TIS Update Sep.

Search/Filter for Country/Industry

- Search in info field
  - attack type: WannaCry, Steganography
  - location: hong kong, taiwan
  - CVE: CVE-2015-5122
  - campaign: pawn storm
  - target: bank, office
- Search in tag field
  - industry: finance
  - platform: win32, androidOS

Tagging

- From source
  - CIRCL, inThreat, Botvrij
- From Orgc name
  - CASES.lu, CERT-RLP, CiviCERT, clearskysec.com, Crimeware, ESET, FOXIT-CERT, INCIBE, NCSC-NL
- From Tag
  - "misp-galaxy:tool=\"Emotet\"" => tool, emotet
  - "osint:source-type=\"blog-post\"" => blog-post
  - "circl:topic=\"finance\"" => finance
- From category
  - "Network activity"
  - "Payload delivery"
- From info

Top Tags

```
1016 "tlp:white"
 394 "Type:OSINT"
 233 "osint:source-type=\"blog-post\""
 204 "circl:incident-classification=\"malware\""
  99 "malware_classification:malware-category=\"Ransomware\""
  97 "ecsirt:malicious-code=\"ransomware\""
  70 "tlp:green"
  68 "misp-galaxy:ransomware=\"Locky\""
  28 "OSINT"
  28 "circl:topic=\"finance\""
  27 "misp-galaxy:threat-actor=\"Sofacy\""
```

```
24 "misp-galaxy:tool=\"Trick Bot\""
22 "osint:source-type=\"technical-report\""
17 "workflow:todo=\"create-missing-misp-galaxy-cluster-values\""
17 "ms-caro-malware:malware-platform=\"AndroidOS\""
16 "workflow:todo=\"create-missing-misp-galaxy-cluster\""
15 "misp-galaxy:ransomware=\"Fake Globe Ransomware\""
14 "ms-caro-malware:malware-type=\"Ransom\""
14 "misp-galaxy:tool=\"Emotet\""
13 "workflow:state=\"incomplete\""
13 "misp-galaxy:ransomware=\"Jaff\""
12 "ms-caro-malware-full:malware-family=\"Banker\""
```

Tags in inThreat

```
15 "Type:OSINT"
15 "tlp:white"
15 "inthreat:event-src=\"feed-osint\""
12 "osint:source-type=block-or-filter-list"
12 "osint:lifetime=ephemeral"
 3 "circl:incident-classification=malware"
 2 "tor:tor-relay-type=exit-relay“
 1 "tor:tor-relay-type="
 1 "osint:lifetime=perpetual"
 1 "osint:certainty=50"
1 "misp-galaxy:Ransomware=\"CryptoWall\""
 1 "malware_classification:malware-category=Trojan"
 1 "malware_classification:malware-category=\"Botnet\""
 1 "europol-event:brute-force-attempt="
 1 "circl:incident-classification=\"system-compromise\""
 1 "circl:incident-classification=\"spam\""
 1 "circl:incident-classification=\"phishing\""
```

Tag from Report

- misp-galaxy
  - tool, ransomware, threat-actor
  - Trick Bot, Emotet, WannaCry, Locky, Sofacy
- Source:
  - OSINT, blog-post, technical-report

Tag List

- Attack type
- Campaign
- Vulnerability
- Location/Country
- Industry
- Platform
- Census Prevalence
- Census Age
- Census Country
- Census Industry
- PAFI Detection Rate

- Source
- Category

Tags from info

- Attack type
- Campaign
- Vulnerability
- Location/Country
- Industry
- Platform

Tags from info

- Attack type by keywords in info
  - attack-type:infostealer
  - attack-type:ransomware
  - attack-type:malspam
  - attack-type:malware
  - attack-type:phishing
  - attack-type:botnet
  - attack-type:backdoor
  - attack-type:spam
  - attack-type:exploit
  - attack-type:APT

Tags from info

- Campaign by keywords in info
  - campaign:”Pawn Storm”
  - campaign:RedOctober
  - campaign:Fareit
  - campaign:Locky
  - campaign:Emotet
  - campaign:Dridex
  - campaign:WannaCry
  - campaign:”Poison Ivy”
  - campaign:APT28

Tags from info

- Vulnerability by CVE or other keywords in info
  - vulnerability:CVE-2014-4114
  - vulnerability:ShellShock
- Location/Country by keywords in info
  - target-location:”Hong Kong”, target-location:Korean, target-location:Russian
- Industry by keywords in info
  - target-industry:finance, target-industry:government

Tags from info

- Platform by keywords in info
  - target-platform:OpenDNS
  - target-platform:”Windows 10”
  - target-platform:”Google Play Store”
  - target-platform:android
  - target-platform:”Flash Player”
  - target-platform:mobile
  - target-platform:infrastructure
  - target-platform:iOS

Keywords in info

- targeting

"20150415D: Fareit Malware Targeting Steam Users from ThreatConnect"

"OSINT Dust Storm Campaign Targeting Japanese Critical Infrastructure"

"OSINT - Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices"

"OSINT - New Poison Ivy Activity Targeting Myanmar, Asian Countries"

"OSINT - Setting Sights On Retail: AbaddonPOS Now Targeting Specific POS Software"

"OSINT - The Curious Case of an Unknown Trojan Targeting German-Speaking Users"

Keywords in info

- exploit, exploit kit

"OSINT Shellshock exploitation from Red Sky Weekly blog post"

"OSINT Angler Exploit Kit Utilizing 302 Cushioning and Domain Shadowing by Zscaler"

"OSINT Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114 by Citizen Lab“

"OSINT Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually From Ransomware Alone by Cisco Talos"

"OSINT Phishing sites and exploit kits december 2015 - part 2 by TechHelpList"

"OSINT Neutrino Exploit Kit – One Flash File to Rule Them All by SpiderLabs"

Keywords in info

- operation

"OSINT - Operation Ghoul: targeted attacks on industrial and engineering organizations"

"OSINT - PSA: Conference Invite used as a Lure by Operation Lotus Blossom Actors"

"OSINT - Operation RAT Cook: Chinese APT actors use fake Game of Thrones leaks as lures"

"OSINT - Operation Groundbait: Espionage in Ukrainian war zones"

Keywords in info

- fake
  - "OSINT - Real News, Fake Flash: Mac OS X Users Targeted"
- APT
  - "OSINT - APT Attack In the Middle East: The Big Bang"
- actor
  - "OSINT - Threat actor goes on a Chrome extension hijacking spree"

Tag from misp galaxy

- misp-galaxy:tool
  - campaign
- misp-galaxy:ransomware
  - attack-type:ransomware
  - campaign
- misp-galaxy:threat-actor
  - campaign

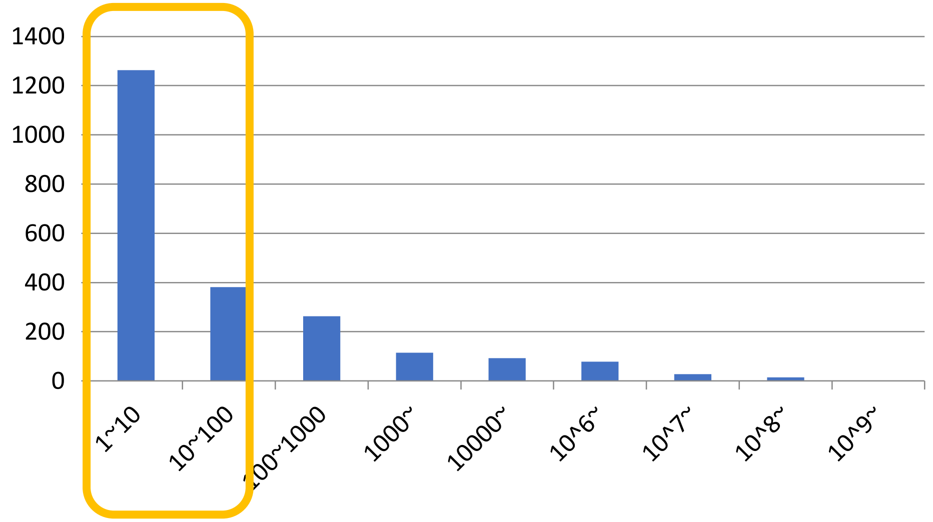
Tag from File Census

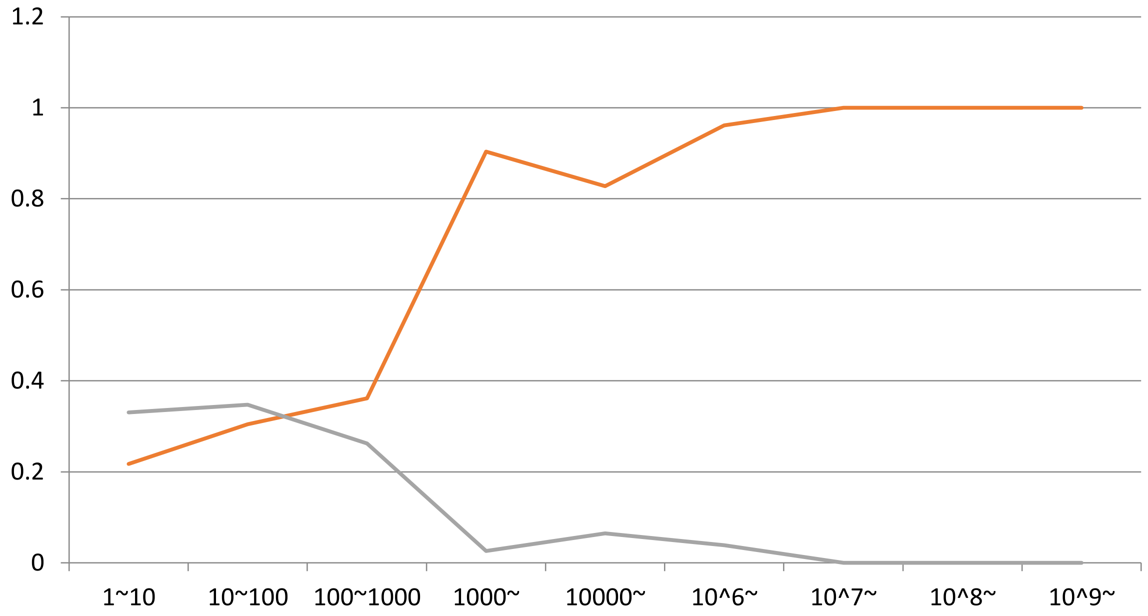
- Prevalence
  - census-prevalence:high >10,000
  - census-prevalence:medium 100~10,000
  - census-prevalence:low <100

- Age
  - census-age:old >1 years
  - census-age:young 1week~1 years
  - census-age:new <1week

Prevalence

	1~10	10~100	100~1000	1000~	10000~	10^6~	10^7~	10^8~	10^9~
All non detect	0.2169	0.3044	0.3612	0.9035	0.8279	0.9615	1	1	1
All detect	0.3301	0.3471	0.2619	0.0263	0.0645	0.0384	0	0	0
Count	1263	381	263	114	93	78	27	14	1
Ratio	0.565	0.170	0.117	0.051	0.041	0.034	0.012	0.0062	0.00044





Tag from File Census

- Country (Top countries?)
  - census-country:TW, census-country:JP, census-country:widespread
  - For countries, Ratio>0.35, Count>10 => top country
- Industry (Top industries?)
  - For icat, Ratio>0.5 (explcude icat:0), Count>10 => top industry

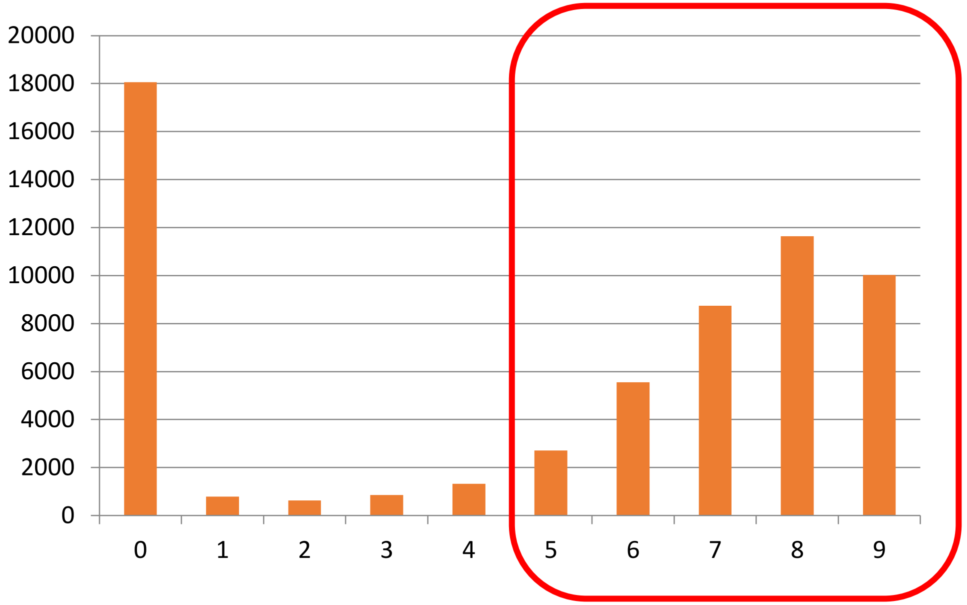
- File Name/path?

Tag from PAFI

- Detection count (For 9 top vendors)
  - pafi-detect-rate:high 5~9
  - pafi-detect-rate:low 1~4
  - pafi-detect-rate:none 0
- Detection name?

PAFI for all Files in CIRCL

0	18061
1	787
2	627
3	858
4	1321
5	2713
6	5558
7	8746
8	11641
9	10024



Tag List

- Attack type
- Campaign
- Vulnerability
- Location/Country
- Industry
- Platform
- Census Prevalence
- Census Age
- Census Country
- Census Industry
- PAFI Detection Rate

- Source
- Category

	e2101519714f8a4056a9de18443bc6e8a1f1b977	bd44d0ab543bf814d93b719c24e90d8dd7111234
Attack Type	APT	ransomware
Campaign	APT28 Sofacy	WannaCry
Vulnerability		
Target Country	Russia	
Target Industry		
Platform		
Census Prevalence	Low	High
Census Age	Old	Old
Census Country		CHN, IND
Census Industry		Government, education
PAFI Detection Rate	None	High
Category	Payload	Dropped
Source	CIRCL	CIRCL

2ea06433f5ae3bffa5896100d5361458

- info: OSINT Analysis of KRIPTOVOR: Infostealer+Ransomware by FireEye
- PAFI: 5/9
- Tags
  - attack-type:infostealer
  - attack-type:ransomware
  - pafi-detect-rate:high

3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe

- info: OSINT Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites by Citizen Labs
- Prev: 1300, Sep. 2011, PAFI:0
- Tags
  - attack-type:malware
  - target-industry:government
  - census-prevalence:medium
  - census-age:old
  - census-country:JPN (574/963, 59%)
  - pafi-detect-rate:none

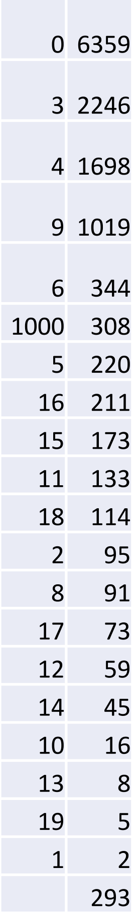
icat	#
0	126
4	21
3	12
13	4
17	2
1	2
1000	2
9	1
8	1
5	1
19	1
N/A	780

e2101519714f8a4056a9de18443bc6e8a1f1b977

- info: OSINT - Part I. Russian APT - APT28 collection of samples including OSX Xagent
- tags: misp-galaxy:threat-actor="Sofacy"
- Prev: 1, Feb 2017, PAFI: 0
- Tags
  - attack-type:APT
  - campaign:APT28
  - campaign:Sofacy
  - target-location:Russia
  - census-prevalence:low
  - census-age:old
  - pafi-detect-rate:none

bd44d0ab543bf814d93b719c24e90d8dd7111234

- info: OSINT - Alert (TA17-132A) Indicators Associated With WannaCry Ransomware
- Prev: 14036, May 2017, PAFI: 9
- Tags
  - attack-type:ransomware
  - campaign:WannaCry
  - prevalence:high
  - age:old
  - ccensus-ountry:CHN (3854, 27%), census-country:IND (2568, 18%)
  - census-icat:government (2246/7677, 29%), census-icat:education (1698/7677, 22%)
  - pafi-detect-rate:high



0	6359
3	2246
4	1698
9	1019
6	344
1000	308
5	220
16	211
15	173
11	133
18	114
2	95
8	91
17	73
12	59
14	45
10	16
13	8
19	5
1	2
	293

3f502030ae1fbd66b033bf236dbe65acac526a203cb7be1594e21de486c2558e

- info: OSINT Expansion on Systematic cyber attacks against Israeli and Palestinian targets going on for a year by Norman
- Prev:1846, Apr. 2013, PAFI:8
- Tags
  - target-location:Israel
  - target-location:Palestine
  - prevalence:medium
  - census-country:USA (325/1369, 24%) census-country:TUR (239/1369, 17%)
  - census-industry:Oil-Gas
  - pafi-detect-rate:high

11	50
0	10
3	7
13	7
4	6
15	3
2	2
17	2
1000	2
16	1
	141

Title	Industry ID
Not specified	0
Communication and Media	1
Healthcare	2
Government	3
Education	4
Financial	5
Food and beverage	6
Fast-Moving Consumer Goods	7
Real estate	8
Manufacturing	9
Media	10
Oil and Gas	11
Banking	12
Energy	13
Retail	14
Technology	15
Telecommunications	16
Transportation	17
Insurance	18
Materials	19
Utilities	20
Others	1000

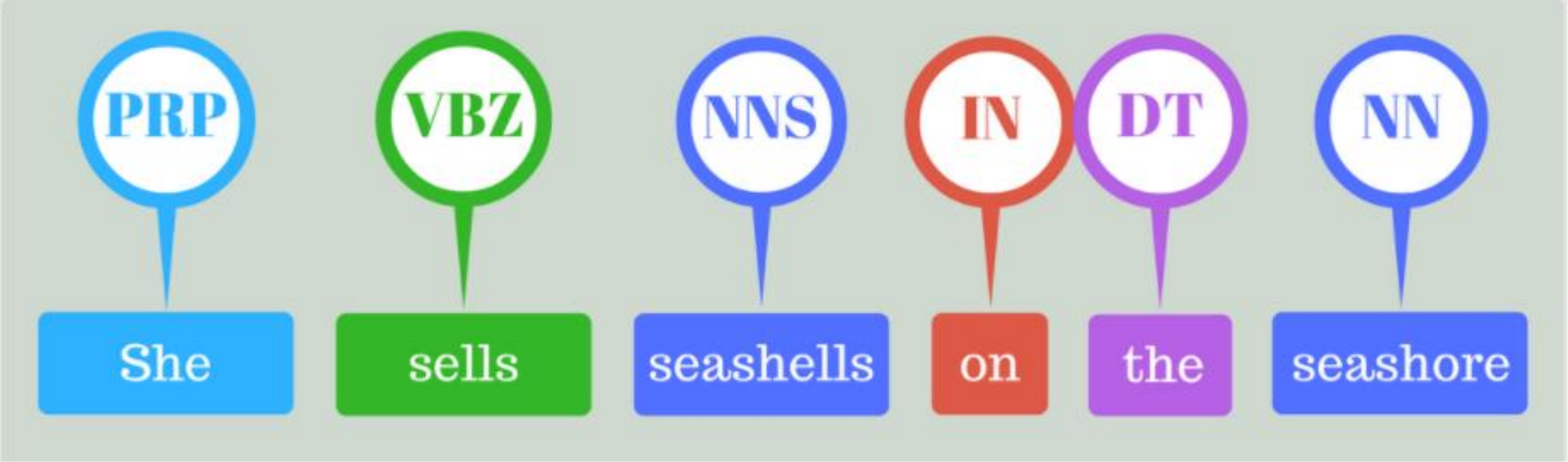
POS for info Tagging

- Fareit Malware Targeting Steam Users from ThreatConnect

  campaign target

- Setting Sights On Retail: AbaddonPOS Now Targeting Specific POS Software

  campaign target



POS for info Tagging

- Use NLP: Part of Speech
- Generate tagging from info/title/comment
- Training data
  - Initial from keyword based method
  - Use report tagging
  - Apply on other feeds
  - From tech news/twitter