CyDefSIG: Cyber Defence Signature Sharing Platform, version: 1.1.1

Table of contents

Attribute Categories and Types

Attribute Categories vs Types

Category	Internal reference	Antivirus detection	Payload delivery	Artifacts dropped	Payload installation	Persistence mechanism	Network activity	Payload type	Attribution	External analysis	Other
md5			X	X	X					X	
sha1			X	X	X					X	
filename			X	X	X	X				X	
filename|md5			X	X	X					X	
filename|sha1			X	X	X					X	
ip-src			X				X			X	
ip-dst			X				X			X	
hostname			X				X			X	
domain			X				X			X	
email-src			X								
email-dst			X				X				
email-subject			X								
email-attachment			X								
url			X				X			X	
user-agent			X				X			X	
regkey				X		X				X	
regkey|value				X		X				X	
AS			X				X			X	
snort							X			X	
pattern-in-file			X	X	X		X			X	
pattern-in-traffic			X		X		X			X	
pattern-in-memory				X	X					X	
yara			X	X	X						
vulnerability			X		X					X	
attachment		X	X	X	X		X			X	

malware-sample			X	X	X					X	
link	X	X	X							X	
comment	X	X	X	X	X	X	X	X	X	X	X
text	X	X	X	X	X	X	X	X	X	X	X
other	X	X	X	X	X	X	X	X	X	X	X
Category	**Internal reference**	**Antivirus detection**	**Payload delivery**	**Artifacts dropped**	**Payload installation**	**Persistence mechanism**	**Network activity**	**Payload type**	**Attribution**	**External analysis**	**Other**

Categories

Category	Description
Internal reference	Reference used by the publishing party (e.g. ticket number)
Antivirus detection	List of anti-virus vendors detecting the malware or information on detection performance (e.g. 13/43 or 67%). Attachment with list of detection or link to VirusTotal could be placed here as well.
Payload delivery	Information about the way the malware payload is initially delivered, for example information about the email or web-site, vulnerability used, originating IP etc. Malware sample itself should be attached here.
Artifacts dropped	Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system
Payload installation	Location where the payload was placed in the system and the way it was installed. For example, a filename|md5 type attribute can be added here like this: c:\windows\system32\malicious.exe|41d8cd98f00b204e9800998ecf8427e.
Persistence mechanism	Mechanisms used by the malware to start at boot. This could be a registry key, legitimate driver modification, LNK file in startup
Network activity	Information about network traffic generated by the malware
Payload type	Information about the final payload(s). Can contain a function of the payload, e.g. keylogger, RAT, or a name if identified, such as Poison Ivy.
Attribution	Identification of the group, organisation, or coountry behind the attack
External analysis	Any other result from additional analysis of the malware like tools output Examples: pdf-parser output, automated sandbox analysis, reverse engineering report.
Other	Attributes that are not part of any other category

Types

Type	Description
md5	You are encouraged to use filename|md5 instead. A checksum in md5 format, only use this if you don't know the correct filename
sha1	You are encouraged to use filename|sha1 instead. A checksum in sha1 format, only use this if you don't know the correct filename
filename	Filename
filename|md5	A filename and an md5 hash separated by a | (no spaces)
filename|sha1	A filename and an sha1 hash separated by a | (no spaces)
ip-src	A source IP address of the attacker
ip-dst	A destination IP address of the attacker or C&C server. Also set the IDS flag on when this IP is hardcoded in malware
hostname	A full host/dnsname of an attacker. Also set the IDS flag on when this hostname is hardcoded in malware

domain	A domain name used in the malware. Use this instead of hostname when the upper domain is important or can be used to create links between events.
email-src	The email address (or domainname) used to send the malware.
email-dst	A recipient email address that is not related to your constituency.
email-subject	The subject of the email
email-attachment	File name of the email attachment.
url	url
user-agent	The user-agent used by the malware in the HTTP request.
regkey	Registry key or value
regkey|value	Registry value + data separated by |
AS	Autonomous system
snort	An IDS rule in Snort rule-format. This rule will be automatically rewritten in the NIDS exports.
pattern-in-file	Pattern in file that identifies the malware
pattern-in-traffic	Pattern in network traffic that identifies the malware
pattern-in-memory	Pattern in memory dump that identifies the malware
yara	Yara signature
vulnerability	A reference to the vulnerability used in the exploit
attachment	Please upload files using the ***Upload Attachment*** button.
malware-sample	Please upload files using the ***Upload Attachment*** button.
link	Link to an external information
comment	Comment or description in a human language. This will not be correlated with other attributes (NOT IMPLEMENTED YET)
text	Name, ID or a reference
other	Other attribute