Web Proxy Hunting and Detection Cheat Sheet

Version 1.0
Mehmet Ergene @Cyb3rMonk

Attribute	Technique	What to look for
Duration	Calculate the sum per SourceIP-DestinationIP pair over 12/24 hours	Higher values may indicate beaconing
HTTP Status	Calculate the total count of the HTTP Status Codes per SourceIP or per SourceIP-DestinationIP over a specific time period.	Higher values of an uncommon HTTP Status Code may indicate C2 activity.
	List URLs having only HTTP Error codes	C2 servers may rotate their dns records, malware tries every domain and causes http errors.
Bytes In	Calculate the count of BytesIn per Source-Destination pair over 12/24 hours	Higher values may indicate beaconing. C2 servers reply with the same data, making Bytes In value the same
	Calculate the ratio of count(BytesIn) per Source-Destination pair	Higher values of ratio may indicate beaconing
Bytes Out	Calculate the sum of BytesOut per Source-Destination pair over 12/24 hours	Higher values may indicate data exfiltration
	Calculate the ratio of count(BytesOut) per Source-Destination pair over 12/24 hours	Higher values of ratio may indicate beaconing
HTTP Method	Calculate the ratio of POST or PUT over GET per Source-Destination over 4/8/12/24 hours	Higher values may indicate beaconing or exfiltration
URL Hostname	Compare with top 1M domains and calculate hit count	Hit count <5 and Hostname is not in top 1M may indicate malicious payload delivery
	Calculate hit count per Hostname	Less hit count may indicate malicious payload delivery
URL Path	Calculate count per Source-Destination-URLPath pair	Higher values may indicate beaconing
URL Query	Calculate count per Source-Destination-URLQuery	Higher values may indicate beaconing
	Calculate length of URLQuery	Higher values may indicate encoded data, a sign of exfiltration or beaconing
	Look for base64 encoded strings in URLQuery	Encoded strings may indicate beaconing or exfiltration
Content Type	List Content Type per Source-Destination pair	Uncommon Content types may indicate malicious file
User Agent	Calculate count within the environment(long tail analysis)	Lower values may indicate a malicious binary
URL Category	Query for Uncategorized, Dynamic DNS, and other suspicious categories. Calculate dcount of SourceAddress by URLHostname	Small dcount values may indicate abnormal/suspicious/malicious activity. If an uncategorized URL is visited by many users, it is less likely that the URL is malicious.
HTTP Version	Check HTTP versions	1.0 is older, might be suspicious
Protocol	Compare ports with protocols	Common Protocol-Uncommon Port or Common Port-Uncommon Protocol may indicate malicious traffic
File Name	Entropy analysis on filenames.	May indicate malicious payload delivery