

**Style Guide**  *[b4/p68]* Formalization of anything that is useful in a mid/long term context for progression of the intel teams function.

**Support the Hypotheses** *[b4/p42]* Seek additional evidence, include deductions/assumptions, discuss missing evidence.

**Synthesis** *[b1/p26]* Combination of ideas to form a theory or system.

**System 1 & 2 Thinking** *[b1/p34]* System 1 = Intuitive Thinking/Fast/Historical knowledge System 2 = Analytic Thinking/Slow/Scientific Method

**Systems Analysis** *[b1/p118]* Orderly grouping of interdependent components linked together according to a plan to achieve a specific goal.

# Tt

**TAXII** *[b5/p39]* Standard for much of the gov sharing that takes place. How to share the data.

**Team Structure**  *[b1/p98]* Centralization and graphic depicting intelligence function in relation to teams.

**Template Matching** *[b1/p30]* Templates are models stored in long term mem. Perception and interpretation are part of templates.

**Temporal Data Analysis**  *[b4/p56]* Analysis of data over time.

**Terminology**  *[b1/p53]* List of common words and concepts used in CTI.

**Threat** *[b1/p55]* Intent + Opportunity + Capability = Threat

**Threat Actor** *[b1/p59]* Cluster of intrusions representing "who" is responsible.

**Threat Data Feeds** *[b3/p68]* Feeds with IOCs to be vetted and analyzed for use in security tooling or intelligence efforts.

**Threat Intelligence Quotient (TIQ)** *[b3/p69]* Open source resource for evaluating your own threat feeds.

**Threat Modeling**  *[b1/p119]* Allows prioritization of security efforts by depicting issues and targeting of malware, groups, etc.

**Time Card System** *[b2/p133]* System used for tracking time input by employees.

**TLS Certificates** *[b3/p93]* Digital certificate used in secure host-to-host network communications.

**Top-down Analysis** *[b1 /p31]* Pattern matching using previous knowledge to filling the gaps when complete information is not available.

**Tradecraft** *[b1/p64]* Refers to the way the adversary achieves their success (M.O)

**Traffic Light Protocol** *[b1/p61]* RED, AMBER, GREEN, WHITE

**Trend Analysis** *[b4/p58]* Intelligence over time reveals patterns between intrusions.

**TTPs** *[b1/p63]* Tactics, Techniques, and Procedures

**Turkey Pipeline Explosion**  *[b4/p35]* 2008 explosion at the Baku-Tbilisi-Ceyhan pipeline.

# Uu

**Ukraine Power Grid**  *[b1/p101]* Power grid ICS attack on Ukraine Case Study.

# Vv

**VERIS**  *[b1/p127]* Framework that provides a common language for describing security incidents used by Verzion Data Breach report.

**Victim** *[b2/p35]* Recipient of capabilities.

**VirusTotal** *[b3/p19]* Malware dataset that is public and free to the community.

**Visual Communication of TTPs** *[b4/p10]* Intelligence that focuses on the visual aspect while providing value to the defenders/stakeholders of intelligence.

**Visualization**  *[b1/p37]* Capturing parts of a problem in an organized, often visual, manner to understand.

**Volatility** *[b2/p63]* Memory analysis tool cli and image based collection and analysis.

# Ww

**Wadhrama Attack Chain** *[b4/p6]* Good example of abstraction of technical detections to provide a new view on the kill chain.

**Weaponization**  *[b2/p12]* Process of brining together tools and infra needed for the mission.

**Working Memory**  *[b1/p30]* The system that processes inputs and determines whether or not they are important then encoding for mem type - short or long term.

# Yy

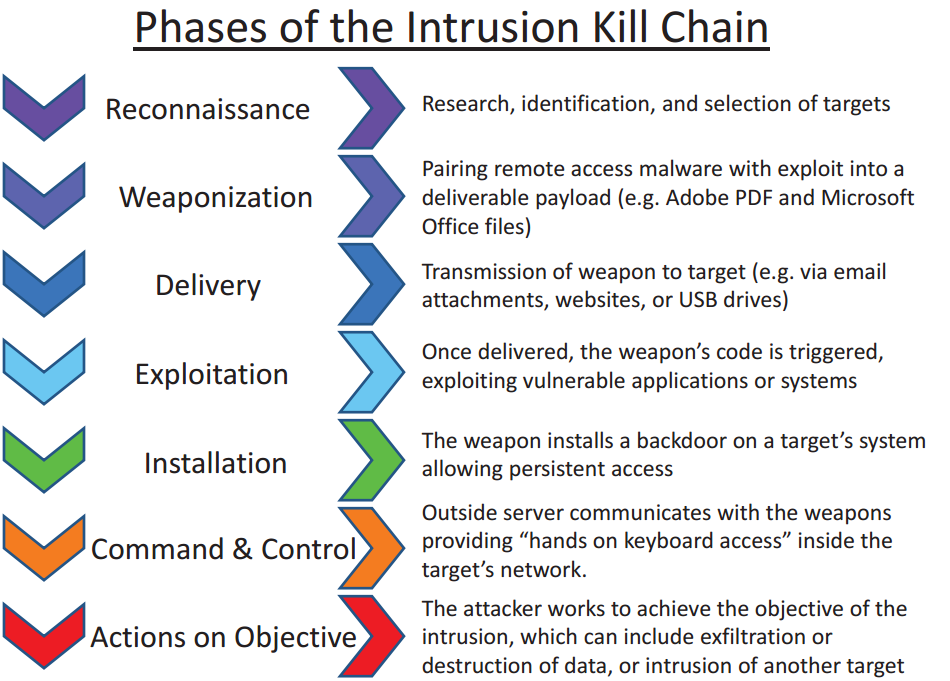
**YARA** *[b5/p13]* Pattern matching tool used to create signatures.

**YARA Strings** *[b5/p15]* Text, Hex, Regex

A picture containing line, diagram, text, plot

Description automatically generated

A picture containing text, screenshot, font, line

Description automatically generated

A picture containing text, screenshot, font, web page

Description automatically generated

