Web Proxy Event Analysis Cheat Sheet

Version 1.0.1
Florian Roth @cyb3rops and the community

Attribute	Less Relevant	Relevant	Highly Relevant
Category	All other categories	Content Delivery Networks Government/Legal Internet Connected Devices Phishing Potentially Unwanted Software Remote Access Suspicious Web Hosting Web Infrastructure	Uncategorized Computer/Information Security Dynamic DNS Host Hacking Malicious Outbound Data/Botnets Malicious Sources/Malnets “Newly Created Domains”
User Agent	-	Random Characters Empty Very Short (<20 Chars, e.g. “Mozilla”) Mozilla/4.0 Mozilla/3.0 Mozilla/2.0 Mozilla * (no slash after Mozilla)	*PowerShell/* Microsoft-CryptoAPI/* CertUtil* Microsoft BITS* * WinHttp* (Macro Downloader) curl/* Googlebot* See User Agent Sigma Rules[1] with “proxy_ua_” prefix
Source System	CERT / CSIRT machines Security Appliances	Workstation Other Servers	Domain Controller Print Server DMZ Server Jump Server Admin Workstation
Blocked File	Files > 10 MB	Not Archived / Extracted Common Archive (ZIP)	Uncommon Archive (RAR, 7z, encrypted Archive) File Extensions: .EXE .PNG .GIF .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .ISO .RAR .7z .JAR
Scan Result	-	-	Scan Errors: Unknown compression, password protected, DLP etc.)
User	-	Regular Users	Service Accounts Domain Administrators Local Administrators Guest Account
Time	-	Regular Work Hours	Outside Regular Work Hours
Bytes In / Out	-	Big requests (uploads)	
SSL/TLS	-	Invalid Certificate Newly Created Certificates	Revoked Certificate
Remote Host	-	Hosting Service (e.g. *.amazonaws.com)	IP address in URL raw.* (e.g. raw.githubusercontent.com)
URL Entropy	-		High Entropy[2]
Method	GET, HEAD	POST	CONNECT POST (without GET from same source)
Target Port			Unequal 443/tcp and 80/tcp

[1] https://github.com/Neo23x0/sigma/tree/master/rules/proxy
[2] https://www.splunk.com/en_us/blog/tips-and-tricks/when-entropy-meets-shannon.html