# MISP - Malware Information Sharing Platform

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

# What is an "Indicator" (IoC's)

# domainName IPaddress HashabaRouting bitcoinWallet WhoisRegistrant

# 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

950 PM Servicepack !misp 183ad96b931733ad37bb627a958837db

PM III trustedmatrix https://workgroup.trustedmatrix.org/events/view/2375

Date = 2020-08-19

Title = Operation Dream Job - Targeting Defense/Gov - ClearSkySec

### Servicepack !misp lazarus

trustedmatrix https://workgroup.trustedmatrix.org/events/view/195

Date = 2015-11-03

Title = OSINT Fidelis Threat Advisory #1019 Ratcheting Down on JSocket: A PC and Android Threat by Fidelis Cybersecurity

trustedmatrix https://workgroup.trustedmatrix.org/events/view/690

Date = 2017-02-12

Title = OSINT - Attackers target dozens of global banks with new malware

trustedmatrix https://workgroup.trustedmatrix.org/events/view/694

Date = 2017-02-18

Title = OSINT - Demystifying targeted malware used against Polish banks

trustedmatrix https://workgroup.trustedmatrix.org/events/view/696

Date = 2017-02-20

Title = OSINT - LAZARUS' FALSE FLAG MALWARE

trustedmatrix https://workgroup.trustedmatrix.org/events/view/738

Date = 2017-04-08

Title = OSINT - The Blockbuster Sequel

trustedmatrix https://workgroup.trustedmatrix.org/events/view/766

Date = 2017-05-12

Title = Ransomware spreading through SMB attacking multiple companies

Lot trustedmatrix https://workgroup.trustedmatrix.org/events/view/782
Date = 2017-05-22

Title = WannaCry: Ransomware attacks show strong links to Lazarus group

trustedmatrix https://workgroup.trustedmatrix.org/events/view/935 Date = 2017-09-15

Title = OSINT - Hangul Word Processor and PostScript Abused Via Malicious Attachments

trustedmatrix https://workgroup.trustedmatrix.org/events/view/960

Date = 2017-09-28

Title = OSINT - Money-making machine: Monero-mining malware

trustedmatrix https://workgroup.trustedmatrix.org/events/view/1037

Date = 2017-11-14

Title = OSINT - HIDDEN COBRA - North Korean Remote Administration Tool: FALLCHILL

trustedmatrix https://workgroup.trustedmatrix.org/events/view/1038

Date = 2017-11-14

Title = OSINT - HIDDEN COBRA - North Korean Trojan: Volgmer

Servicepack !misp we11point.com

trustedmatrix https://workgroup.trustedmatrix.org/events/view/129

Date = 2015-07-01

Title = BlackVine - Symantec

trustedmatrix https://workgroup.trustedmatrix.org/events/view/147

Date = 2015-07-28

Title = OSINT Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 by Symantec

trustedmatrix https://workgroup.trustedmatrix.org/events/view/148

Date = 2015-07-30

Title = OSINT Technical Analysis Tracks the Sakula Malware Family by SecureWorks

trustedmatrix https://workgroup.trustedmatrix.org/events/view/203

Date = 2015-11-18 Title = Sakula Reloaded

trustedmatrix https://workgroup.trustedmatrix.org/events/view/1542

Date = 2015-02-09

Title = Black Vine / Deep Panda / APT19 - IBM X-Force - Crowdstrike - Symantec

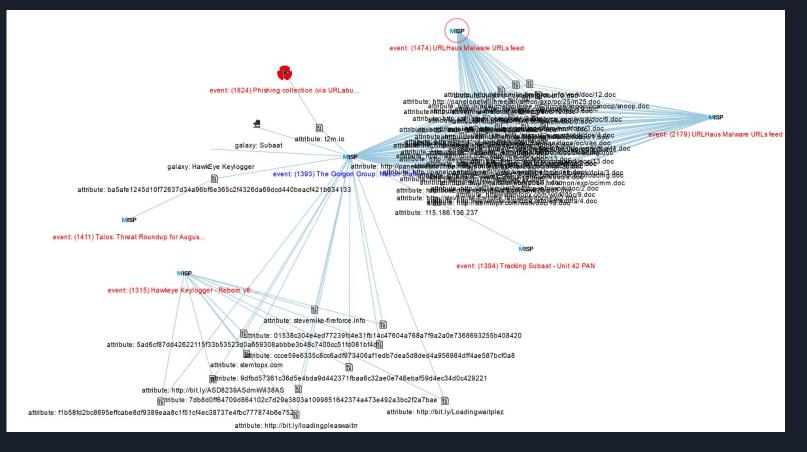
# MISP Platform - Adding Data

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.bt
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.bt
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.bt
booterblacklist.com		network	http://booterblacklist.com /data/booterlist_latest.bt
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.bd

# Correlation - the Gorgon Group



# MISP Integrations - Data Enrichment













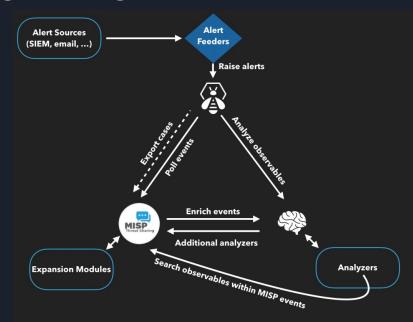
IBM X-Force Exchange



# 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/