DRAGOS

Whitepaper

OPEN SOURCE INTELLIGENCE

DECEMBER 2020

By Casey Brooks & Selena Larson

DRAGOS, INC.

Intel@Dragos.com

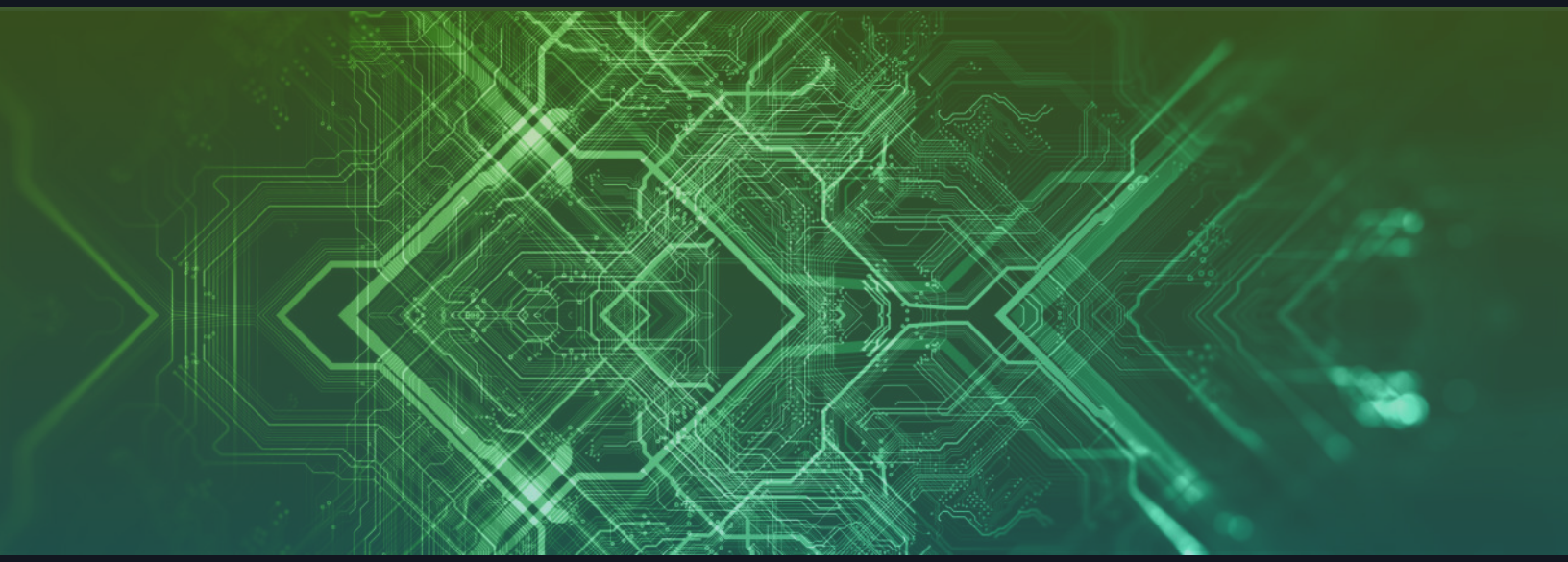
@DragosInc

EXECUTIVE SUMMARY

Publicly and semi-publicly available data, referred to as open source intelligence, can enable an adversary to develop targeting, identify access and ingress to a target, and understand how a target may respond to disruptive attacks on infrastructure. Adversaries who target Industrial Control Systems (ICS) for disruptive purposes seek open source information to plan and execute attacks that are different from adversaries targeting traditional enterprise resources. For example, Dragos observed adversaries conducting ICS-targeting activities that sought data about energy infrastructure and physical processes necessary to recover from a compromise. With this data, an adversary could target operational functions that are pertinent to recoverability to further the consequences of an attack.

Dragos created an Open Source Intelligence (OSINT) collection risk framework to help defenders better identify and restrict openly available information most valuable to adversaries intending to disrupt critical infrastructure. This framework helps prioritize countermeasures and mitigations to deny an adversary the opportunity to use OSINT collection against a victim.

TABLE OF CONTENTS



WHAT IS OPEN SOURCE INTELLIGENCE?

OSINT covers a wide variety of applications. Fundamentally, OSINT refers to the collection of publicly and semi-publicly available information that is used to inform multiple functions including intelligence gathering and reporting, business and policy analysis, and adversary attack development. For the purposes of this report, Dragos will focus on OSINT from a cyber threat intelligence perspective, with applications for Industrial Control System (ICS) asset owners, ICS operators, and adversaries.

Adversaries and defenders collect OSINT from a variety of sources. This is not an exhaustive list but demonstrates the types of publicly available information that could facilitate attack planning:

- Search engines
- Social media websites
- Job listings
- News websites
- Company websites
- Vendor websites and documentation including installation documentation containing default passwords
- Financial and legal resources such as 10-K filings or indictments
- Government and regulation authority body websites
- Reconnaissance tools such as Shodan[1] or Censys[2]
- Online scanning engines such as VirusTotal[3]
- Business solicitation portals such as VendorLink[4]
- Usernames and passwords in public repositories dumped by adversaries or stored in GitHub
- Using tools like the OSINT Framework[5]

1 https://www.shodan.io/
2 https://censys.io/
3 https://virustotal.com/
4 https://www.myvendorlink.com/common/default.aspx
5 https://osintframework.com/

KEY INFORMATION TYPES

Adversaries may seek multiple types of information in an attempt to conduct reconnaissance on a target and create a plan of attack. Identifying this information and educating company personnel on the potential risks of public exposure can enable defenders to proactively assess or remove potential information that can be weaponized.

The following definitions can help identify relevant and potentially exploitable information, based on the United States (U.S.) Department of Defense CARVER matrix, and assist in establishing risk language used in the OSINT framework.[6]

Personal/Personnel Information: Allows for identification of critical personnel, general personnel, or outside source personnel (e.g. contractors, third-party operators)

Example: LinkedIn profiles or construction contractors building a new facility for the target.

Criticality Information: Informs an adversary of the impact of an attack for a target's continued operations. A target's criticality is determined if its compromise or destruction has a highly significant impact in the overall organization and its ability to conduct business or operations.

Example: "Crown Jewels"[7] of operations, like safety controllers in oil and gas operations or data historians in manufacturing.

Accessibility Information: Informs the adversary of the ability or method to remotely/physically access or egress from a target.

Example: Remote Desktop Protocol (RDP) exposed to the internet.

Recoverability Information: Gives an adversary insight into the ability for a target's process, system, or network infrastructure to recover from an attack or compromise.

Example: Information about electric utility service restoration in the event of a disruptive event.

Vulnerability Information: Informs an adversary of a vulnerability that exists in the target's infrastructure, processes, or response actions.

Example: An unpatched vulnerability affecting Virtual Private Network (VPN) appliances that enables initial access.

Effect Information: Information about the amount of direct or indirect loss a target would have from an attack or compromise. Information on the effects that losses would have on the target, its organization, processes, or operations.

Example: Physical effects of a disruptive cyberattack targeting a Safety Instrumented System (SIS); financial losses accrued from multiple days of downtime.

Recognizability Information: Assists adversaries in the ease of identifying targets for operational gain and the level of obscurity that the target has from internal and external sources.

Example: MAC address of target workstation within the ICS.

6 https://en.wikipedia.org/wiki/CARVER_matrix

7 https://dragos.com/blog/industry-news/combating-cyber-attacks-with-consequence-driven-ics-cybersecurity/

TARGETING ICS

When mapped to the ICS Cyber Kill Chain,[8] OSINT largely represents Stage 1 reconnaissance activity that can support Stage 2 objectives. It can be used to identify potential vulnerabilities, identify detections, implement persistence mechanisms, or reduce the time required to achieve objectives and avoid detection. Details on equipment, vendors, and processes can be used for later malware or malicious tool development.

Adversaries target industrial entities for a variety of reasons. Attacks on ICS entities that serve critical functions within society can be used to further political, economic, or national security goals. Depending on an adversary's objective, attacks can be used for messaging purposes or retaliation. The potential impact may extend to citizens of a target's community. Understanding critical infrastructure can put an adversary at a tactical advantage in times of conflict to establish a foothold as a contingency option when conflict occurs.

Targeting ICS can provide monetary value to an adversary. ICS entities increasingly experience ransomware attacks that, in many cases, disrupt operations.[9] For some companies, disrupting operations can have significant daily financial impacts, costing thousands and sometimes millions of dollars in downtime. In these cases, an operator may be more willing to pay a ransom to unlock computers and limit downtime, especially if proper backups are not maintained. For example, in July 2020, wearables manufacturer and Global Positioning System (GPS) service provider Garmin experienced a ransomware attack and opted to pay an undisclosed ransom to get its operations back online.[10]

ICS environments may also be more insecure than traditional enterprise systems, especially for entities with immature cybersecurity postures. This can be due to legacy operating systems in use across various environments and inadequate segmentation. It is not uncommon to observe outdated Windows operating systems, such as Windows XP or Windows 7, within ICS due to interoperability of some ICS devices and limitations on patch management. ICS systems are fundamentally complex, and security mechanisms like patching are conducted based on weighing the risk of compromise against the outcome of a potential cyberattack. Practicing defense in depth, including conducting OSINT risk assessments to strengthen external security postures and limiting the ability for adversaries to operationalize public information, can prevent initial access and movement within an operational environment.

8 https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

9 https://dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/

10 https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/

DEVELOPING AN OSINT SECURITY ASSESSMENT

By identifying and prioritizing data that could be used in OSINT collection, defenders can establish methods to reduce the availability of potentially high-risk company and user data and limit the information an adversary can use in a potential attack.

Scope the Scenarios

Defenders should begin by scoping multiple scenarios and potential for attacks. These can be identified from examples of known cyberattacks, results of tabletop exercises and red team activities, and scenarios developed by internal security teams. The goal of this step is to identify the type of adversary or attack that defenders try to prevent.

Dragos advises leveraging consequence-driven security assessments to identify adversary objectives and how to combat them. The Dragos Crown Jewel Analysis model of consequence-driven ICS cybersecurity scoping helps defenders visualize how an adversary would access the system to achieve a specific consequence[11]. By identifying assets within the system and the functional outputs and dependencies, the level of exposure, and interaction between each network layer, organizations can visualize how an adversary may achieve a specific consequence by targeting different elements within the system.

Collaborate Across the Company

It is important that OSINT assessments leverage experience and data across multiple teams. Security operators and network technicians from Information Technology (IT), incident responders and forensic specialists, security operators and engineers from ICS environments, and physical security specialists should be consulted while conducting the assessment. These individuals can provide insight on the value of information from an adversary perspective and how OSINT can enable potential attack scenarios. Additionally, business units including human resources and legal should also be consulted to identify publicly available information and the requirements or policy functions the information serves.

Detail the System and Network

A detailed map of the network should be developed and maintained to visually describe where information is hosted, stored, and maintained via system diagrams, flow charts, or network maps. The map should also detail context of the information hosted. For example, when evaluating a web portal that hosts contractor information and third-party network access, the content of the information hosted should be as detailed as the technical specifications of the actual hosting server. The quality and quantity of useful data should be noted and assessed if additional intelligence can be generated from it in aggregate.

Identify Sources and Collect Information

Source identification is an important step in the collection process. Defenders can use the resources described above to find relevant, publicly available information. However, sources will vary for individual companies. Asset owners and operators should also consider information exposed by third-party entities that could be used in reconnaissance operations. For example, a vendor may publish case studies or press releases describing how customers implement specific products or services within their operations environment, which could provide adversary insight into what technologies are used in a target environment.

Information collection should focus on publicly available information that could be used to facilitate reconnaissance or attack development. This includes information about vendors and partners; documents, schematics, and data sheets; job advertisements; information about system operations and recovery processes; geographic data like maps detailing plant locations; ports and services identified via Shodan; and credentials in public dumps. Security teams should also identify gaps in security architecture, like remote login portals that lack strong passwords and multi-factor authentication including RDP and VPN services.

11 https://dragos.com/wp-content/uploads/ConsequenceDrivenICSCybersecurity-Scoping_Dragos.pdf

Conduct Analysis and Risk Assessment

Once data is collected, users should determine how an adversary may operationalize data to achieve objectives outlined in potential attack scenarios. Data should be assigned severity scores on the risk that data poses to the organization, based on the matrix in Figure 1. For example, information that could facilitate initial access and is easily accessible to the adversary should be assigned a higher score compared to information that does not enable an adversary to fulfill an attack objective and is difficult to obtain.

Example: A piece of information (e.g. error logs, system headers, etc.) describes a server running a vulnerable piece of software, but it is unknown how or if the adversary uses the information. The information is highly accessible and recognizable, and likely easy for the adversary to use. In combination with other collection by an adversary, this software vulnerability information has a higher score than just the individual piece of information.

OSINT Collection and Risk Scoring Matrix

To enable asset owners and operators to better understand the risk that openly collected information poses to an organization, Dragos developed the OSINT Collection and Risk Scoring Matrix. With this matrix, users can quickly apply scores to identified information and the risk of an adversary operationalizing it against them.

The data is rated from one to three and by color, including green, orange, and red. The higher the number, the greater the value of the OSINT to an adversary. Green indicates a low value item and red indicates a high value item. The colors help an analyst determine how to quickly prioritize remediation and defense. This is explained in the Priorities of Defense and Mitigation section below.

OSINT Collection Risk and Vulnerability Matrix	Information is of Low Relevance/Importance for Intelligence Collection	Information is of Medium Relevance/Importance for Intelligence Collection	Information is of High Relevance/Importance for Intelligence Collection
Adversary utilization requires little to no analytical effort for operational integration	2	3	3
Adversary utilization requires moderate to specialized analytical effort for operational integration	1	2	3
Adversary utilization requires highly technical analytical effort for operational integration	1	2	2

Figure 1: OSINT Collection and Risk Scoring Matrix

Example: An OSINT assessment identified a document containing engineering diagrams of an oil production facility. The document included device type and implementation information of safety systems and integration of Enterprise Resource Planning (ERP) software. This document was found in a vendor Request for Proposal (RFP) repository.

This document is scored as a 3 and is of high value and relevance to an adversary interested in infiltrating or disrupting operations. It requires specialized analytical effort for intelligence value for an adversary. This means to use information from this document, an adversary must establish knowledge of the ICS environment, devices, and software used.

Example: An OSINT assessment of 10-K financial filings identified an automotive manufacturing organization working with Accounting Firm X to facilitate the acquisition of an additive manufacturing startup. A LinkedIn search identified the name of the accountant at Accounting Firm X likely working on this acquisition.

This information is scored a 2. The adversary requires moderate analytical effort to operationalize this data, and it would be straightforward to create phishing lures based on the information identified. The adversary requires additional access, like to the accountant's email directly, to launch a likely successful phishing attack. This information is also of low importance for intelligence collection because it is only tangentially related to the target organization.

Priorities of Defense and Mitigation

As information is assessed and scores assigned, defenders can leverage the Priorities of Defense and Mitigation (PODAM) table to visualize how collected data could be operationalized, the value of the information, and if protections and mitigations are in place to address the potential risk.

The PODAM table used to assess OSINT collection contains multiple examples and potential use cases for operationalizing OSINT including target identification, exploitation, infrastructure development, delivery, capabilities development, and actions on the objective. The importance of each piece of information is designated by color, like Figure 1 above. Different characters represent the ability for an entity to mitigate the potential risk, and if risk mitigation is an issue of policy or prioritization.

The table is an example of how an analyst can determine the priorities of defense and mitigation based on open source data collected. The legend icons represent requirements and the ability for the company to implement defensive measures to prevent exploitation of the data, what actions should take priority, if a network policy configuration is required to fix, and if data came from threat intelligence reporting. The colors represent the value of the intelligence gathered to adversary operations.

Example: An analyst collects three different types of information: the location of facilities, names and emails of engineers, and vendor names and contract information of companies they work with. An adversary uses this information in different ways for targeting, exploitation, and infrastructure development operations. An analyst must identify how it may be used, the importance of the data based on the Risk Scoring Matrix above, and if the organization has adequate visibility, defensive measures, and security policies in place to prevent exploitation of the information. The analyst completes the table as provided in the example below.

Analyst Note: A full list of definitions detailing the data types and how information can be used is available in the appendix. An empty PODAM worksheet is also provided in the appendix for use in security operations.

ADVERSARY OSINT COLLECTION PODAM																															
		Target Identification			Exploitation			Infrastructure Development					Delivery						Capabilities Development									Actions on the Objective				
Information Collected ID	Utilization	Personnel	Technology	Organizational	Vulnerability	Social Engineering	Supply Chain	Domain Spoof	Legitimate Compromise	Vendor Supply Chain	Establishment	Staging	Phishing	Watering Hole	Downloader/Dropper	Credential Capture	Legitimate Access	Authentication Bypass	Research & Development	Automation	Evasion	Obfuscation	Installation	Environment Awareness	Weaponization	Interactive Operations	Command and Control	Persistence	Maneuver	Cyber Key Terrain
Geographic Locations of Entities	Targeting			$																									x	
Names and Emails of Engineers	Targeting, Exploitation	$					o										\ o	\											x	
Vendor Names and Contracts	Targeting, Infrastructure Development, Exploitation	$	$	$			o			o							\ o	\												

Legend					
High Target Importance		X	Defense Capability Gap	*	Intelligence Data
Medium Target Importance		O	Missing Dependencies	$	Policy Issue
Low Target Importance		\	Requires Implementation		
N/A					

Table 1: Sample Adversary OSINT Collection PODAM

By using this table, an analyst can determine the highest priority items to address. In this case it is publicly available vendor names and contracts. The following are recommended steps for remediation plans to begin addressing the issues:

- Remove sensitive information from public sources where applicable.
- Conduct an assessment of third-party and vendor integrations within the operations environment.
- Ensure third-party connections are properly secure with access restrictions, Multi-Factor Authentication (MFA), segmentation, and defense in depth measures.
- Work with vendors and contractors to identify and acknowledge maintenance and related operations in advance to determine schedules and baseline legitimate activity.

OSINT Collection Mitigation and Vulnerability Remediation

Once defense and mitigation priorities are established, users should identify corrective actions to prevent or lower the risk of adversaries exploiting vulnerabilities or operationalizing information identified in the previous stages of the assessment. These can include issuing patches to vulnerable hardware and applications, removing sensitive data from public websites or databases, implementing MFA to access documentation on cloud storage systems, and changing default passwords on devices within the ICS.

Users should conduct this section of the assessment in two parts: one for hardware and physical systems and the other for software and user policies. Each assessment should include a description of the vulnerability or issue identified, how the company can correct it, and the resources required to do so. The assessment should include any potential obstacles that prevent the company from implementing the recommended fixes.

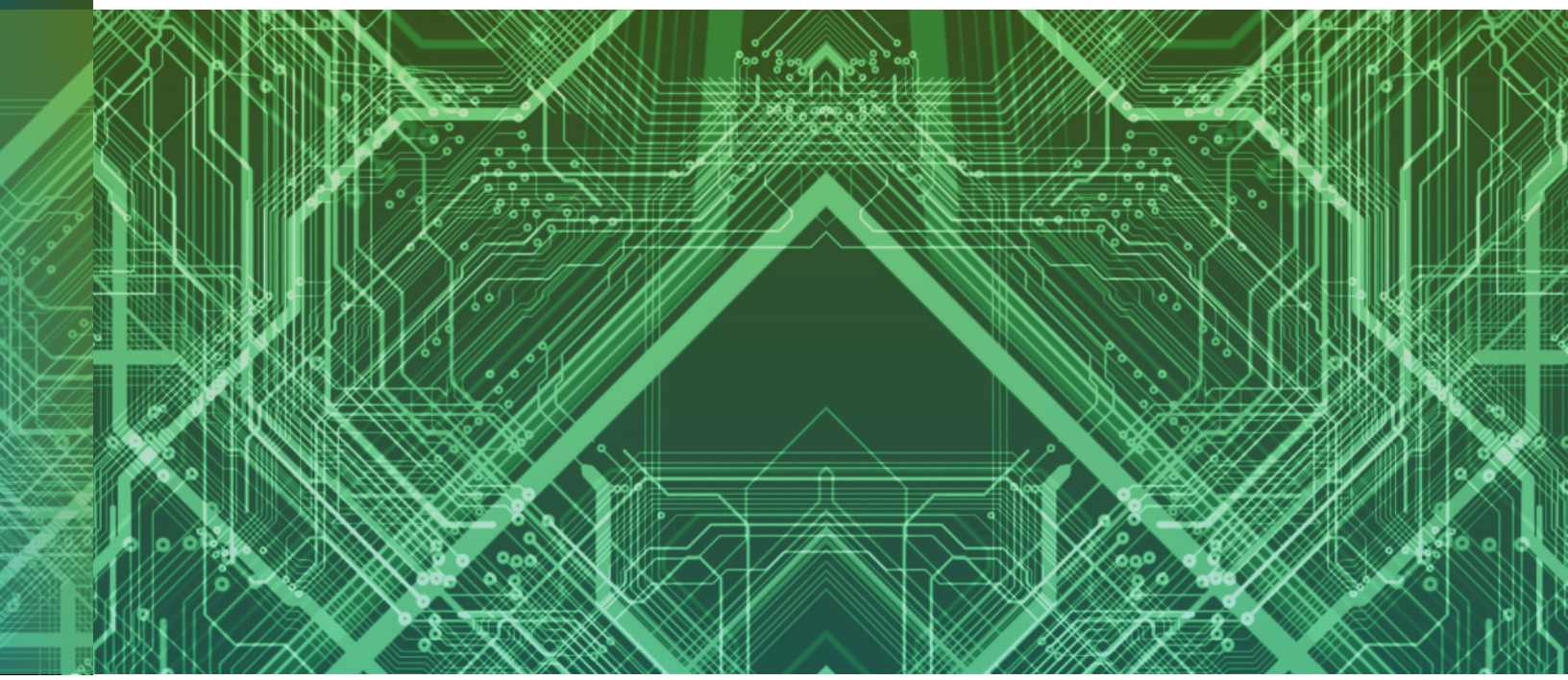
To illustrate the potential risk the vulnerabilities or information pose to an organization, defenders are encouraged to leverage threat intelligence reporting that provides examples of adversaries operationalizing identified issues and consequences of activities.

Regardless of the issues identified, all mitigation efforts should include defense in depth approaches to prevent a single point of failure within the system or network. Visibility of assets is crucial to implement effective defense in depth approaches to establish barriers to entry, secure or restrict communications between assets, and identify anomalous behaviors. This requires a complete view of an organization's assets.

Taking Action

Based on the information gathered and the assessed risk to the organization, users should implement remediation plans that focus on the most critical to least critical information for adversary operationalization. Plans should be documented and include realistic timelines required to address issues and identify the entity responsible for addressing, removing, or correcting information and vulnerabilities.

Once an assessment is completed, the results should be shared across teams. This includes entities like human resources, who may need to alter job descriptions based on feedback, and public policy teams, who regularly share publicly accessible data with regulators, municipal, state, and federal agencies.



CONCLUSION

Conducting regular OSINT collection risk assessments as part of quarterly or bi-annually scheduled cybersecurity reviews can improve an organization's defense against adversary operationalization of publicly available information and exploitation of known vulnerabilities. By following the framework introduced above, defenders can better identify potential risk to an organization, understand the risk of publicly exposed data, and create mitigation strategies that effectively reduce risk.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT WWW.DRAGOS.COM.

APPENDIX

Definitions

The following definitions describe the various types of information associated with the PODAM.

Personnel - Individual people who have an OSINT footprint. This can help an adversary identify targets that could be a likely source for access and exploitation.

Technology - Information about specific technology that is present in the defended environment. This information can come from personnel profiles, job listings, or fingerprinting by the adversary.

Organizational - Information about the organization's physical location, partnerships, business details, etc. that can be used to develop targeting.

Vulnerability - A vulnerability existing in a business or operational process that informs an adversary for a likely avenue of exploitation.

Social Engineering - A method used to trick a user to activate or download a delivered capability, or to provide information to the adversary as a trusted party.

Supply Chain - An entity or entities that enable the production or operation of a business process. It acts as an avenue into a victim environment via trusted channels or connections.

Domain Spoof - A tactic of establishing infrastructure that mimics or closely matches a trusted domain or entity infrastructure. This can be used for delivery, command and control, or for social engineering.

Legitimate Compromise - A tactic adversaries use to gain access to an indented victim by exploiting trust or the legitimate nature of another domain or organization. This is most often observed as a command and control point for interaction with a victim, avoiding the necessity of establishing and maintaining adversary created infrastructure.

Vendor Supply Chain - This informs an adversary of potential targets for legitimate compromises, crafting spoofing domains, supply chain compromise, or for information on trusted party relationships involved with business operations that can enable phishing opportunities.

Establishment - An adversary's operational process of creating infrastructure, developing and testing capabilities, and performing the initial planning stages for reconnaissance and targeting.

Staging - An adversary's operational process of preparing infrastructure and capabilities to act in unison for use in delivery, exploitation, or command and control functions. Staging can also be initiated when a part of infrastructure is transferred from inactive to active hosting.

Phishing - An adversary can use a combination of either adversary controlled or legitimate compromised infrastructure and phishing themes to lure victims into a false sense of security and evade scrutiny. This can often lead to having victims visit watering holes, avoiding immediate detection by security operations or technologies, and creating a trust relationship with the adversary sender.

Watering Hole - An adversary-controlled or legitimate but compromised domain that the adversary uses to lure victims to gather information, deliver capabilities, or collect credentials for legitimate access.

Downloader/Dropper - A capability that enables the delivery of additional capabilities without need of victim interaction.

Credential Capture - A method an adversary uses to collect legitimate credentials that enables access to targeted victim.

Legitimate Access - A method in which an adversary uses captured credentials, harvested credentials from OSINT information, or brute force authentication to achieve access as a trusted, legitimate user. This also occurs when an adversary is able to create user personas in a victim environment to allow for persistent access without relying on backdoors or other capabilities that enable illegitimate access.

Authentication Bypass - This technique involves finding infrastructure that allows for access behind an authentication

APPENDIX

control, but a vulnerability exists in either the technology or organizational process for access approval, or a valid user account was compromised to let an adversary bypass this authentication gate.

Research and Development - A business function that generates new information of value for an adversary or that contains intellectual property that is either not publicly available or patented.

Automation - A process that follows specific steps without manual or user interaction.

Evasion - A capability design, tactic, or technique taken by an adversary for avoiding detection by security infrastructure, technology, or defender manipulation.

Obfuscation - A capability design, tactic, or technique taken by an adversary to avoid scrutiny.

Installation - The process in which an adversary is able to load a capability into a victim environment and gain successful execution of the capability to allow for further access or continued interaction operations.

Environment Awareness - The ability for an adversary to determine where in the victim network they are located, identifying infrastructure for pivoting or information that better enables capability selection in compromise operations.

Weaponization - The activity performed by an adversary to take a vulnerability or benign software or documents and turn it into an operational capability that can lead to satisfying adversary intent.

Interactive Operations - The activity wherein the actor accesses the victim environment through manual means or performing offensive tasks without automation or the use of capabilities to achieve information collection, reconnaissance, persistence, or exfiltration.

Command and Control - The channels an adversary uses to direct its operations, enabling bi-directional communication of information.

Persistence - The method of maintaining access and command and control within a victim environment.

Maneuver - The method used to move within a victim environment.

Cyber Key Terrain - Infrastructure, processes (either business, technical, or personnel) or technology that is essential to the operational integrity, confidentiality, and availability of a network.

Defense Capability Gap - A gap in organizational structure, network architecture, cybersecurity, or user policies that would be required for defense against adversary exploitation.

Missing Dependency - A security feature or mechanism that enables a core security function but is not present within the environment.

Requires Implementation - A security feature or mechanism that is present within in an organization, but is not yet implemented, and is required for defense against adversary exploitation.

Intelligence Data - Information gleaned from threat intelligence data, either from a third-party or an organization's internal threat intelligence team.

Policy Issue - An item that requires a change in organizational or user policy to address.

		ADVERSARY OSINT COLLECTION PODAM																												
		Target Identification			Exploitation			Infrastructure Development					Delivery						Capabilities Development								Actions on the Objective			
Information Collected ID	Utilization	Personnel	Technology	Organizational	Vulnerability	Social Engineering	Supply Chain	Domain Spoof	Legitimate Compromise	Vendor Supply Chain	Establishment	Staging	Phishing	Watering Hole	Downloader/Dropper	Credential Capture	Legitimate Access	Authentication Bypass	Research & Development	Automation	Evasion	Obfuscation	Installation	Environment Awareness	Weaponization	Interactive Operations	Command and Control	Persistence	Maneuver	Cyber Key Terrain

Legend					
	High Target Importance	X	Defense Capability Gap	*	Intelligence Data
	Medium Target Importance	O	Missing Dependencies	$	Policy Issue
	Low Target Importance	\	Requires Implementation		
	N/A				