MISP - Malware Information Sharing Platform

Tony Pujals - Prepared for HackMiami - 9/19/2020

What is an “Indicator” (IoC’s)

Why do we collect them?

Industry ISAC sharing

Malware Campaign Tracking

Validating and enriching your siem content

Making sure your vendors are working on threats/Communication with vendors

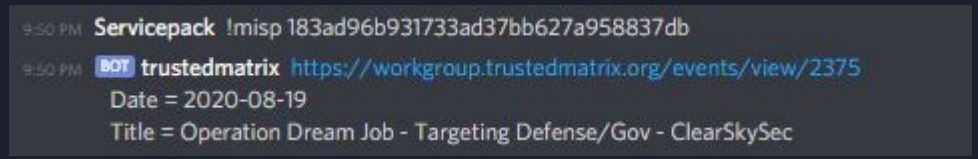
Historical searching and review of data

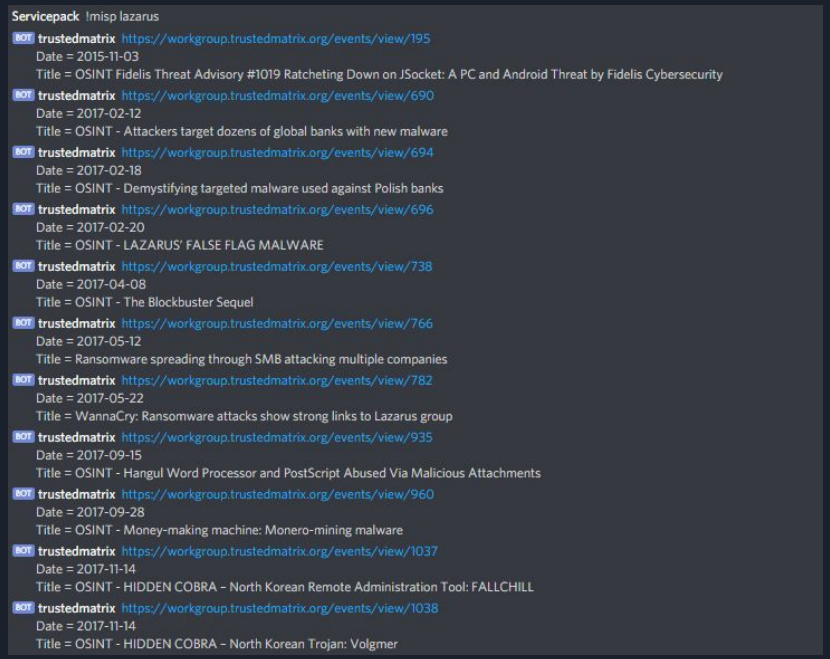
AUTOMATION

Use Cases for MISP

1) Analysts Search/ API search - check against database for indicator/campaign
    a) Skip google dorking and get right to the kind of data you're looking for
    b) The important step of linking the activity back to a publication or blog/writeup
2) Profiling and tracking Threat Actors targeting your organization
    a) att&ck framework behavior
    b) Infrastructure over time
3) Dumping data from dynamic sandboxes into somewhere
4) Connecting the dots between campaigns that are seemingly unrelated
5) Collaborate with your team - making notes and capturing findings
6) Validating your SIEM content is working - Checking visibility - adding context to firing signatures.

Discord Integration





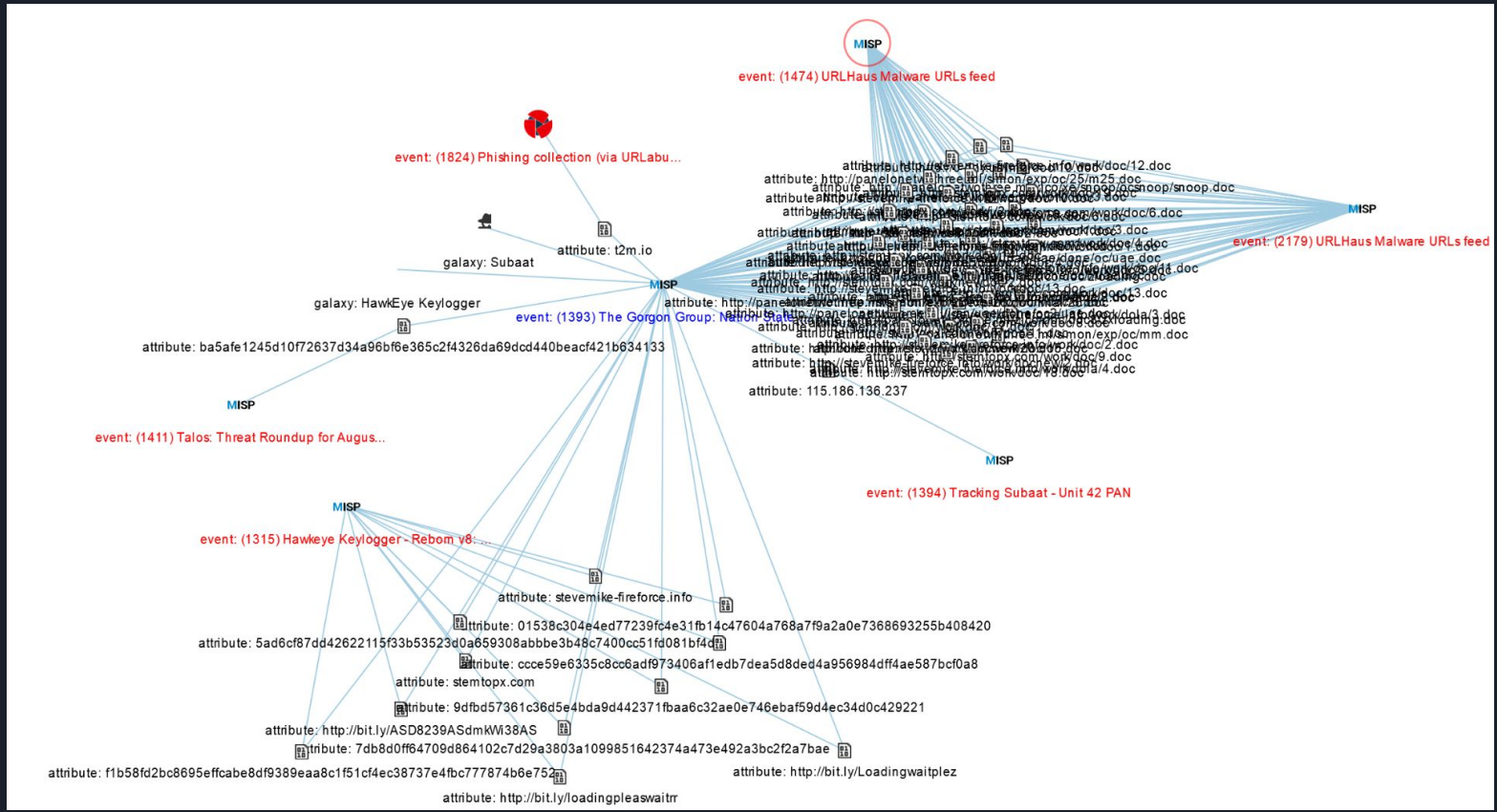
MISP Platform - Adding Data

Sources: AlienVault OTX (AT&T), Palo Alto Unit42 blog, Cisco Talos Blog, IBM X-force exchange, Cylance Blog, SentinelOne/VK_intel, Circl.lu, Botvirj.eu, etc.

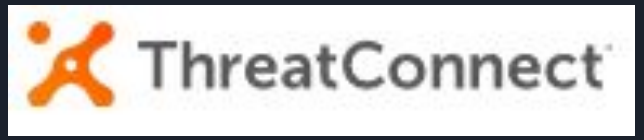
Automated Feeds/Participants ->>

Provider	Org	Source	URL
CIRCL		network	https://www.circl.lu/doc/misp/feed-osint
Botvrij.eu		network	http://www.botvrij.eu/data/feed-osint
inThreat		network	https://feeds.inthreat.com/osint/misp/
zeustracker.abuse.ch		network	https://zeustracker.abuse.ch /blocklist.php?download=ipblocklist
zeustracker.abuse.ch		network	https://zeustracker.abuse.ch /blocklist.php?download=compromised
rules.emergingthreats.net		network	http://rules.emergingthreats.net /blockrules/compromised-ips.txt
malwaredomainlist		network	https://panwdbl.appspot.com/lists /mdl.txt
TOR Node List from dan.me.uk		network	https://www.dan.me.uk/torlist/?exit
TOR Node List from dan.me.uk		network	https://www.dan.me.uk/torlist/
cybercrime-tracker.net		network	http://cybercrime-tracker.net/all.php
http://dns-bh.sagadc.org		network	http://dns-bh.sagadc.org /dynamic_dns.txt
http://labs.snort.org		network	http://labs.snort.org/feeds/ip-filter.blf
longtail.it.marist.edu		network	http://longtail.it.marist.edu/honey /current-ip-addresses.txt
longtail.it.marist.edu		network	http://longtail.it.marist.edu/honey/last-7-days-ip-addresses.txt
pan-unit42		network	https://raw.githubusercontent.com/pan-unit42/iocs/master/diamondfox /diamondfox_panels.txt
booterblacklist.com		network	http://booterblacklist.com /data/booterlist_latest.txt
home.nuug.no		network	https://home.nuug.no/~peter /pop3gropers.txt
Ransomware Tracker abuse.ch		network	https://ransomwaretracker.abuse.ch /feeds/csv/
abuse.ch		network	https://feodotracker.abuse.ch/blocklist /?download=ipblocklist
hosts-file.net		network	https://hosts-file.net/psh.txt

Correlation - the Gorgon Group



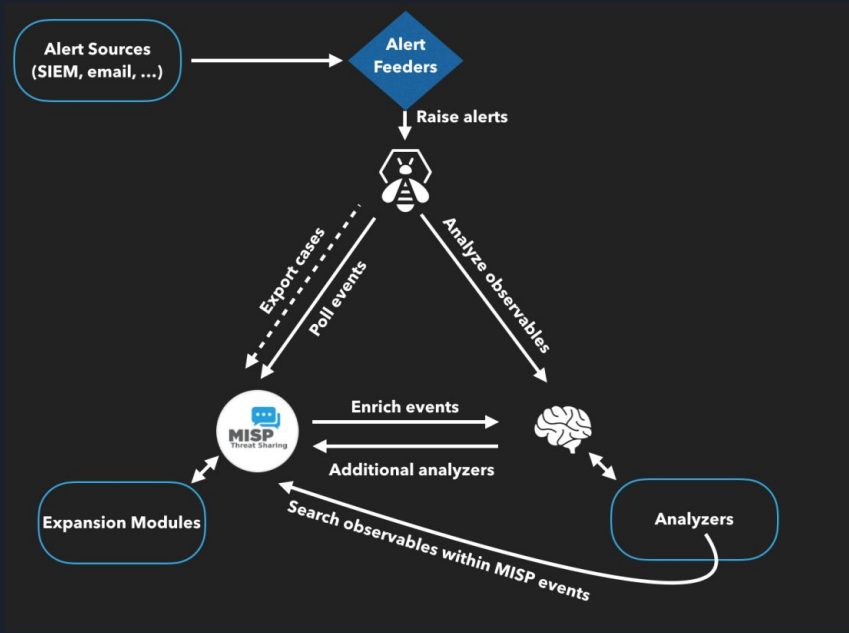
MISP Integrations - Data Enrichment



MISP Hive/Cortex/Maltego integrations

Hive - a Security Incident Response Platform (SIRP). It can receive alerts from different sources (SIEM, IDS, email. etc.) via its REST API.

Allows you to create middleware between the SIEM and the Threat Intel to do searching and observable recording.



Links

https://github.com/MISP/MISP

https://thehive-project.org/

https://www.misp-project.org/