SHARE

Strategies for Gathering and Contextualizing Cyber Threat Intelligence

Sep 28 2022 | 4 min. read

By Allen Funkhouser

Request Demo

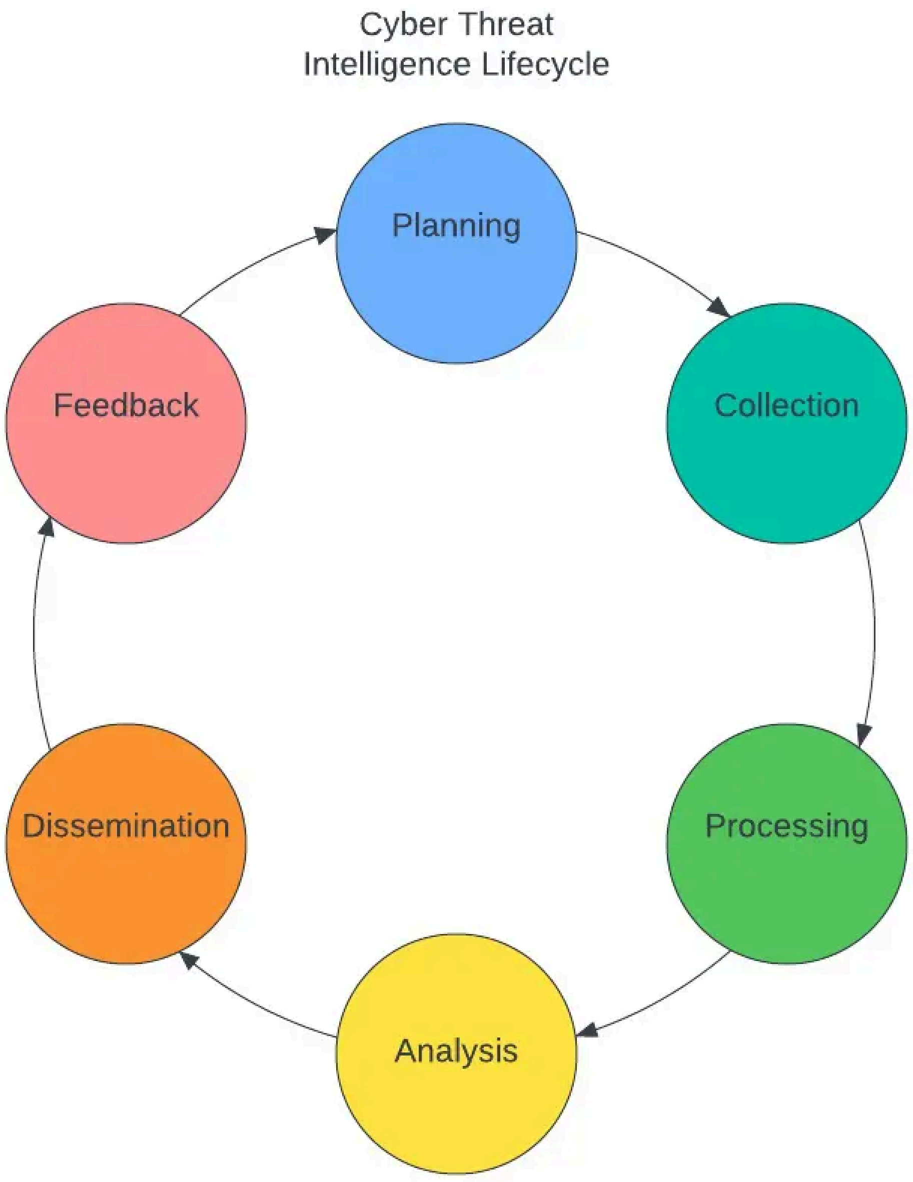
In my previous blog, I covered the many different types of cyber threat intelligence and why gathering CTI is beneficial to security teams. In this post, I will dig into the cyber threat intelligence lifecycle framework and a model to help correlate and contextualize your findings.

Cyber threat intelligence lifecycle

Performing cyber threat intelligence gathering should be approached with a method in mind. This is where the CTI lifecycle can help provide a framework for how to accomplish CTI. Similar to the scientific method, CTI can be broken into six phases, each with a specific goal to enhance either the CTI process or the information gathered while performing CTI.

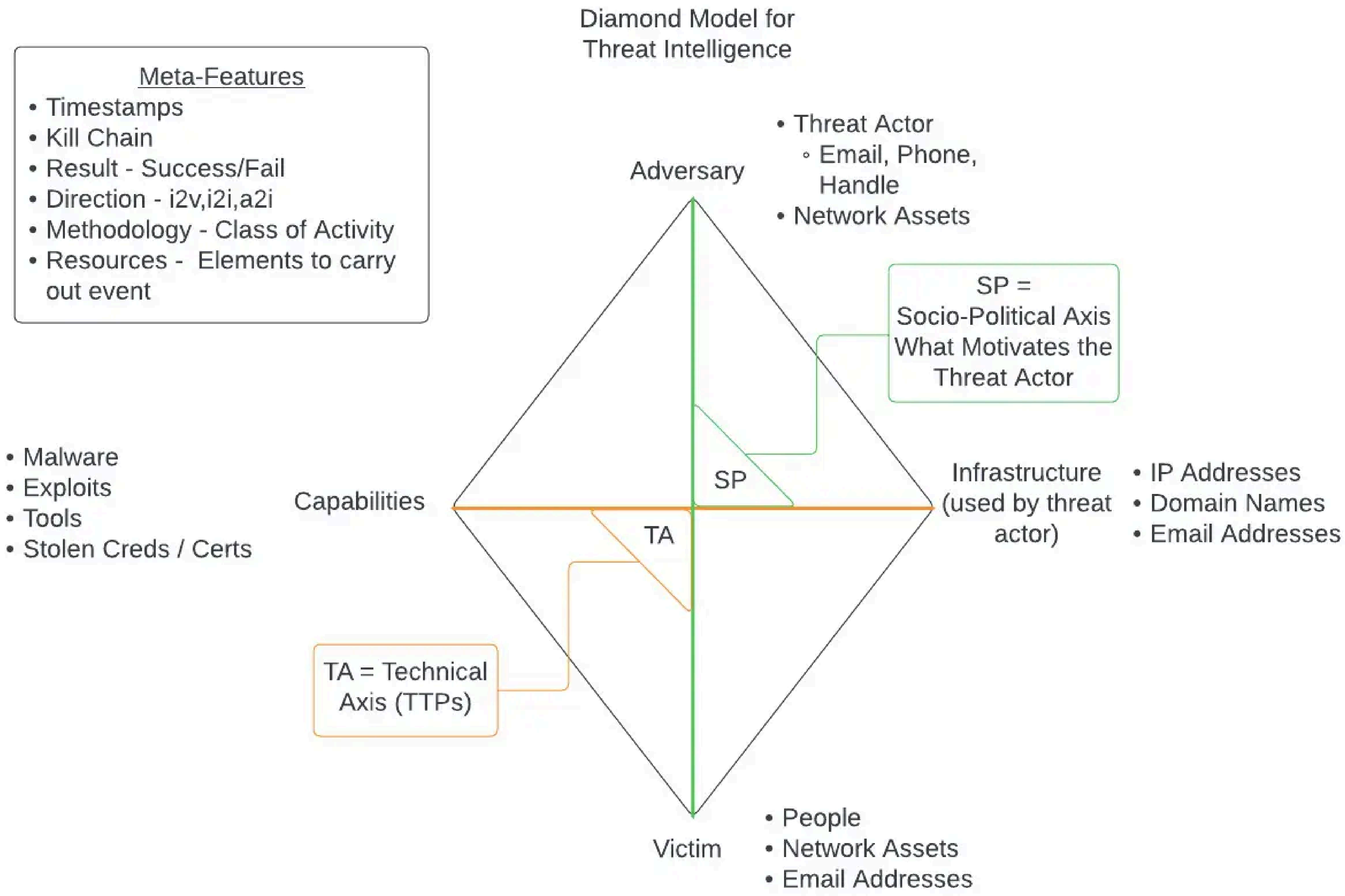
1. Planning – Set requirements, goals, and methods for intelligence gathering to answer a specific question.
2. Collection – The process of gathering information from sources.
3. Processing – Organizing information gathered in the Collection phase.
4. Analysis – Examining information to place relevance, priority, and potential actional items
5. Dissemination – Delivering information to the teams that can best utilize it.
6. Feedback – Asking did the information gathered answer the question, help or enhance a team's objective? What information does the team still need?

Here at Netskope one of the many ways teams utilize the CTI lifecycle, and multiple other intelligence gathering tools, is to feed data into the Netskope Cloud Threat Exchange platform, providing up-to-date threat intelligence, including IoCs. This way Netskope and Netskope customers can detect, alert, and block the latest threats. To start the process, the analyst plans to ingest accurate and relevant IoCs that are found in the wild. Collection then occurs with tools curating intelligence and the analyst building automation to go to the next stage of processing. Processing provides context through other threat intelligence gathered, such as threat actors and TPPs, along with the IoCs. In the Analysis phase, IoCs are enriched and then, depending on relevance, formatted to share with different teams. Dissemination is where these IoCs are then shared through intel channels built between teams in the format that works best for their objective. With Feedback regular team meetings ensure any gaps within the intelligence shared are discovered and a plan is formulated to fill these gaps.



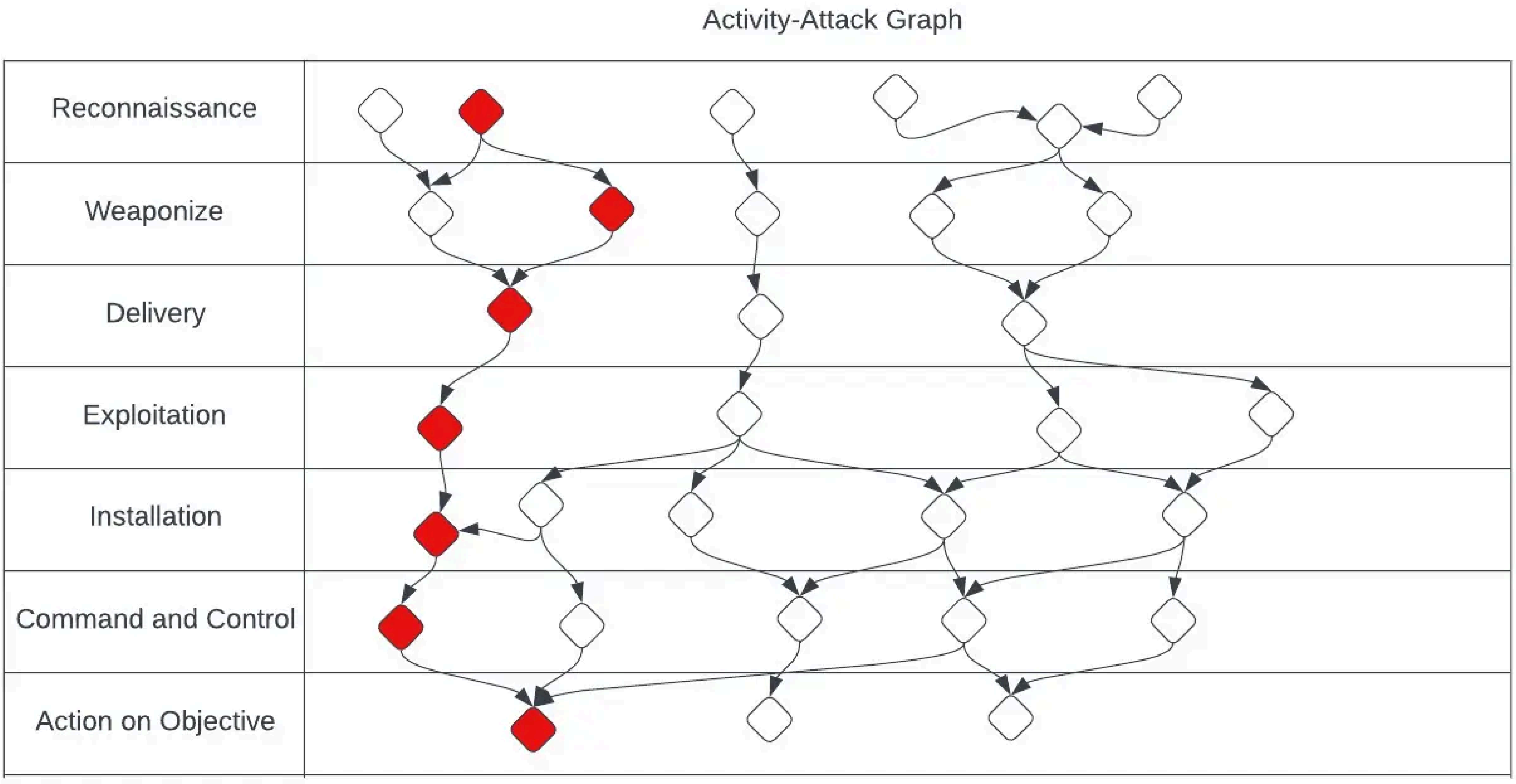
Diamond model

While it is important to have a process to methodize intelligence gathering, it is just as important to have a model that helps correlate and contextualize that information gathered. One such model that can help consumers of threat intelligence is the diamond model (pictured below).



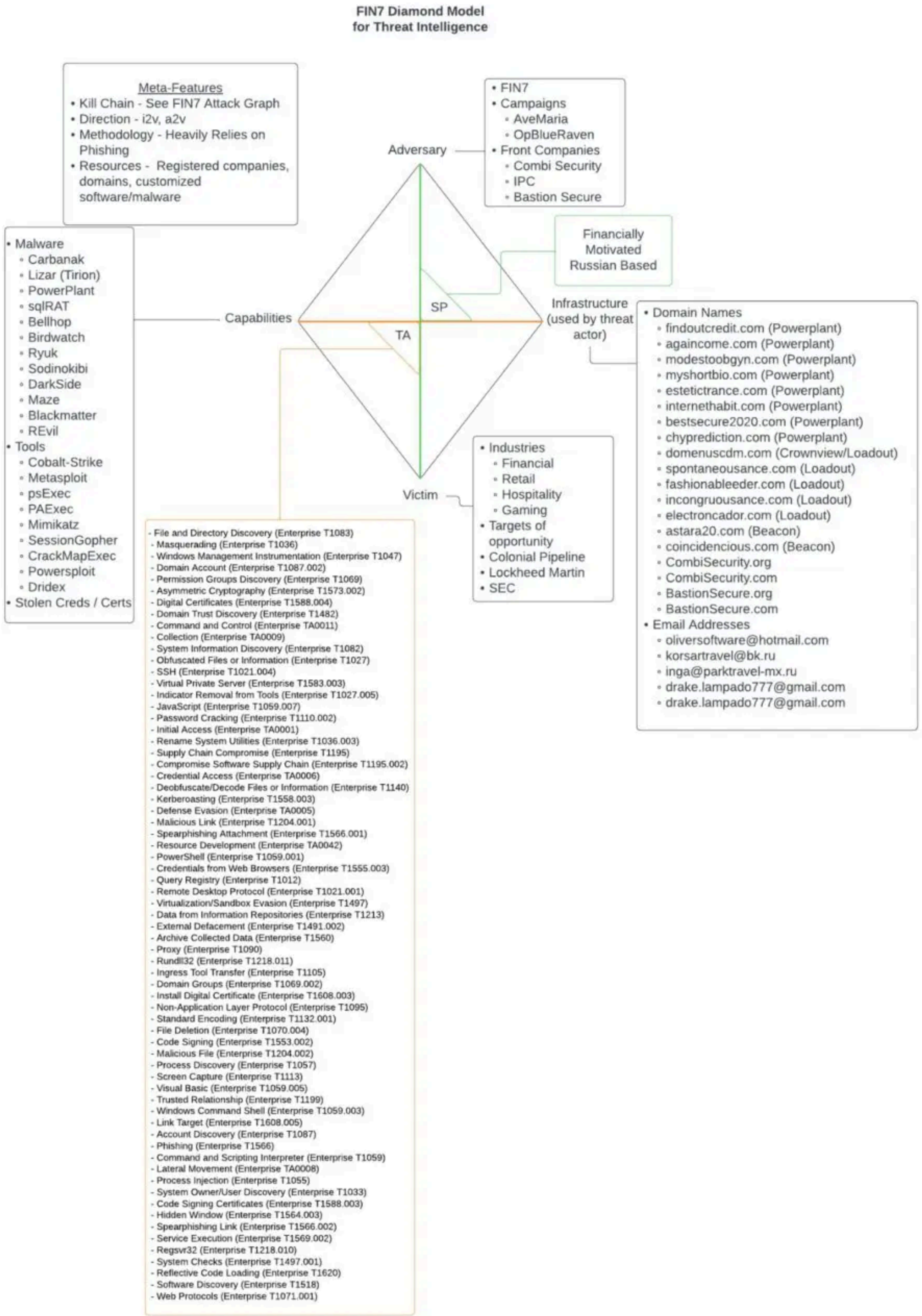
One important aspect of the diamond model for threat intelligence is that it allows analysts to easily pivot from one piece of intelligence to another, which helps either fulfill the full picture while gathering, or show blindspots in intelligence. The main focus of the model is to track adversaries, capabilities, infrastructure, and victims over time. This activity is shown through the use of an activity thread which correlates trends of attackers, TPPs, and infrastructure across attacks against multiple different victims. The activity thread is helpful in building out potential future paths threat actors could take, which allows defenders and responders to take a proactive approach to security and not reactive.

Another key aspect of the diamond model is the ability to form activity groups and activity-attack graphs. Activity groups are groupings of common identifying behavior such as particular APT activity or a common attack pathway used by threat actors signaling a specific type of attack. Activity-attack graphs are graphical representations of actual attacks occuring in the threat landscape along the cyber kill chain. This allows CTI analysts to track current activity in the threat landscape and correlate the MITRE ATT&CK TPPs to the cyber kill chain in order to formulate scenarios an organization may face. Using these attack graphs, security teams can formulate specific threat hunt scenarios and ensure their security stack protects against attacks found in the wild.

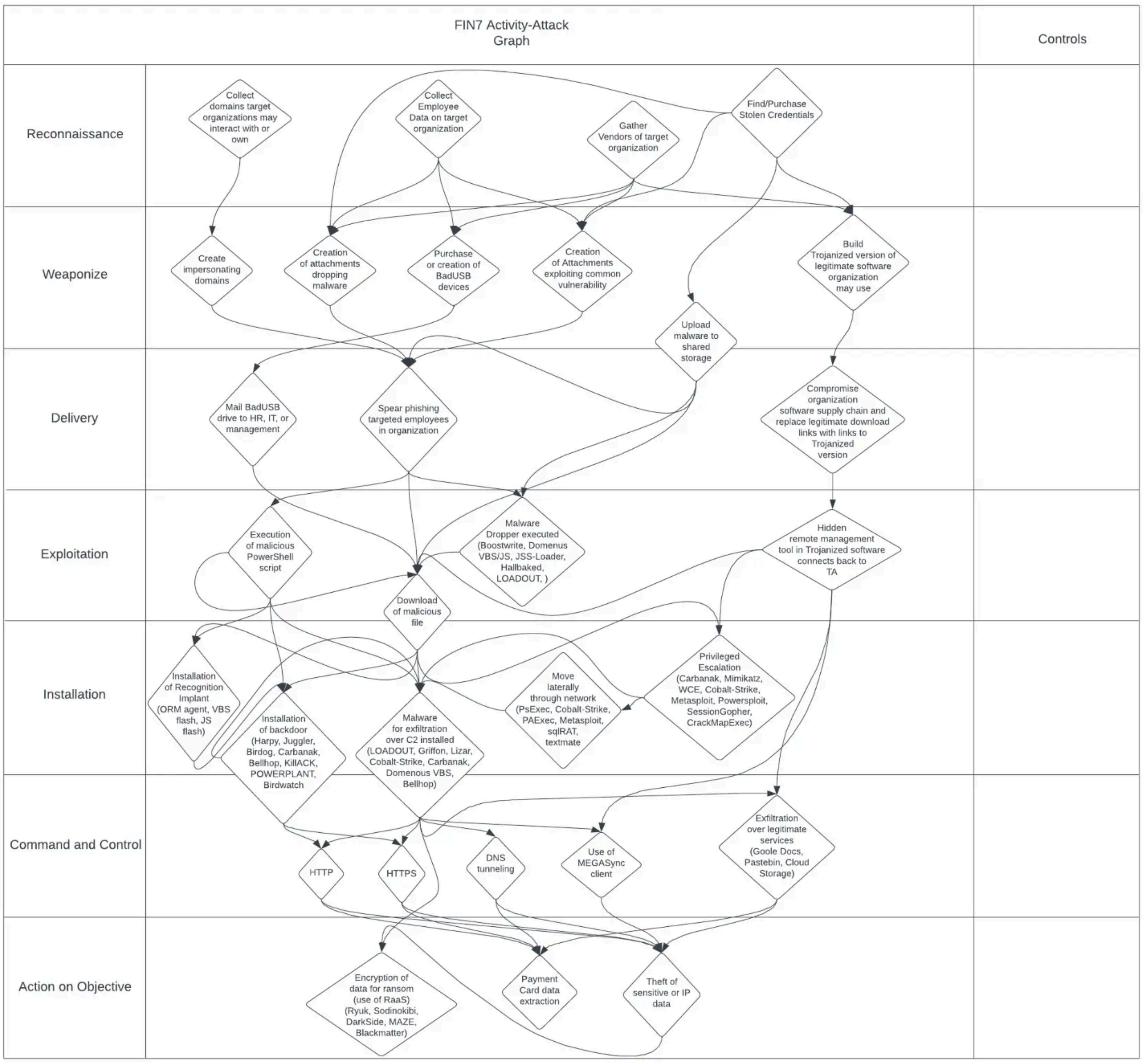


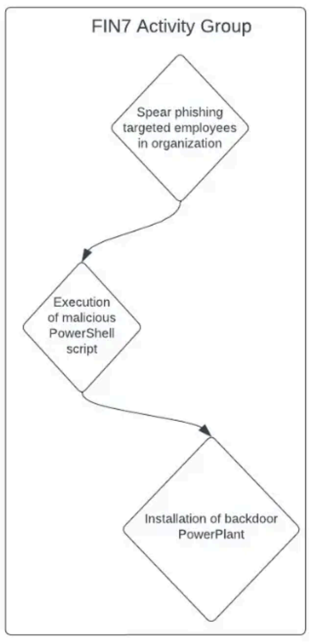
For more information on the diamond model and activity-attack graphs with the diamond model see the original paper by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz here.

Here the diamond model is used to put together intelligence on the threat actor FIN7. I started with formulating a diamond based on the known adversary and then doing a high-level analysis of capabilities, infrastructure, and victims of the threat actor's previous attacks.


FIN7 Diamond Model
for Threat Intelligence
Meta-Features
• Kill Chain - See FIN7 Attack Graph
• Direction - i2v, a2v
• Methodology - Heavily Relies on Phishing
• Resources - Registered companies, domains, customized software/malware
Adversary
• FIN7
• Campaigns
◦ AveMaria
◦ OpBlueRaven
• Front Companies
◦ Combi Security
◦ IPC
◦ Bastion Secure
Financially Motivated Russian Based
Capabilities
SP
TA
Infrastructure (used by threat actor)
Victim
• Malware
◦ Carbanak
◦ Lizar (Tirion)
◦ PowerPlant
◦ sqlRAT
◦ Bellhop
◦ Birdwatch
◦ Ryuk
◦ Sodinokibi
◦ DarkSide
◦ Maze
◦ Blackmatter
◦ REvil
• Tools
◦ Cobalt-Strike
◦ Metasploit
◦ psExec
◦ PAExec
◦ Mimikatz
◦ SessionGopher
◦ CrackMapExec
◦ Powersploit
◦ Dridex
• Stolen Creds / Certs
• Domain Names
◦ findoutcredit.com (Powerplant)
◦ againcome.com (Powerplant)
◦ modestoobgyn.com (Powerplant)
◦ myshortbio.com (Powerplant)
◦ estetictrance.com (Powerplant)
◦ internethabit.com (Powerplant)
◦ bestsecure2020.com (Powerplant)
◦ chyprediction.com (Powerplant)
◦ domenuscdm.com (Crownview/Loadout)
◦ spontaneousance.com (Loadout)
◦ fashionableeder.com (Loadout)
◦ incongruousance.com (Loadout)
◦ electroncador.com (Loadout)
◦ astara20.com (Beacon)
◦ coincidencious.com (Beacon)
◦ CombiSecurity.org
◦ CombiSecurity.com
◦ BastionSecure.org
◦ BastionSecure.com
• Email Addresses
◦ oliversoftware@hotmail.com
◦ korsartravel@bk.ru
◦ inga@parktravel-mx.ru
◦ drake.lampado777@gmail.com
◦ drake.lampado777@gmail.com
• Industries
◦ Financial
◦ Retail
◦ Hospitality
◦ Gaming
• Targets of opportunity
• Colonial Pipeline
• Lockheed Martin
• SEC
- File and Directory Discovery (Enterprise T1083)
- Masquerading (Enterprise T1036)
- Windows Management Instrumentation (Enterprise T1047)
- Domain Account (Enterprise T1087.002)
- Permission Groups Discovery (Enterprise T1069)
- Asymmetric Cryptography (Enterprise T1573.002)
- Digital Certificates (Enterprise T1588.004)
- Domain Trust Discovery (Enterprise T1482)
- Command and Control (Enterprise TA0011)
- Collection (Enterprise TA0009)
- System Information Discovery (Enterprise T1082)
- Obfuscated Files or Information (Enterprise T1027)
- SSH (Enterprise T1021.004)
- Virtual Private Server (Enterprise T1583.003)
- Indicator Removal from Tools (Enterprise T1027.005)
- JavaScript (Enterprise T1059.007)
- Password Cracking (Enterprise T1110.002)
- Initial Access (Enterprise TA0001)
- Rename System Utilities (Enterprise T1036.003)
- Supply Chain Compromise (Enterprise T1195)
- Compromise Software Supply Chain (Enterprise T1195.002)
- Credential Access (Enterprise TA0006)
- Deobfuscate/Decode Files or Information (Enterprise T1140)
- Kerberoasting (Enterprise T1558.003)
- Defense Evasion (Enterprise TA0005)
- Malicious Link (Enterprise T1204.001)
- Spearphishing Attachment (Enterprise T1566.001)
- Resource Development (Enterprise TA0042)
- PowerShell (Enterprise T1059.001)
- Credentials from Web Browsers (Enterprise T1555.003)
- Query Registry (Enterprise T1012)
- Remote Desktop Protocol (Enterprise T1021.001)
- Virtualization/Sandbox Evasion (Enterprise T1497)
- Data from Information Repositories (Enterprise T1213)
- External Defacement (Enterprise T1491.002)
- Archive Collected Data (Enterprise T1560)
- Proxy (Enterprise T1090)
- Rundll32 (Enterprise T1218.011)
- Ingress Tool Transfer (Enterprise T1105)
- Domain Groups (Enterprise T1069.002)
- Install Digital Certificate (Enterprise T1608.003)
- Non-Application Layer Protocol (Enterprise T1095)
- Standard Encoding (Enterprise T1132.001)
- File Deletion (Enterprise T1070.004)
- Code Signing (Enterprise T1553.002)
- Malicious File (Enterprise T1204.002)
- Process Discovery (Enterprise T1057)
- Screen Capture (Enterprise T1113)
- Visual Basic (Enterprise T1059.005)
- Trusted Relationship (Enterprise T1199)
- Windows Command Shell (Enterprise T1059.003)
- Link Target (Enterprise T1608.005)
- Account Discovery (Enterprise T1087)
- Phishing (Enterprise T1566)
- Command and Scripting Interpreter (Enterprise T1059)
- Lateral Movement (Enterprise TA0008)
- Process Injection (Enterprise T1055)
- System Owner/User Discovery (Enterprise T1033)
- Code Signing Certificates (Enterprise T1588.003)
- Hidden Window (Enterprise T1564.003)
- Spearphishing Link (Enterprise T1566.002)
- Service Execution (Enterprise T1569.002)
- Regsvr32 (Enterprise T1218.010)
- System Checks (Enterprise T1497.001)
- Reflective Code Loading (Enterprise T1620)
- Software Discovery (Enterprise T1518)
- Web Protocols (Enterprise T1071.001)

Using this graph I was then able to build out a high-level activity-attack graph based on how the threat actors operate in the wild. Building the attack graph allowed me the ability to pull out an activity grouping specific to FIN7 as well in which they favor the use of phishing, powershell scripts, and their own PowerPlant backdoor.


FIN7 Activity-Attack Graph
Controls
Reconnaissance
Weaponize
Delivery
Exploitation
Installation
Command and Control
Action on Objective
Collect domains target organizations may interact with or own
Collect Employee Data on target organization
Gather Vendors of target organization
Find/Purchase Stolen Credentials
Create impersonating domains
Creation of attachments dropping malware
Purchase or creation of BadUSB devices
Creation of Attachments exploiting common vulnerability
Build Trojanized version of legitimate software organization may use
Upload malware to shared storage
Mail BadUSB drive to HR, IT, or management
Spear phishing targeted employees in organization
Compromise organization software supply chain and replace legitimate download links with links to Trojanized version
Execution of malicious PowerShell script
Malware Dropper executed (Boostwrite, Domenus VBS/JS, JSS-Loader, Hallbaked, LOADOUT,)
Hidden remote management tool in Trojanized software connects back to TA
Download of malicious file
Installation of Recognition Implant (ORM agent, VBS flash, JS flash)
Installation of backdoor (Harpy, Juggler, Birdog, Carbanak, Bellhop, KillACK, POWERPLANT, Birdwatch
Malware for exfiltration over C2 installed (LOADOUT, Griffon, Lizar, Cobalt-Strike, Carbanak, Domenous VBS, Bellhop)
Move laterally through network (PsExec, Cobalt-Strike, PAExec, Metasploit, sqlRAT, textmate
Privileged Escalation (Carbanak, Mimikatz, WCE, Cobalt-Strike, Metasploit, Powersploit, SessionGopher, CrackMapExec)
HTTP
HTTPS
DNS tunneling
Use of MEGASync client
Exfiltration over legitimate services (Goole Docs, Pastebin, Cloud Storage)
Encryption of data for ransom (use of RaaS) (Ryuk, Sodinokibi, DarkSide, MAZE, Blackmatter)
Payment Card data extraction
Theft of sensitive or IP data


FIN7 Activity Group
Spear phishing targeted employees in organization
Execution of malicious PowerShell script
Installation of backdoor PowerPlant

With the activity-attack graph, the ability for security teams to be responsive to FIN7 attacks is greatly enhanced. The SOC can now reference this when implementing controls to close gaps or understand where lack of visibility occurs, threat hunters can easily come up with the hypothesis needed to begin hunting, and incident response can reference it when doing IR to help provide context to the forensic artifacts that are uncovered.

Learn more here about how cyber threat intelligence is a key part of Netskope Cloud Threat Exchange

< Back

Next >

Allen Funkhouser

Read full Bio

More articles

Related Articles

Gri

Platform, Products, & Services

How SASE and the Internet Took Over Wide Area Networks (Part 2)

By François Devienne