SANS

Analyst Program

Whitepaper

SANS 2022 ATT&CK® and D3FEND™ Report: Incorporating Frameworks into Your Analysis and Intelligence

Written by **Matt Bromiley**

January 2022

DEVO

Introduction

This paper was developed during the middle of yet another cybersecurity crisis, in which the cybersecurity industry simultaneously combatted the impact of the Apache Log4j[1] vulnerability and an Amazon Web Services (AWS) outage. While the latter was temporary, the former sent defenders, security professionals, and developers scrambling to patch vulnerable systems and prevent attacks on, and access to, their networks.

Adversaries have embraced a new vector for gaining a foothold into a targeted organization, further adding to a long list of capabilities that they have at their disposal. Unfortunately, defenders have had to document and plan for nearly any technique adversaries could use against them, all while trying to keep their organizations' networks secure. Luckily, during the past few years, the cybersecurity industry has witnessed the emergence of multiple frameworks that assist with this process, providing defenders with excellent resources for combatting cyber threats.

In this whitepaper, we look at two complementary frameworks that defenders should be utilizing: MITRE ATT&CK® and MITRE D3FEND™. Aptly named, these frameworks describe adversary techniques and defense countermeasures, respectively. ATT&CK is no stranger to most enterprise security practitioners: Since its introduction, multiple security controls and vendors have aligned their products and detections to ATT&CK. However, we have seen little representation of D3FEND—something we aim to change with this whitepaper.

This whitepaper covers the following topics:

- An understanding of the ATT&CK and D3FEND frameworks
- The strengths of each framework as it pertains to enterprise security
- How the frameworks can be utilized to help strengthen incident analysis and response
- How to incorporate both frameworks into your threat intelligence capabilities

If this is your first time exploring these frameworks, we encourage you to consider the following questions:

- Do these frameworks already exist within our tooling and/or threat intelligence capabilities?
- Many organizations utilize ATT&CK to explain adversary actions—have we looked at D3FEND to implement countermeasures?
- What can D3FEND tell us about the countermeasures we currently have in our organization versus what we should have?

This paper also explores case studies that highlight how to bring the power of ATT&CK and D3FEND together. By examining both adversary tactics and countermeasures together, security teams can look to test and/or increase their security capabilities to mitigate certain techniques.

[1] "Apache Log4j Security Vulnerabilities," https://logging.apache.org/log4j/2.x/security.html

Analysis Frameworks

Before examining how each framework can assist defenders, a quick exploration of their history and purpose is in order. MITRE ATT&CK is a dynamic framework that catalogs adversary tactics and techniques based on threat intelligence and threat actor observations. Figure 1 shows a screenshot of ATT&CK Matrix for Enterprise as of the writing of this paper.

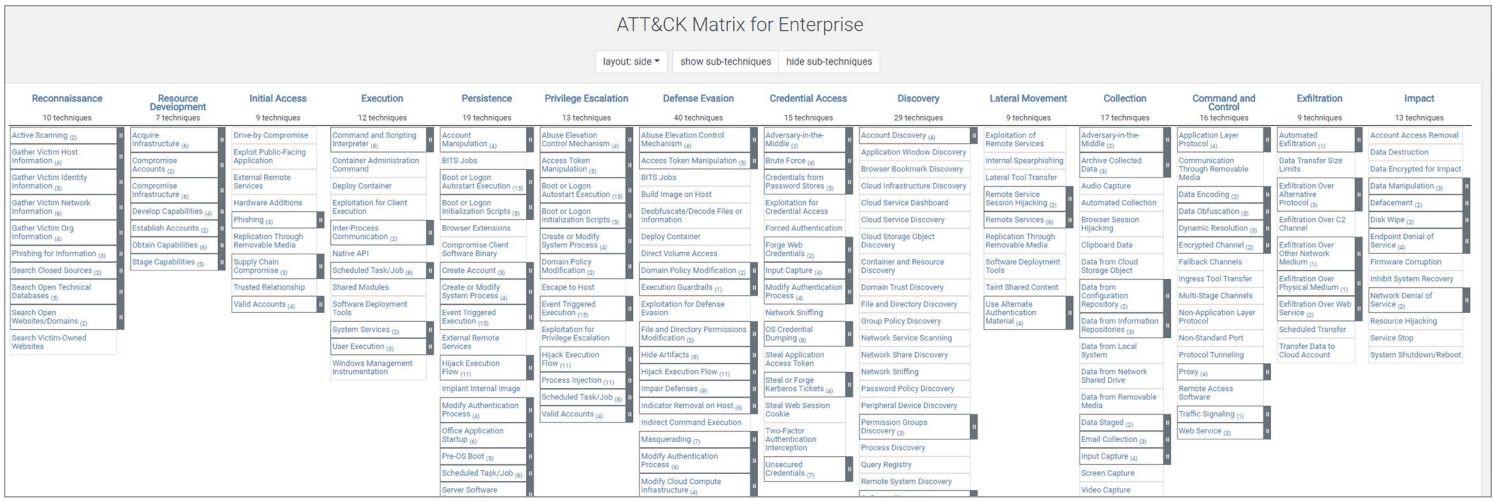

Figure 1. ATT&CK Matrix for Enterprise

In the past few years, we have seen many threat intelligence, incident detection and response, and endpoint and network security platforms align their observations with ATT&CK to serve as a reference point for analysts. One of the best parts of this is that as new adversary tactics and techniques are observed, the matrix and/or its knowledge base grows. For example, when first introduced, ATT&CK did not feature the Impact tactic. However, after enough observation, it was clear that Impact was a goal of some adversaries, and this tactic was subsequently included in the matrix.

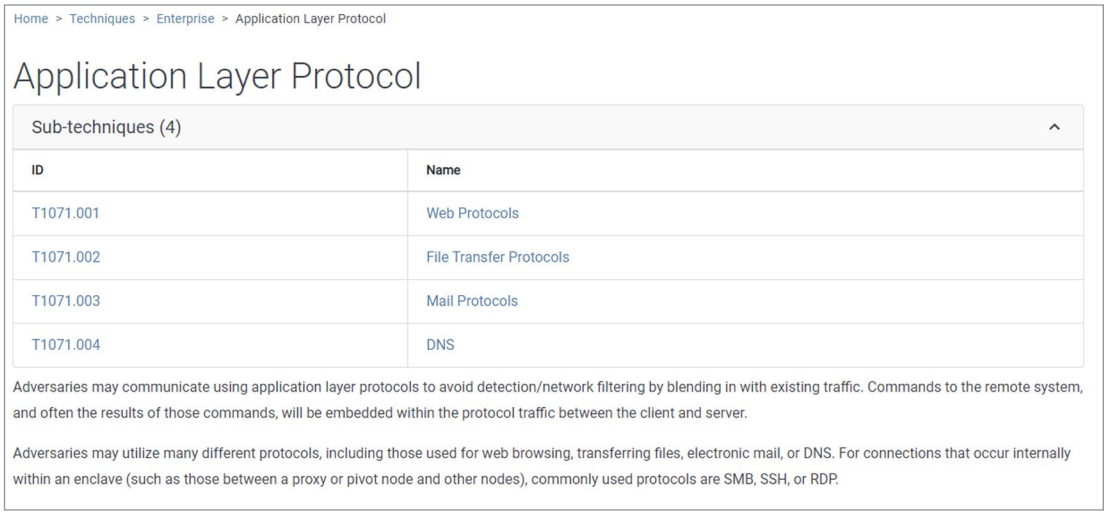

Figure 2. Application Layer Protocol Technique from ATT&CK

ATT&CK also breaks high-level adversary tactics into techniques and, in recent years, has included sub-techniques that drill down further. This allows for more granular definition and determination of exactly how a technique may apply to an organization and how to mitigate it. For example, Figure 2 shows the high-level technique Application Layer Protocol and four associated sub-techniques.

With the introduction of sub-techniques, ATT&CK created unique detection and mitigation capabilities. For example, consider Figure 2. Rather than security teams trying to expand on every application layer protocol abuse that might exist, sub-techniques provide specific insight into how adversaries are abusing those protocols. Because ATT&CK is backed by observed adversary activity, defenders can rest assured that these are not hypotheticals.

Thus, when a team receives an alert that HTTP/HTTPS protocol abuse has been detected (in the form of C2 communications, port mismatch, etc.), analysts can reference ATT&CK to determine how that abuse may have occurred and learn about the known threat groups and malware for that specific abuse. The power of this knowledge base cannot be understated, especially for security teams without massive threat intelligence feeds.

However, despite its rich capabilities and global, up-to-date knowledge base, ATT&CK was not designed to provide countermeasures or defenses. Continuing with this example, knowledge of HTTP abuse is only half the battle. Defenders should also know how to defend against adversary techniques. This is where many organizations fall short.

Enter D3FEND, created by MITRE and the National Security Agency (NSA). D3FEND is geared to pick up where defenders naturally leave off: "How do I defend against this?" A collection of countermeasures, D3FEND is similarly aligned by security objectives (such as Harden, Detect, or Isolate) and then organized by techniques and sub-techniques. Figure 3 shows a screenshot of D3FEND as of the writing of this paper.

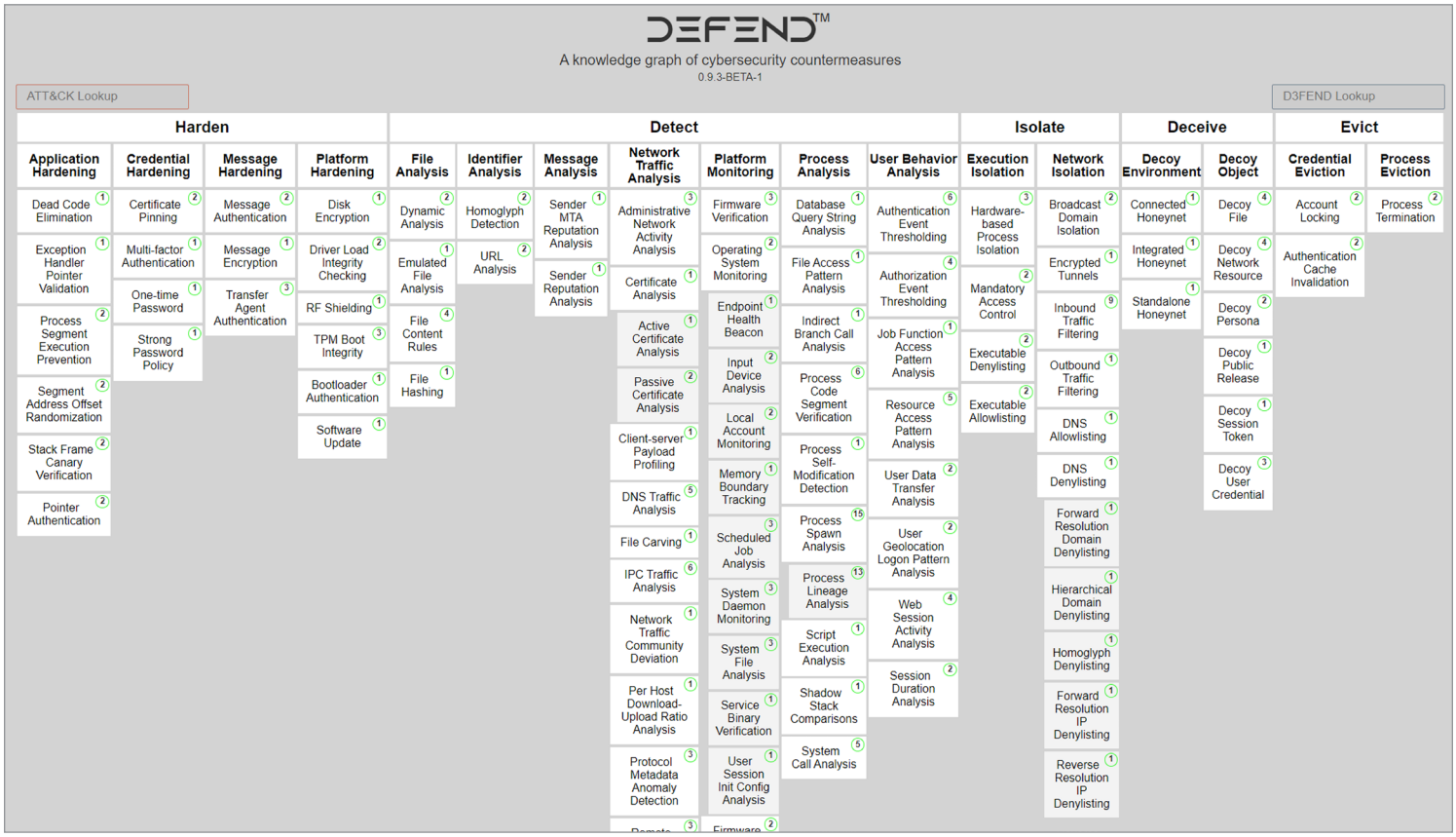

Figure 3. D3FEND Matrix

The largest representation of countermeasures within D3FEND lies within the Detect objective; however, that does not identify priority for defenders. Rather, D3FEND is designed to be a perfect complement to ATT&CK, allowing defenders to take the knowledge they learn about an adversary technique and port it directly to relevant countermeasures. The benefit is obvious: With these two resources alone, security teams can identify adversary techniques, perform lookups and gain context, and find subsequent countermeasures to combat those techniques in their environment.

Case Studies

Let's look at ways defenders can put these resources to work. In the following two case studies, we will examine how ATT&CK and D3FEND can be combined to help defenders combat various adversary techniques.

Case Study 1: Adversary Abuse of Remote Access Mechanisms

One adversarial trend that occurs year after year is abuse of remote access mechanisms. Whether it's an OS-native protocol, such as RDP, or a third-party tool, such as LogMeIn or TeamViewer, adversaries love an opportunity to gain access into an environment via already-established means. In February 2021, Kaspersky reported record levels of RDP attacks, highlighting as much as 10 times growth in some nations.[2] The COVID-19 pandemic has not necessarily assisted defenders, because many organizations have relied on remote access to support a remote workforce. This has created plenty of opportunities for adversaries, which means a global pandemic has not slowed down defenders' needs to understand adversary tactics and techniques.

We'll analyze this case study by first examining how adversaries use remote access techniques. Within ATT&CK, the technique External Remote Services (T1133) is categorized as both an Initial Access tactic and a Persistence tactic. See Figure 4.

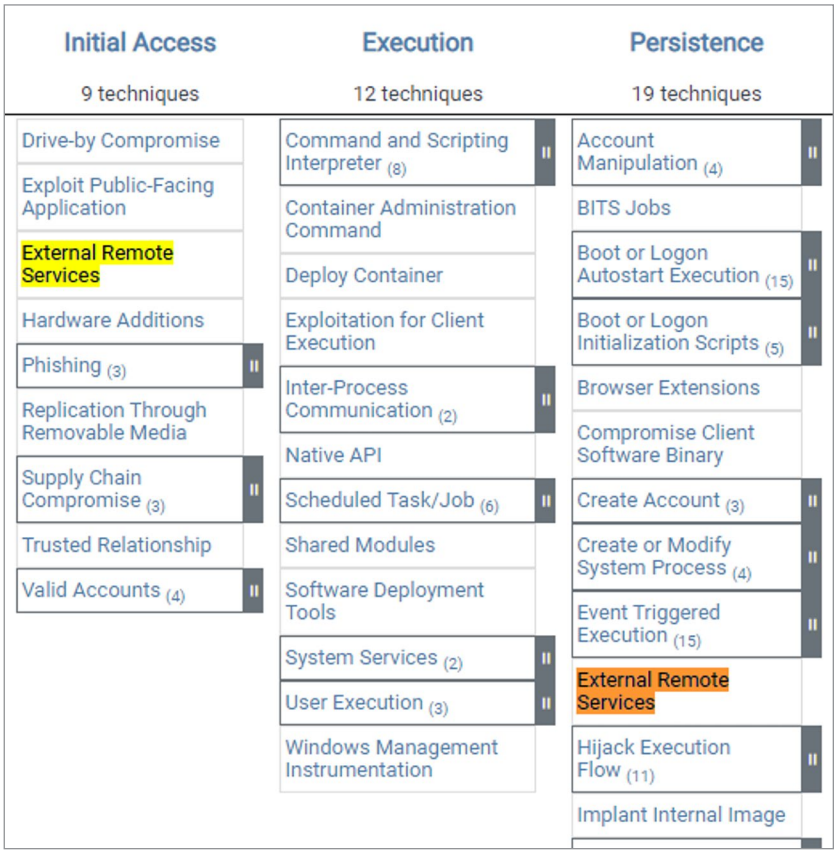

Figure 4. External Remote Services

[2] "RDP Attacks Persist Near Record Levels in 2021," www.darkreading.com/threat-intelligence/rdp-attacks-persist-near-record-levels-in-2021

When an adversary technique like this one is reflected across multiple tactics, this is both *cause for concern* and a *force-multiplying mitigation* for security teams. Let's examine why:

- **Cause for concern:** A technique that is seen within multiple tactics reflects its "flexibility" in an adversary's toolkit. In the present case, external remote access can be used to both initially gain access to an organization and maintain persistence. These highlight "where" during an attack cycle defenders might expect to see this technique used.
  - **Initial Access—**Exposed or insecure external remote services create an opportunity for an adversary to gain a foothold into an environment. As we explore the technique further, we can see that applicable services may include VPNs, Citrix, Windows Remote Management, or Virtual Network Computing (VNC). As previously discussed, this may also include RDP. Figure 5 provides a snippet of the ATT&CK entry for the technique External Remote Services (T1133).

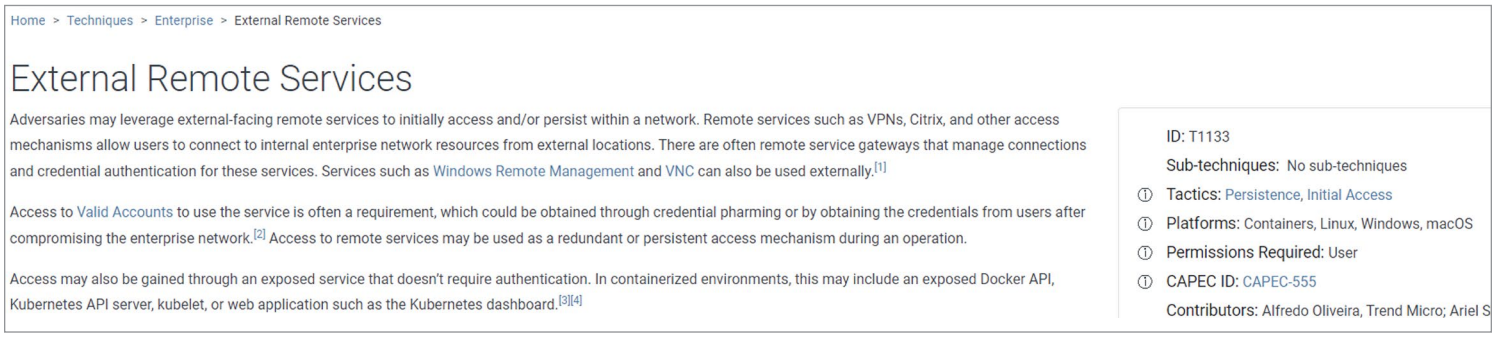

Figure 5. ATT&CK Entry for External Remote Services

  - **Persistence—**Similarly, external remote services provide adversaries an excellent opportunity to maintain persistence inside an environment. Consider, for example, an adversary who must craft a spearphishing campaign, modify and/or deliver malware, execute code, and obtain a remote shell into an environment. These are multiple steps that, if even one is disrupted, can impose more cost to an adversary's intrusion.

    Instead, consider when adversaries gain a foothold into an environment, they discover an existing external remote access channel. The need to establish or craft their own persistence is not as necessary, nor will their persistence be as detectable.

- **Force-multiplying mitigation:** Just as adversaries receive the benefits of multi-use techniques, defenders gain multiple benefits when they mitigate. Consider Remote Desktop Protocol, as demonstrated in Figure 5. When defenders gain visibility, monitoring, and/or blocking control of (or eliminating) RDP within the environment, they have minimized an adversary's ability to abuse it. Removing Initial Access *and* Persistence tactics from an adversary's toolkit can deal a big blow to their capabilities and attack plan.

The benefits to defenders do not stop there. This is one of the best parts about utilizing a reference such as ATT&CK. Looking back to Figure 4, we can see that access to Valid Accounts is often a requirement for remote service abuse. Quickly daisy-chaining from one to the other, defenders can see how locking down external remote services also provides a chance to implement strong account procedures, such as strong and rotating passwords, least privileges, and other recommendations.

Mitigations

ID	Mitigation	Description
M1042	Disable or Remove Feature or Program	Disable or block remotely available services that may be unnecessary.
M1035	Limit Access to Resource Over Network	Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems.
M1032	Multi-factor Authentication	Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Two-Factor Authentication Interception techniques for some two-factor authentication implementations.
M1030	Network Segmentation	Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.

Figure 6. ATT&CK Mitigations for External Remote Services

Sure enough, ATT&CK also includes a list of mitigations for various techniques. Figure 6 provides a snippet of mitigations to help defend against external remote service abuse.

However, mitigations and countermeasures are not the same. After all, a security team may want to quickly mitigate an impending technique but deploy long-term countermeasures to observe and/or defend against future threats. These answers, and more, can be found within D3FEND.

The fastest way to link techniques between the two matrices can be found right on the front page of the D3FEND matrix, at **`https://d3fend.mitre.org/`**. By looking up ATT&CK technique T1133, External Remote Services, we can see the relationships drawn by various countermeasures and this technique. Figure 7 provides a snippet of the linked relationships, as displayed by D3FEND.

Figure 7 displays the various

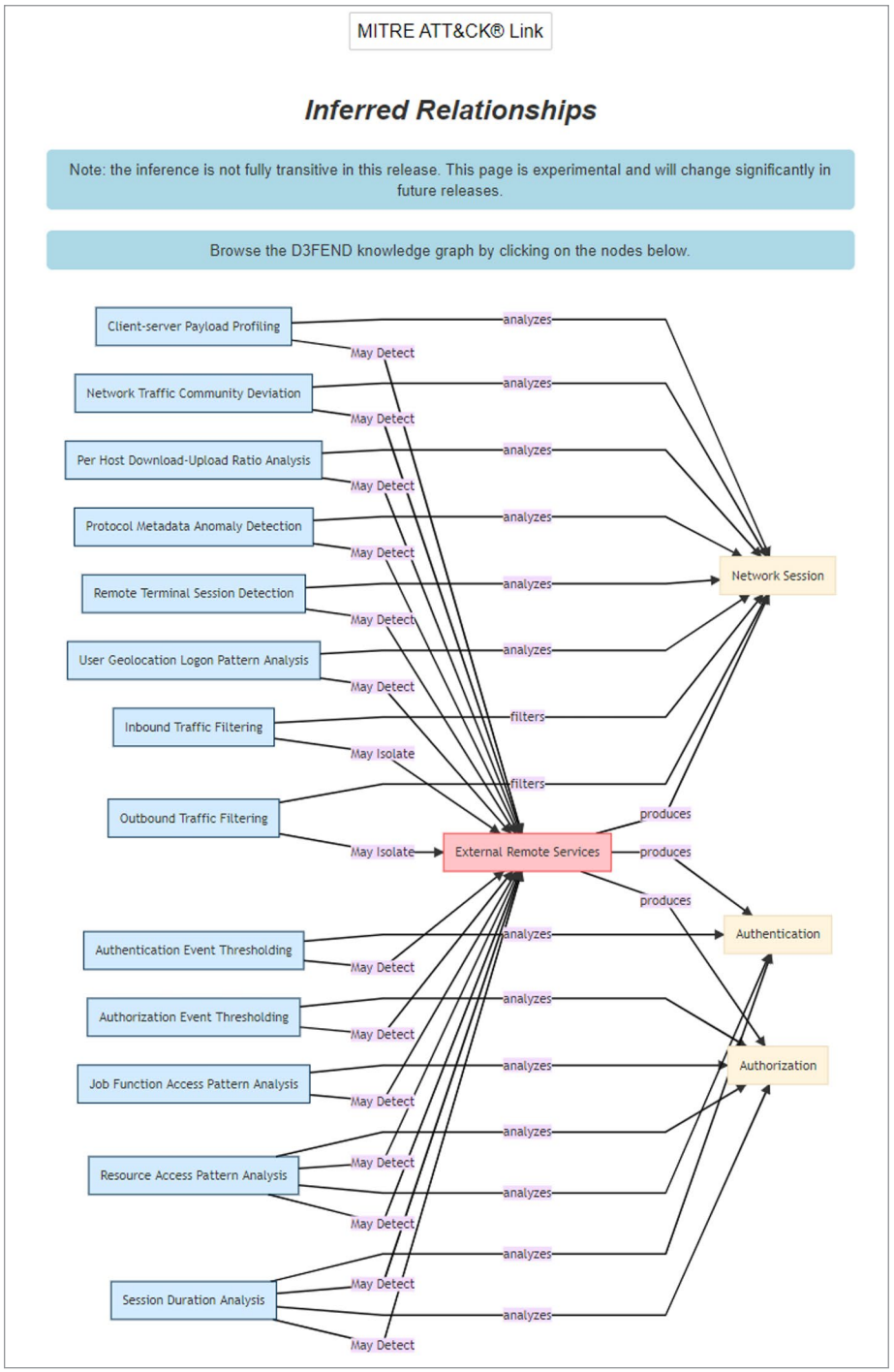

Figure 7. Inferred Relationships Between ATT&CK and D3FEND

countermeasures within D3FEND and how they could be used to counteract against External Remote Services. This is a perfect place for defenders to begin analyzing and deploying effective countermeasures. For this case study, we will focus on the Remote Terminal Session Detection countermeasure, shown in Figure 8.

In Figure 8, we can see a detailed explanation of ways to detect remote terminal sessions, via countermeasures such as network traffic inspection and algorithm analysis. This is extremely insightful knowledge for defenders looking to fine-tune their controls or implement custom detections. However, D3FEND goes a step farther by providing mappings to *other* ATT&CK techniques that these countermeasures may be effective against. See Figure 9.

This is where, via a combination of the two matrices, defenders can gain a true advantage over an adversary. Starting with a single adversary technique, such as External Remote Services, defenders can combine the knowledge from both to deploy countermeasures against that *single* technique. However, in doing so, via the Remote Terminal Session Detection D3FEND technique, they also can disrupt other adversary techniques. As shown in Figure 9, this single countermeasure can impact dozens of other adversary techniques. What do defenders gain with this? They gain a chance to disrupt multiple adversary techniques with a single countermeasure!

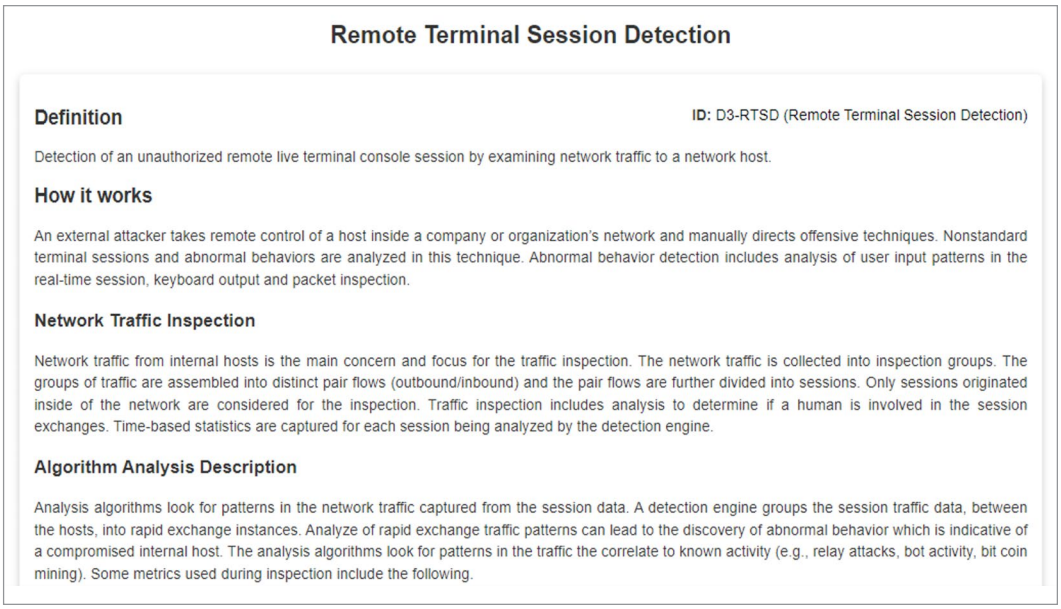

Figure 8. Remote Terminal Session Detection Countermeasure

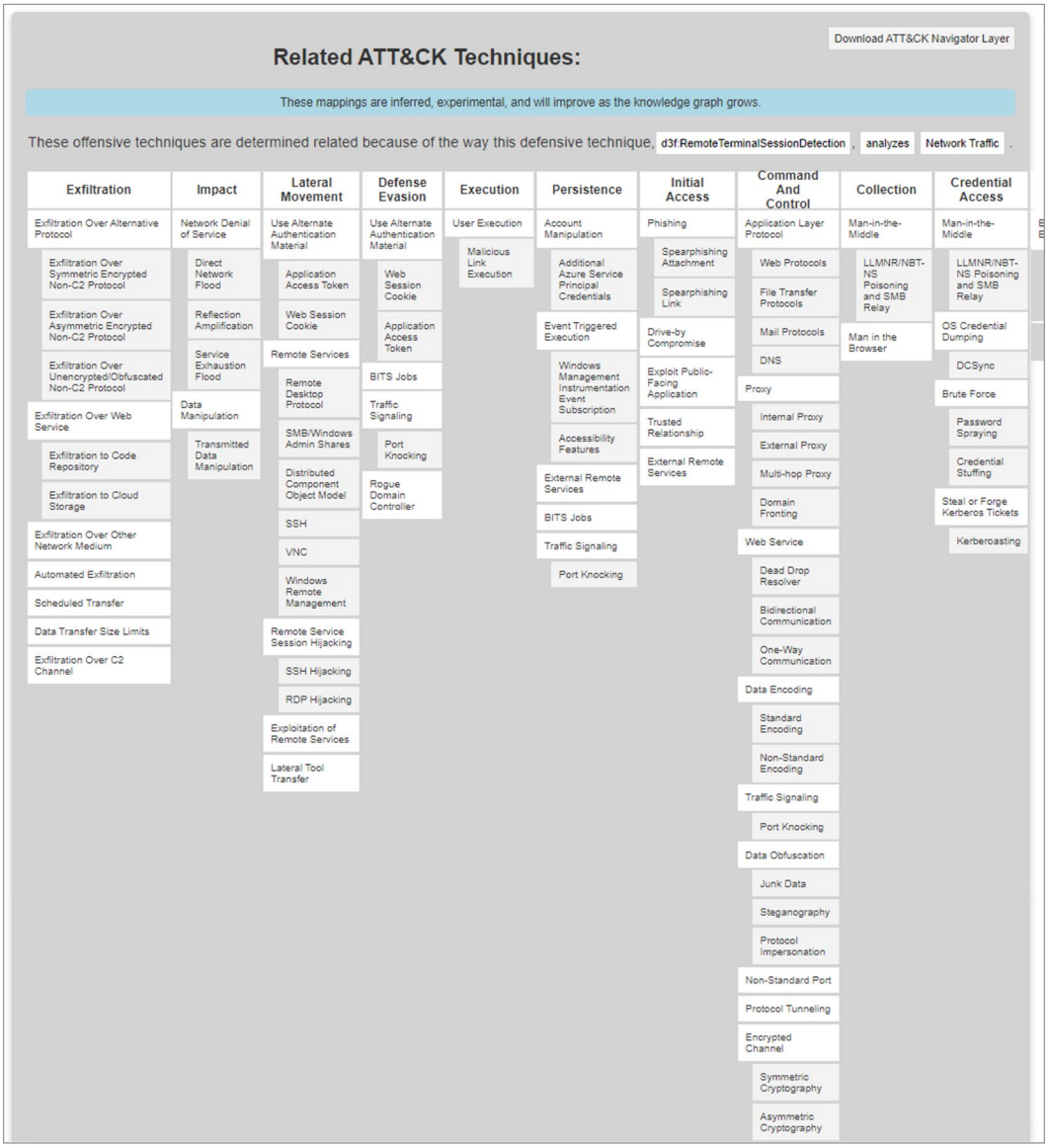

Figure 9. ATT&CK Techniques Related to D3FEND Remote Terminal Session Detection Countermeasure

Case Study 2: Adversary Abuse of DNS

In this case study, we continue with network-based adversary techniques, monitoring, and analysis. Perhaps one of the most ubiquitous and required protocols, DNS is a protocol that adversaries often abuse, with uses ranging from simple callbacks to complex algorithms and piecemeal data exfiltration. However, because DNS is essential for network resolutions and traffic direction, organizations cannot simply "block" DNS to mitigate these threats. Again, defenders can look to combine ATT&CK and D3FEND to find ways to deploy adversary countermeasures.

Beginning with ATT&CK, technique Dynamic Resolution (T1568) pertains to a few DNS-related adversary techniques. As shown in Figure 10, there are three key sub-techniques associated with DNS abuse that adversaries use to shield malware communications from within a targeted network.

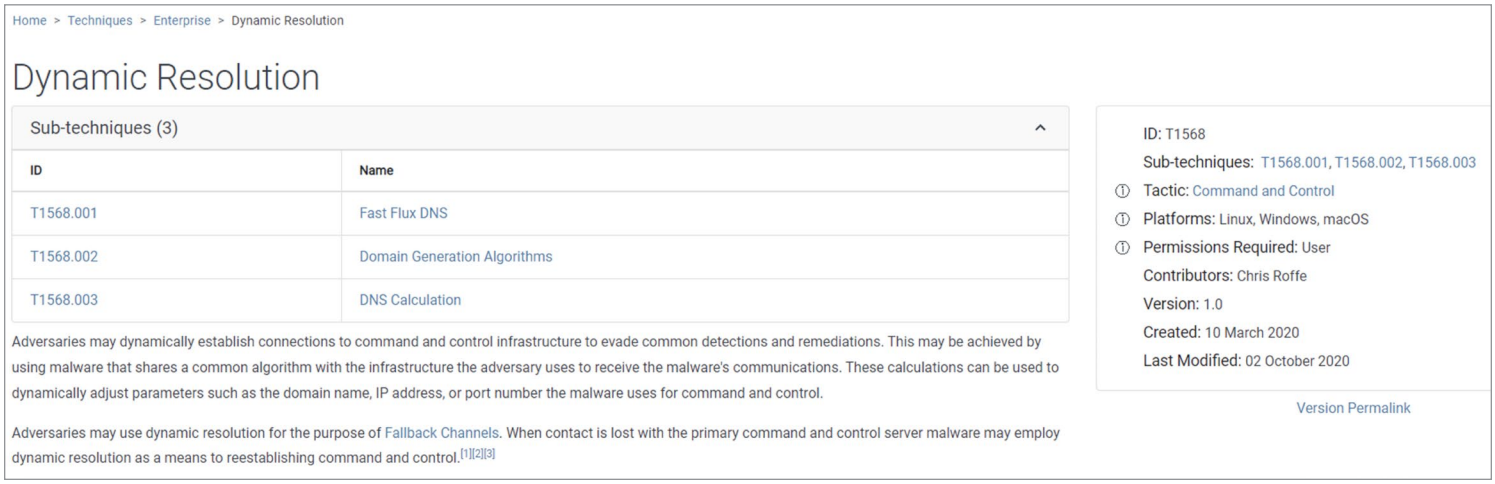

Figure 10. ATT&CK Sub-Technique for Dynamic Resolution

The information page for T1568 highlights some of the key uses for Dynamic Resolution sub-techniques: as a way to evade detection, for remediation, and/or as a fallback channel, in the event that a primary C2 method fails or is unable to successfully begin.

Recognizing its multiple uses by adversaries, ATT&CK also includes sub-technique T1071.004, which pertains to DNS abuse from an application layer protocol perspective. Figure 11 contains a screenshot of that particular sub-technique.

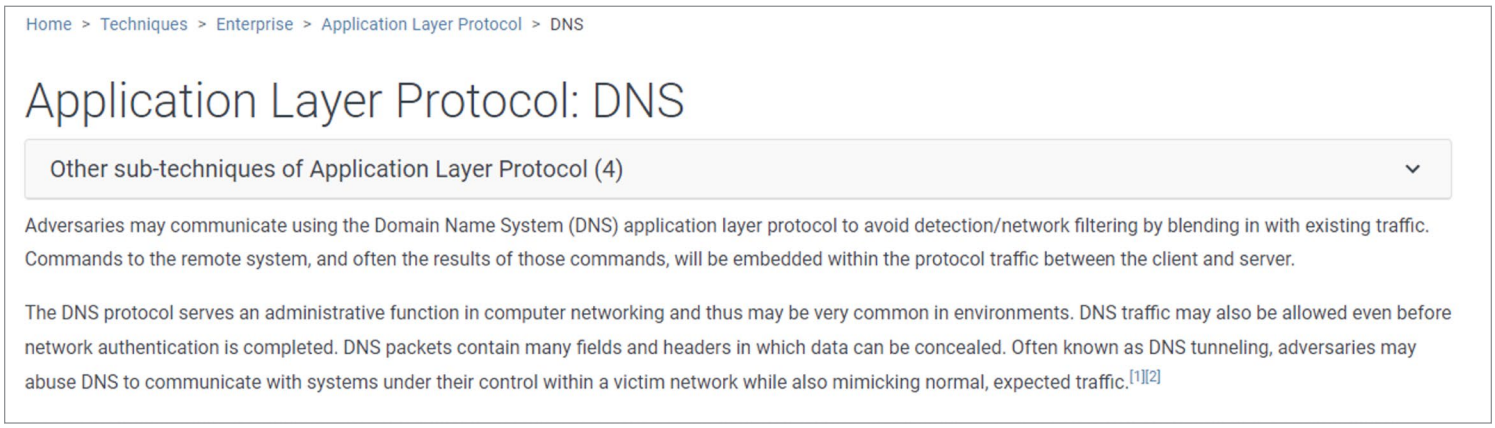

Figure 11. ATT&CK Application Layer Protocol: DNS Knowledge Page

For this protocol, ATT&CK reminds defenders of one thing: **Adversary techniques may be multipurpose and, thus, can be abused in different ways.** Single-purpose techniques may be mitigated with a single configuration change or block. Conversely, multipurpose techniques require that defenders consider all potential abuse paths and implement defenses, detections, and countermeasures appropriately.

With this knowledge in mind, we can hop over to D3FEND to look at DNS countermeasures. At first observation, we can see that DNS falls within both the Detect technique and the Isolate technique—clearly calling out that with correct harnessing, defenders can utilize DNS for multiple purposes. See Figure 12.

On the surface, D3FEND provides two valid viewpoints: Do we want to detect malicious DNS traffic or block it? Why not both? This is yet again where the power of D3FEND comes through—realizing that protocols, applications, pathways, and technologies within an environment can serve multiple purposes. After all, if adversaries can use protocols in multiple ways, why can't defenders realize the same benefits?

Figure 12. D3FEND with an Emphasis on DNS

Also, similar to the previous case study, the ability to deploy a countermeasure helps defenders find success in other areas, not just for a single technique. Utilizing D3FEND, we can examine the inferred relationships with countermeasures and Fast Flux DNS, as an example technique. See Figure 13.

The countermeasures listed in Figure 13 greatly outnumber the three highlighted in Figure 12 (DNS Traffic Analysis, DNS Allowlisting, and DNS Denylisting). This is the first value point for this case study—Fast Flux DNS, as a technique, can have a very specific countermeasure (Outbound Internet DNS Lookup Traffic). However, defenders are not limited to a single detection style. They may also look to detection capabilities such as traffic filtering, reverse resolution denylisting, parked domain detection, or relay pattern analysis, to name a few. The immediate value is being able to assess the capabilities of the security controls they have in place and utilize them effectively.

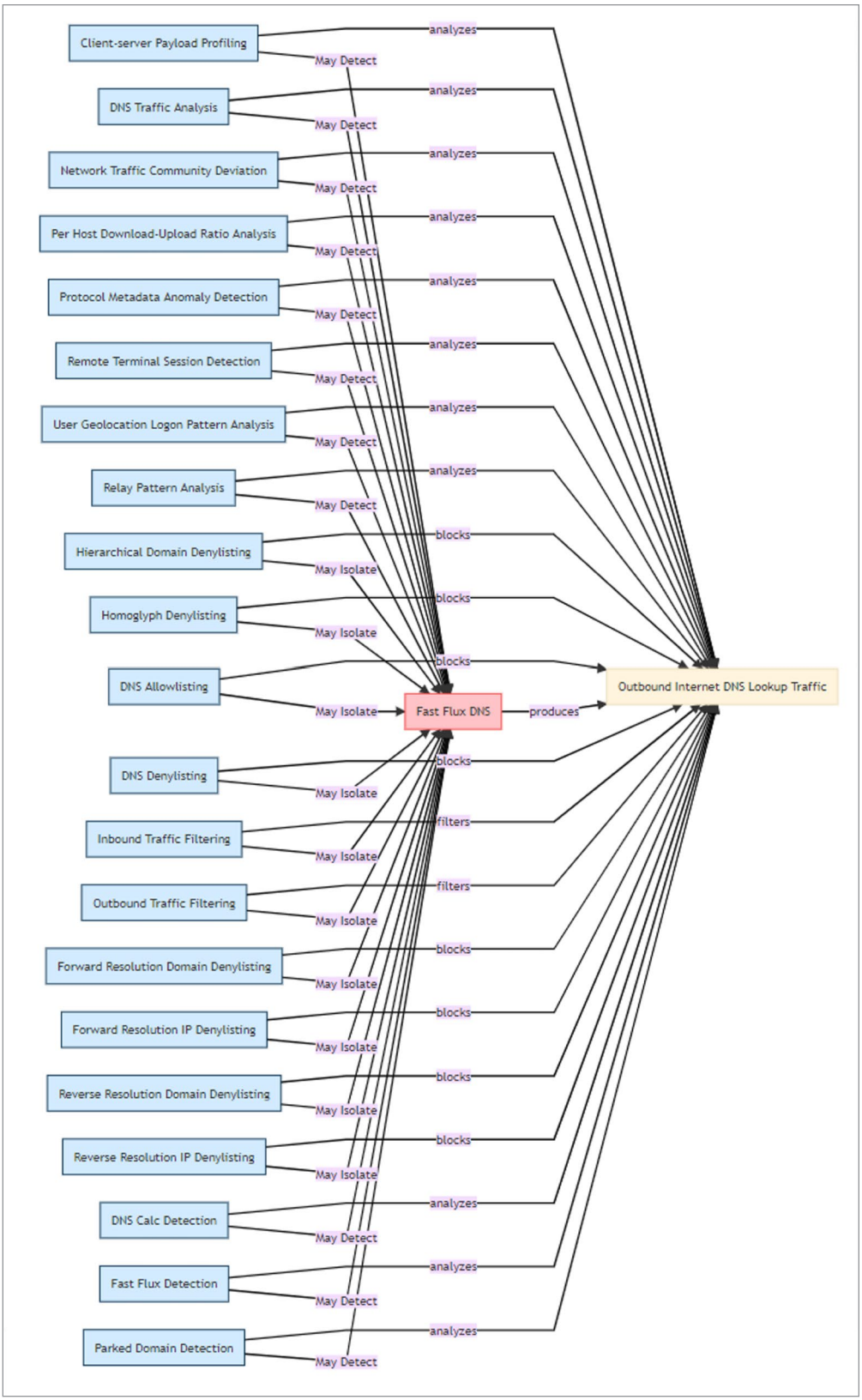

Figure 13. Inferred Relationships Between Fast Flux DNS and Countermeasures

Let us explore further the Outbound Internet DNS Lookup Traffic countermeasure. This is a simple-in-concept technique that looks up, or resolves, outbound traffic from within a network. As shown in Figure 13, defenders can utilize multiple types of detections for this countermeasure. However, does this countermeasure cover a single technique (Fast Flux DNS), or does it straddle multiple techniques? Looking further within D3FEND, Figure 14 directs us to the obvious answer.

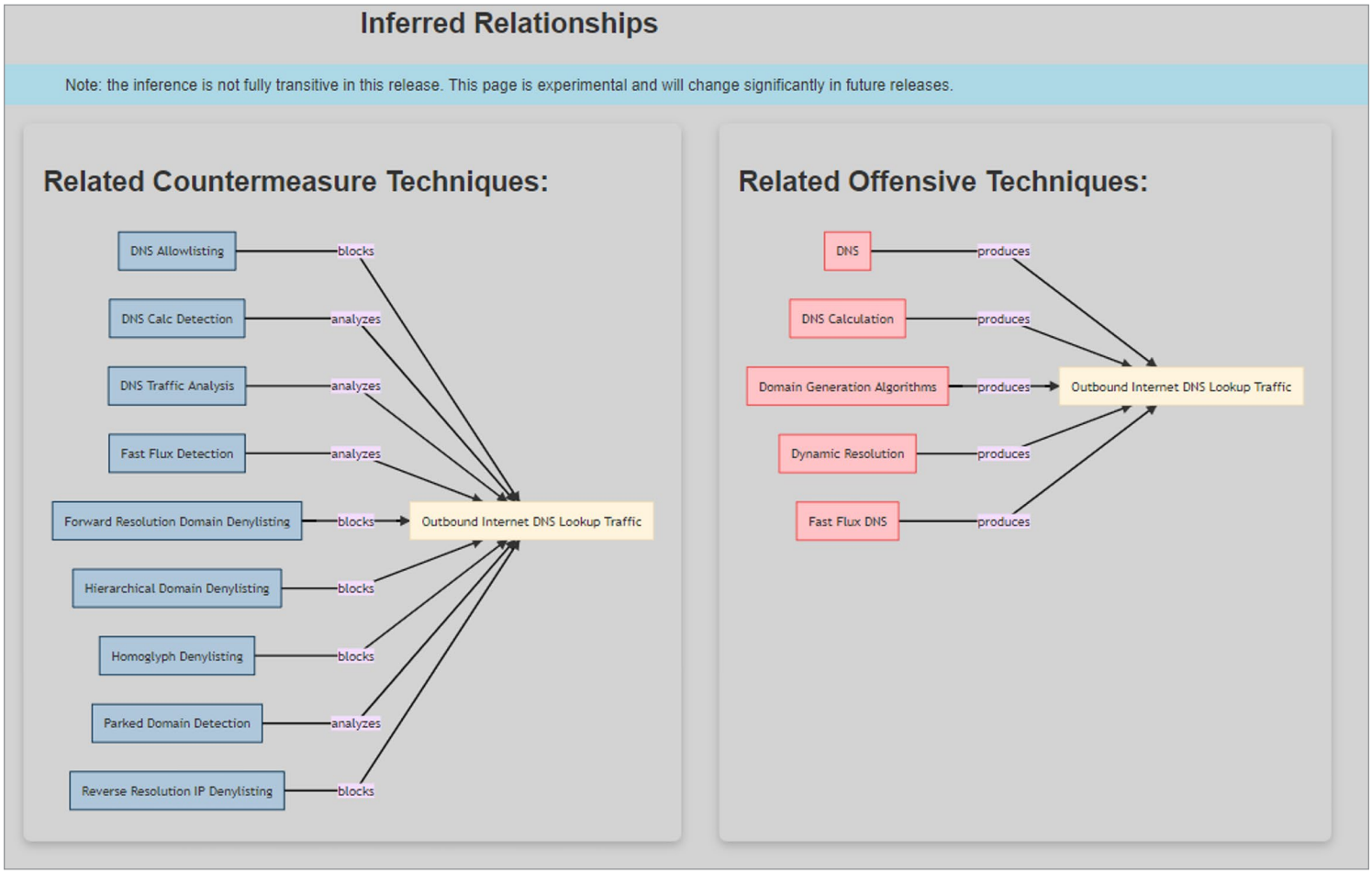

Figure 14. Inferred Countermeasure and Offensive Technique Relationships for Outbound Internet DNS Lookup Traffic

Closing Thoughts

Every day, it feels like adversaries gain new advantages and techniques to gain a foothold into organizations. Fortunately, defenders have multiple resources to help them catalog and classify adversaries' tactics, techniques, and procedures. Perhaps one of the most lauded in recent years has been ATT&CK, which quickly became a cornerstone of threat detection and intelligence pivoting. However, simply knowing of a threat or technique is not enough. Defenders need to know what to do next.

In this whitepaper, we solved this challenge by combining the well-known ATT&CK matrix with D3FEND, another framework brought to us by MITRE and the NSA. D3FEND provides defenders with a matrix-style knowledge graph of cybersecurity countermeasures, allowing them to compare techniques against defense mechanisms. When these two matrices are combined, defenders can deal a serious blow to adversary success rates.

The benefit in combining these two frameworks is clear, as shown in the case studies. Defenders can easily begin from an adversary technique, such as unauthorized remote access or DNS C2 communications, both of which may require deep network inspection to detect, let alone sufficiently record and/or analyze. D3FEND helps defenders zero in on the best return on their efforts, allowing them to deploy effective detections and countermeasures.

Finally, the benefits of combining these two matrices are their inherent relationships. ATT&CK provides relatively up-to-the-minute updates on adversary capabilities. By utilizing a complementary, defense-forward matrix, techniques and countermeasures are easily mapped. Within this link, defenders can find strong vantage points from which they can truly impact adversaries and protect their environments.

Sponsor

SANS would like to thank this paper's sponsor: