hyprfire

Finding threats on your network faster.

Firebug in the Mitre Framework

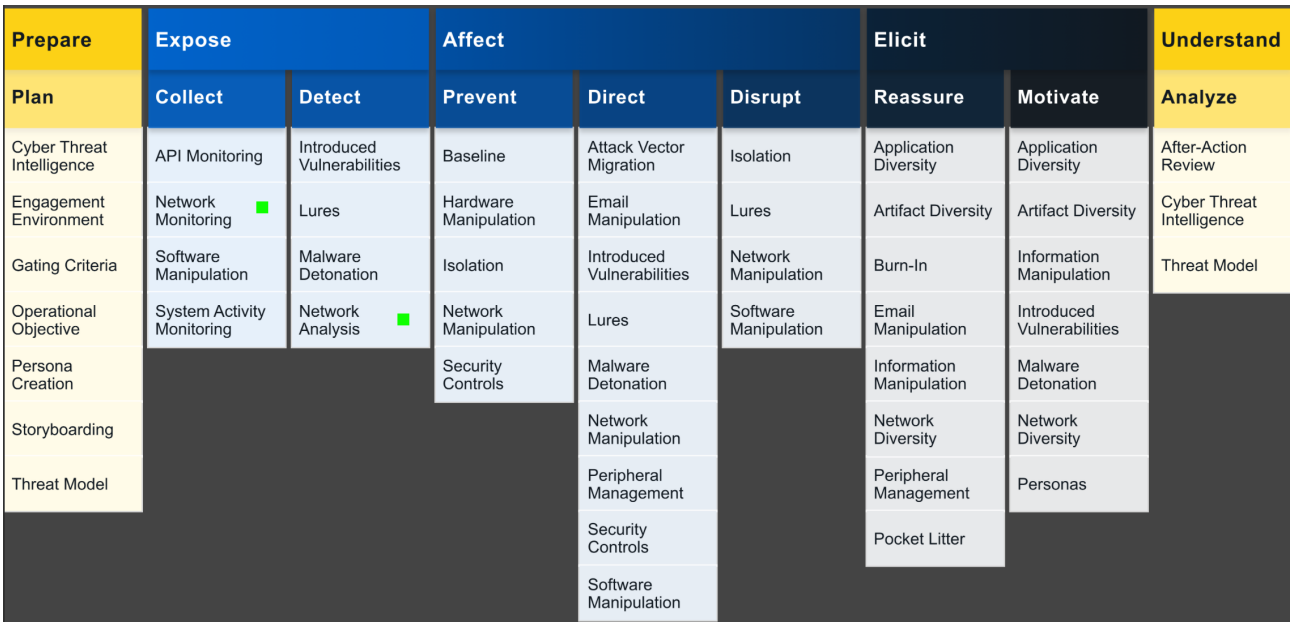
Connecting Firebug, Engage, and Att&ck

This document will discuss Firebug's current use cases and how they integrate with the Mitre cybersecurity frameworks, specifically Mitre Engage and Mitre Att&ck. We will first outline the sample use cases for Firebug, then the Mitre Engage Framework and where Firebug sits inside it, and then we will dive deeper to identify where Firebug can provide additional visibility with regards to the Att&ck framework.

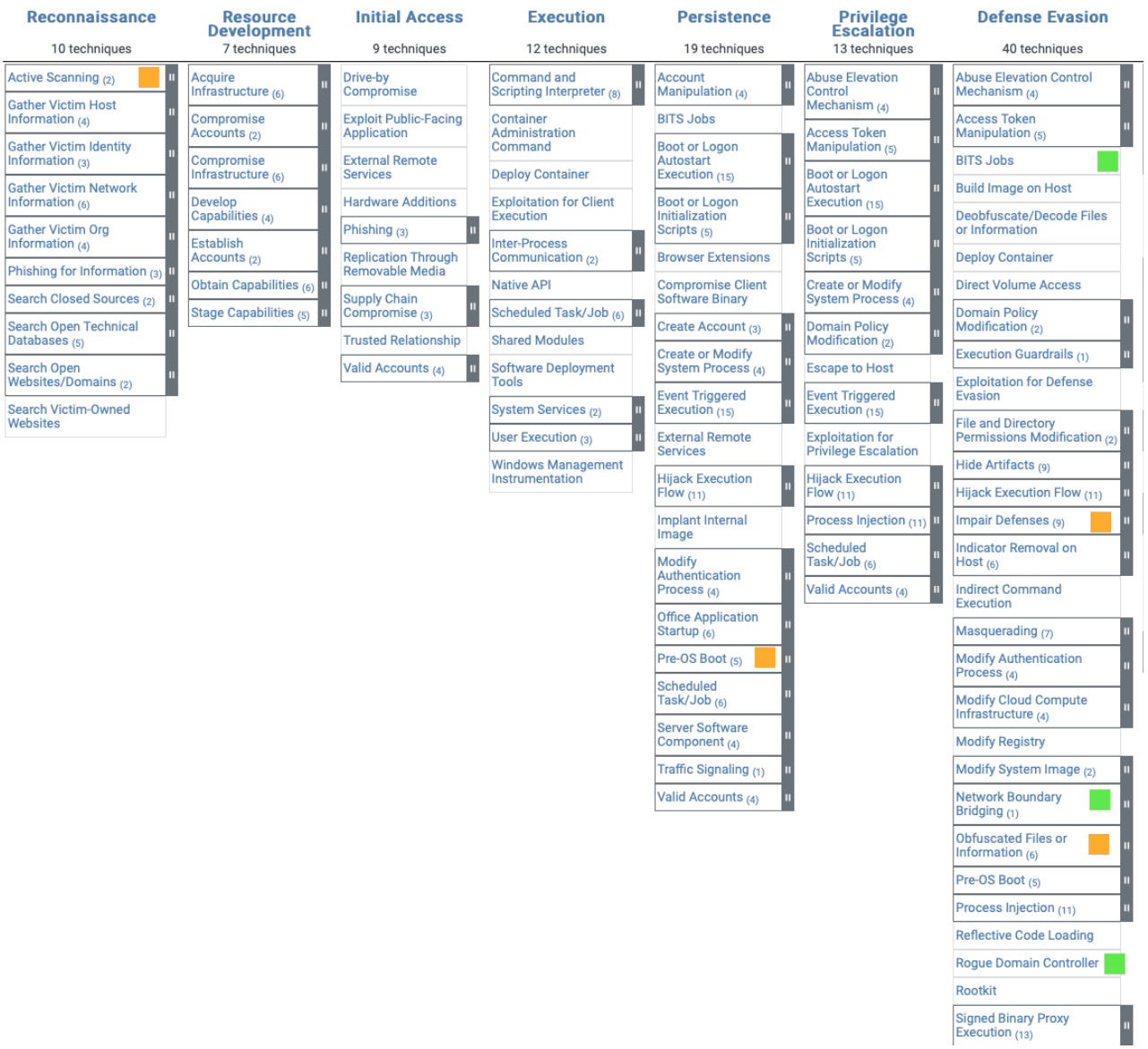
Summary Mapping

: Coverage : Partial Coverage

Engage Positioning

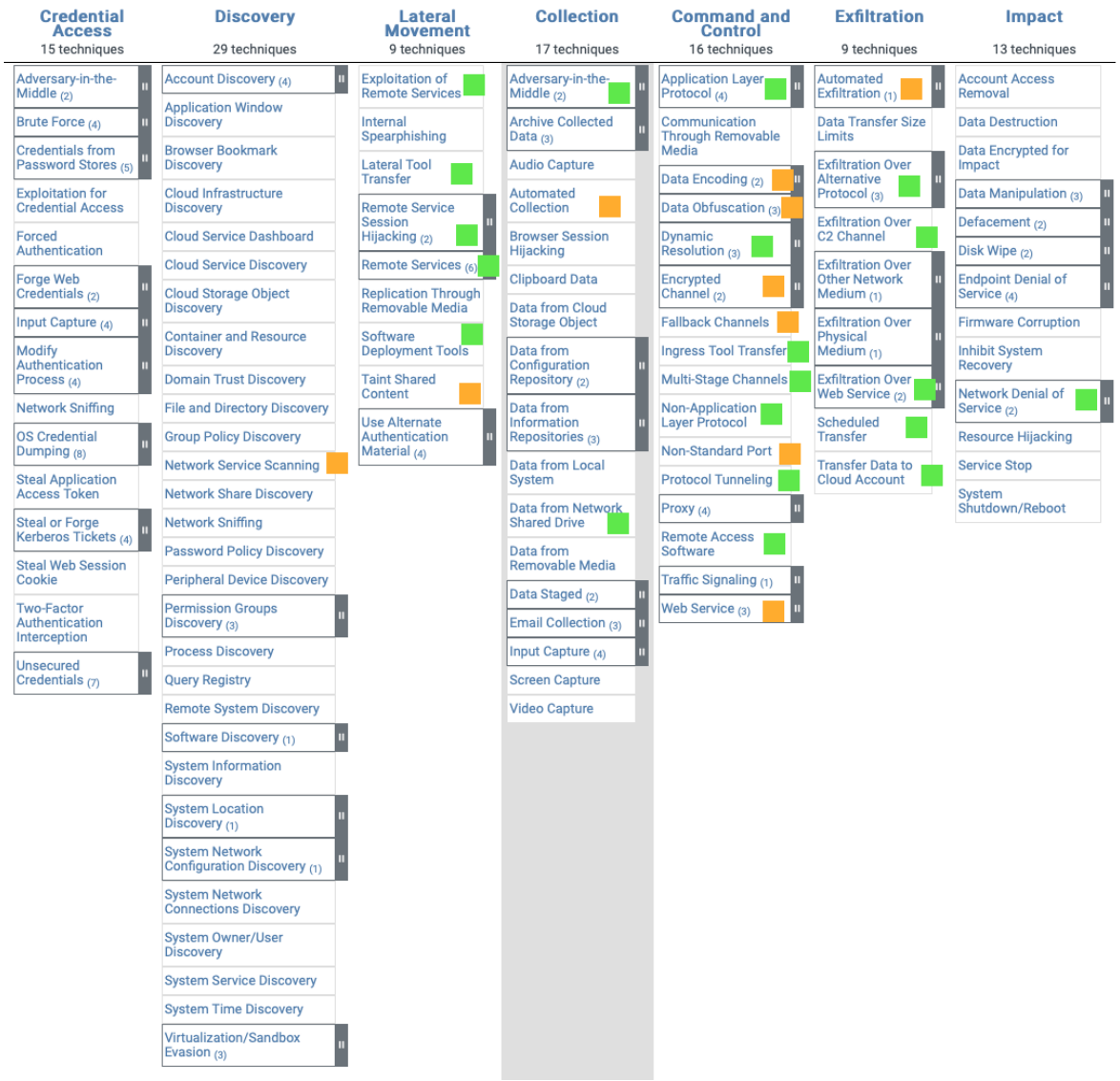


Att&ck Positioning - Part 1



: Coverage : Partial Coverage

Att&ck Positioning - Part 2



: Coverage : Partial Coverage

Firebug Use Cases

Firebug is by design an active network cyber security tool, and as such works best in a threat hunting environment with threat hunting workflows. At its most basic form, Firebug is a threat hunting lead generator with specific focus on abnormal or unusual network traffic, specifically with relation to behaviours (and protocols) that are related to lateral movement and early stage internal reconnaissance. Firebug's unique method of handling network data also means that it does not limit its detection capability to attacks, it is also useful in exposing unwanted user behaviour and overall misconfigurations. Firebug's sample use cases are indicative of this lead-generation concept and workflow, and such a capability precludes simple association of use cases with Att&ck framework strategies (as Firebug does not detect these, it provides a platform to hunt them down, ie it allows an analyst to expose those threats and identify where on the killchain attackers are).

General Use Case

Firebug in general is used to provide:

- Information on security relevant issues inside client networks from the perspective of the hosting network tap.
- The ability to identify abnormal and potentially unwanted usage of lateral movement protocols (SMB, WinRM, LDAP)
- The ability to identify issues in outbound traffic regardless of the existence of outbound firewall policy (or more likely the lack thereof)

These in turn provide:

- Visibility of network issues (misconfigurations, attackers, insider threat) from a security standpoint.
- The ability to identify, classify, and react to abuses and misuses of machines and protocols (ie, bad user behaviour) inside selected networks.
- The ability to identify, classify, and react to outbound events (ie exfiltration, beaconing, unwanted service usage, etc) in selected networks regardless of firewall capability.

These activities through both Firebug's statistic engine and the simple fact that it gives focused attention to network events aligns with Firebug's placement in the Expose elements of the Engage matrix, specifically in Collection and Detection (see Mitre Expose below). The broad detective capability of Firebug allows for more subtle abuses of machines and protocol that go undetected by policy driven or tool detecting threat model security applications. Specific targets here are attackers trying to remain undetected by performing off-the-land attack styles.

Unwanted Service Detection Use Case

Firebug can be used to identify unwanted and unusual service usage inside selected networks. For example:

- Firebug was deployed between BYOD network and internet gateway in Client network
- Client did not have good visibility of outbound traffic from BYOD network
- Client had reason to believe users were using VPN/remote access software to bypass policy
- Firebug was able to detect these from a combination of unusual profile (VPN), rare usage (remote access), and target destinations (abnormal geolocations).
- Reporting was able to allow the client to rectify these issues.

Firebug was able to detect this due to the pDNS capability inside Firebug acting in concert with the statistical deviation detection system at Firebug's core. The behaviour of users using VPN and remote access software was detectable due to their rarity when compared with usual user actions. The fact that domains the remote access tools used were associated with known services was leveraged to extract these events from the Firebug log output. Firebug performs in similar fashion when used to detect attacker behaviour via IOC FQDNs (see Beaconing and IOC detection below). Firebug collects user actions, associates them with the used DNS queries via the pDNS system, and then forwards them as logs as the statistical detection system dictates. This allows for refined and targeted event generation for abnormal behaviour that correlates with DNS entries. This exists across both the Network Monitoring and Network Analysis cells in the Engage Matrix (see Mitre Engage).

Beaconing and IOC Detection

Firebug can be used to identify actor beaconing, exfiltration, and C2 traffic by virtue of its unusual nature and confirmed by known IOCs. One such example is the following:

- Firebug was deployed between Client VPN and Client core network.
- Firebug detected abnormal HTTPS behaviour emanating from the VPN network and passing outbound in the direction of the core switch.
- Firebug was able to identify the remote endpoint FQDN and generate events accordingly.
- Events were correlated with external threat intelligence data and remote FQDN was found to be a known IOC of known threat (in this case a C2 server)
- Event was then acted on, affected machines were identified from event data and isolated, and mitigation steps were taken.

In this case the attacker had not yet begun using the C2 connection, it was still in a beaconing phase. This behaviour however was different enough from HTTPS traffic in the VPN network that Firebug was able to identify its novelty and need to generate events for it. This allowed defenders to take corrective action before the attacker was able to perform further actions.

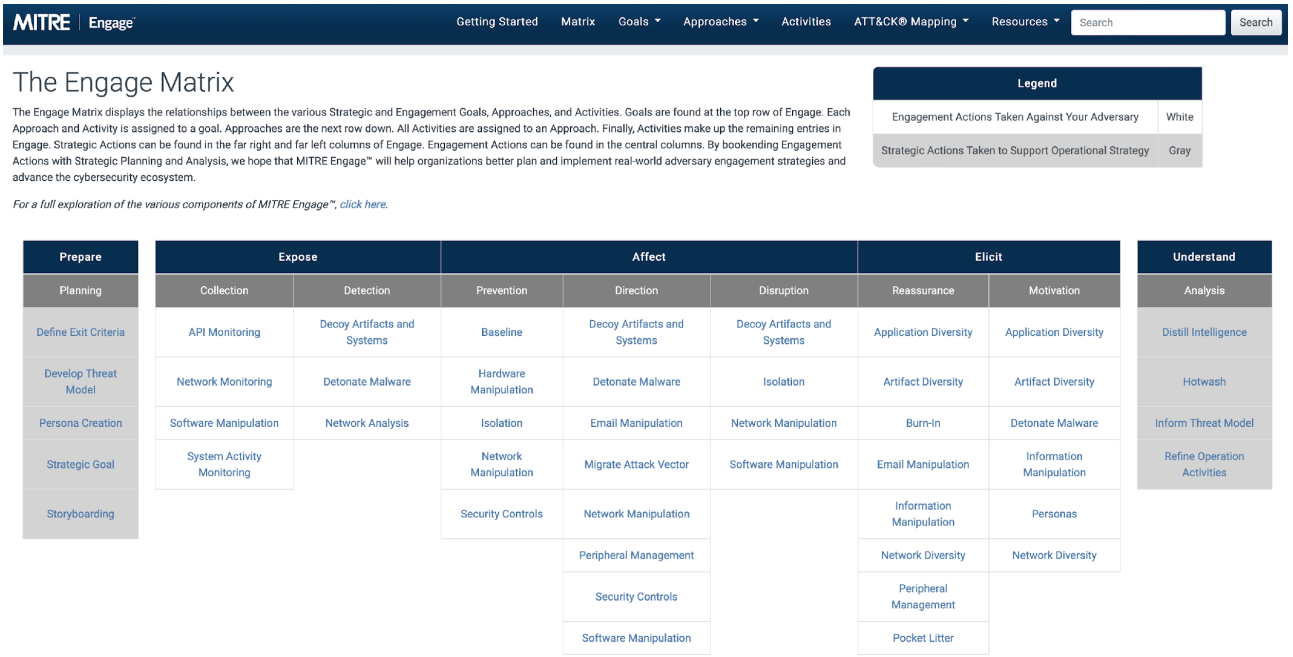
IR/Post IR Lateral Movement Detection

Firebug's rapid time to normalisation allows for drop-in deployments of the system into compromised environments. Firebug has been used in IR scenarios to provide leads in the investigation process as part of a reactive threat hunting scenario. One such example is the following:

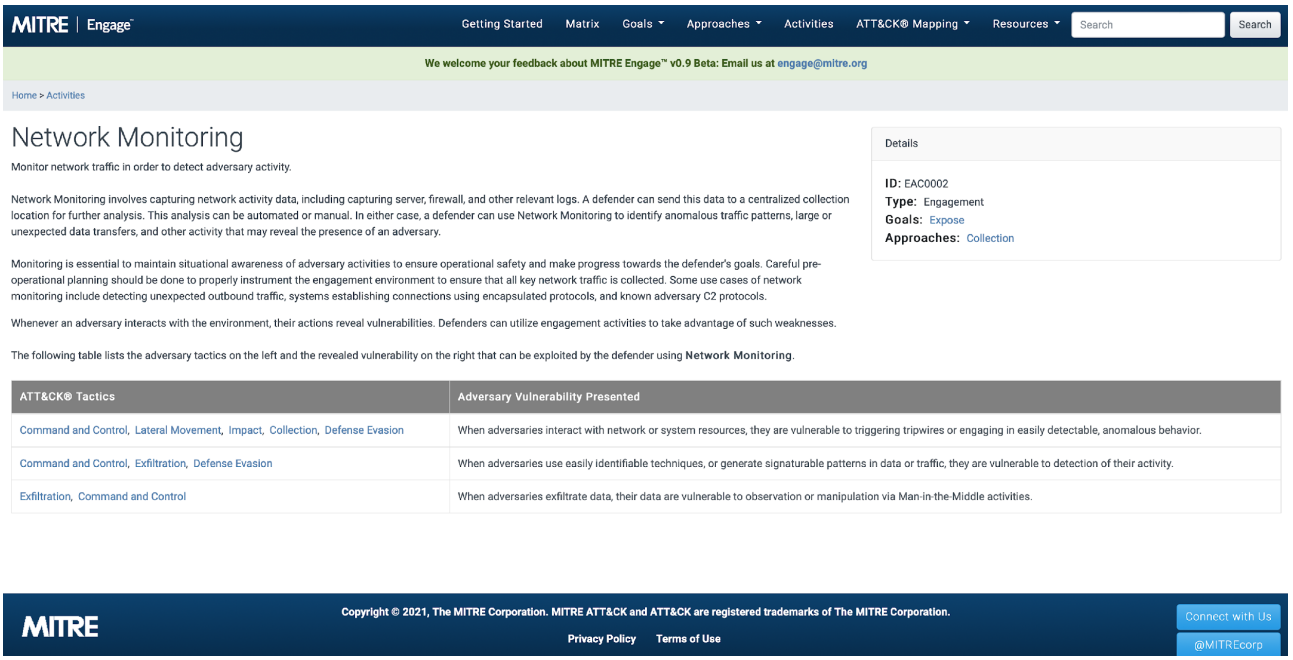
- Firebug was deployed in the DMZ network of Client affected (and compromised by) Log4Shell attack.
- Firebug was able to rapidly provide data on potential lateral movement, common talkers, and any LDAP protocol abuses (in Log4Shell's case, outbound LDAP).
- Firebug allowed the investigative team to rapidly identify and classify DMZ to broader network communications of concern.
- Firebug ultimately gave Client confidence at the end of engagement that the network had been secured from the immediate threat and that no further lateral movement was at that point occurring.

Mitre Engage

The Mitre Engage Framework (found here https://engage.mitre.org/matrix) is a framework that covers the Active Cyber Security strategic cycle. It covers the three main pillars of the Active process, identifying attackers early in the environment, actively engaging attackers in the environment in both direct and indirect methods, and crafting a realistic set of countermeasures to ensure attackers engage with decoys and countermeasures and provide maximum intelligence on their goals and tactics. It also covers the bookending steps in the Active cycle, including preparation for attacks and post attack analysis.

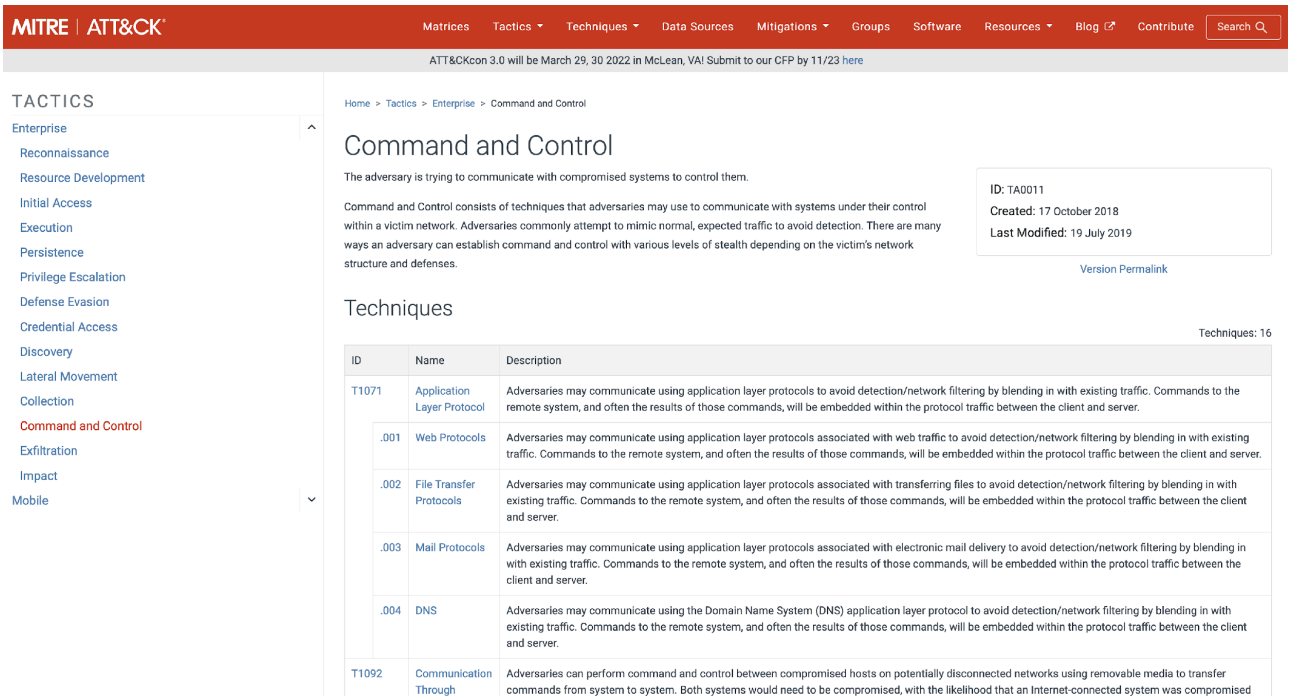


Firebug falls into the first of the three pillars, Expose, for early detection of malicious actors on the network via active threat hunting and intelligence usage. Firebug performance fits into both Network Monitoring activities (for collection of network data) and Network Analysis activities (for determination of network anomalies requiring investigation). Firebug can be classified as an “internal intelligence” system, as it provides intelligence on network events from selected networks that, when combined with additional intelligence and threat hunting, can provide a potent cyber security capability beyond passive automated response tools.



Each of these activities break down into a series of attacker vulnerabilities, or ways the attacker exposes themselves to a defender.

These are aligned with a series of Att&ck framework attacker tactics, like for example the Command and Control tactic. These are the activities in general that describe attacker kill chains in broad strokes.



Each of these directly incorporate techniques of the Att&ck framework itself, the final state of the Engage to Att&ck mapping. These mappings do not identify which Att&ck strategies an active solution or strategy “detects” or “covers”, but rather which locations in the Att&ck kill chain each element can expose. This is important in the threat hunting methodology, as the approach is to identify where an attacker may be in the kill chain from events that are necessarily broader than what can be matched to any given Att&ck technique or subtechnique. In short: We’re not interested in detecting specific techniques, we’re trying to expose their user’s existence.

Mitre Att&ck

For completeness, we have attached below a table that presents an Engage to Att&ck passthrough that gives a broad level understanding of how Firebug "maps" from one to the other. This should give some idea of what Firebug is capable of doing from an Att&ck standpoint, and where it can fit into your security architecture.

Attack Framework Mapping

ENGAGE Activity	ATT&CK Tactic	ATT&CK Element	Covered?	How?
Network Monitoring // Network Analysis	Command & Control	T1701 App Level Protocols	Yes	Firebug can detect sustained abnormal uses of protocols, even when encrypted
		T1132.002 Data Encoding: Non-Standard	Partial	Can detect deviations from normal protocol behaviour
		T1001.001 Data Obfuscation: Junk Data	Yes	Can detect deviations from normal protocol behaviour
		T1001.003 Data Obfuscation: Protocol Impersonation	Yes	Can detect deviations from normal protocol behaviour
		T1568 Dynamic Resolution	Yes	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1573 Encrypted Channel	Partial	Firebug can detect abnormal uses of encrypted channels, though not what they are being used for
		T1008 Fallback Channels	Partial	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1105 Ingress Tool Transfer	Yes	Firebug can detect abnormal file transfers.
		T1104 Multi Stage Channels	Yes	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1095 Non-Application Layer Protocol	Yes	Firebug works on the IP Protocol and catches all abnormal traffic above IP.
		T1571 Non-Standard Port	Partial	Firebug can detect when standard ports are being used inappropriately, as may

				occur when a standard port is being used for a non-standard protocol
		T1572 Protocol Tunnelling	Yes	Firebug can detect tunnelling in DNS, ICMP, and HTTPS.
		T1219 Remote Access Software	Yes	Firebug has detected unauthorised uses of TeamViewer and similar, and can be used to detect such.
		T1102 Web Service	Partial	Firebug can detect abnormal usage of web services, but cannot detect use if the ringfence regularly uses web service in similar fashion
Network Monitoring	Lateral Movement	T1210 Exploitation of Remote Services	Yes	Firebug can detect the change in behaviour of remote services as they are compromised
		T1570 Lateral Tool Transfer	Yes	Firebug can detect abnormal file transfers.
		T1563 Remote Session Hijacking	Yes	Firebug can detect abnormal use of sessions, even when the session has been persistent for some time
		T1021 Remote Services	Yes	Firebug can detect the change in behaviour of remote services as they are used abnormally
		T1072 Software Deployment Tools	Yes	Firebug can detect the change in behaviour of remote services as they are used abnormally
		T1080 Taint Shared Content	Partial	Firebug can detect abnomal behaviour, so if the shared content now behaves differently Firebug can detect the change.
Network Monitoring	Impact	T1498 Network DoS	Yes	Firebug can detect volumetric DoS and DDoS attacks.
Network Monitoring // Network Analysis	Collection	T1557 Adversary in the Middle	Yes	Firebug can detect when attackers are impersonating services like SMB to perform AitM attacks.
		T1119 Automated Collection	Partial	Bulk data replication over networks is detectable by Firebug
		T1039 Data from Network Shared Drive	Yes	Firebug can detect abnormal file transfers.
Network Monitoring	Defense Evasion	T1197 BITS Jobs	Yes	Firebug can detect abnormal file transfers.

		T1562.004 Disable or Modify System Firewall	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1562.007 Disable or Modify Cloud Firewall	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1599 Network Boundary Bridging	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1027.006 HTML Smuggling	Partial	Firebug can detect abnormal usage of HTTP/S
		T1542.005 TFTP Boot	Partial	Firebug can detect abnormal file transfers.
		T1207 Rogue Domain Controller	Yes	Firebug can detect abnormal SMB/LDAP actors, and new
Network Monitoring // Network Analysis	Exfiltration	T1020 Automated Exfiltration	Partial	Bulk data replication over networks is detectable by Firebug
		T1048 Exfiltration over Alternative Protocol	Yes	Firebug can detect abnormal file transfers.
		T1041 Exfiltration over C2 Channel	Yes	Firebug can detect abnormal file transfers.
		T1567 Exfiltration over Web Service	Yes	Firebug can detect abnormal file transfers.
		T1029 Scheduled Transfer	Yes	Firebug can detect abnormal file transfers.
		1537 Transfer Data to Cloud Account	Yes	Firebug can detect abnormal file transfers.

Document History

Document Version	Author Name	Comment	Date
0.1	Stefan Prandl	Initial Version	Tuesday, 16 November 2021
1.0	Stefan Prandl	Added Table	Tuesday, 23 November 2021
2.0	Stefan Prandl	Added Use Cases	Thursday, 7 April 2022
2.1	Stefan Prandl	Added Summary	Friday, 8 April 2022