Threat Intelligence
...and You

Brought to you by: Pulsedive

What is Cyber Threat Intelligence?

Threat intelligence can be *network-, host-, or behavior*-based information that can be used to *detect, alert, and identify* a cyber threat.

- Suppose Bank#1 confirms malicious traffic from IP address *218.65.30.134*.
- Bank#1 knows that if they see this IP address again, it is probably associated with malicious activity.
- *218.65.30.134* becomes an ***indicator of compromise (IOC)***.

```
Nov 12 14:55:32 S2 unix_chkpwd[10160]: password check failed for user (root)
Nov 12 14:55:32 S2 sshd[10141]: pam_succeed_if(sshd:auth): requirement "uid >=
1000" not met by user "root"
Nov 12 14:55:34 S2 sshd[10141]: Failed password for root from 218.65.30.134 por
t 12777 ssh2
Nov 12 14:55:35 S2 unix_chkpwd[10163]: password check failed for user (root)
Nov 12 14:55:35 S2 sshd[10141]: pam_succeed_if(sshd:auth): requirement "uid >=
1000" not met by user "root"
Nov 12 14:55:37 S2 sshd[10141]: Failed password for root from 218.65.30.134 por
t 12777 ssh2
Nov 12 14:55:37 S2 sshd[10141]: Disconnecting: Too many authentication failures
 for root [preauth]
Nov 12 14:55:37 S2 sshd[10141]: PAM 6 more authentication failures; logname= ui
d=0 euid=0 tty=ssh ruser= rhost=218.65.30.134  user=root
Nov 12 14:55:37 S2 sshd[10141]: PAM service(sshd) ignoring max retries; 7 > 3
Nov 12 14:55:41 S2 sshd[10164]: reverse mapping checking getaddrinfo for 134.30
.65.218.broad.xy.jx.dynamic.163data.com.cn [218.65.30.134] failed - POSSIBLE BR
EAK-IN ATTEMPT!
Nov 12 14:55:41 S2 unix_chkpwd[10167]: password check failed for user (root)
Nov 12 14:55:41 S2 sshd[10164]: pam_unix(sshd:auth): authentication failure; lo
gname= uid=0 euid=0 tty=ssh ruser= rhost=218.65.30.134  user=root
Nov 12 14:55:41 S2 sshd[10164]: pam_succeed_if(sshd:auth): requirement "uid >=
1000" not met by user "root"
Nov 12 14:55:43 S2 unix_chkpwd[10169]: password check failed for user (root)
Nov 12 14:55:43 S2 sshd[10164]: pam_succeed_if(sshd:auth): requirement "uid >=
1000" not met by user "root"
```

SSH logs of real brute force attack from botnet
Organization sees malicious activity

What is Cyber Threat Intelligence?

# IP	# Last Reported	Count	ID
193.201.224.109	# 2017-11-08 19:48:14	40	1379871
217.25.195.237	# 2017-10-24 20:37:48	36	1368394
185.190.58.151	# 2017-11-08 09:59:22	33	1374497
176.119.175.13	# 2017-11-05 07:11:40	31	1369591
185.188.207.25	# 2017-10-23 10:16:57	28	1361323
165.227.71.92	# 2017-11-07 23:21:57	26	1380664
51.15.219.16	# 2017-10-28 16:17:55	25	1359854
213.8.199.27	# 2017-11-09 16:49:34	22	1362341
122.9.27.105	# 2017-10-22 03:29:32	22	1365772
173.249.2.90	# 2017-10-30 01:47:24	22	1363431
93.170.108.240	# 2017-11-05 19:37:41	21	1369568
80.76.245.198	# 2017-11-01 17:04:31	21	1361260
195.154.170.50	# 2017-11-11 00:28:11	21	1382786
111.75.200.68	# 2017-11-06 21:09:48	21	1359699
185.55.218.101	# 2017-11-09 08:24:13	20	1368725
178.132.1.9	# 2017-11-12 12:11:10	20	1362205
222.173.194.9	# 2017-11-02 02:35:56	20	1370407
163.172.167.251	# 2017-11-04 23:39:02	19	1378604

Real threat intelligence feed
Organization publishes findings

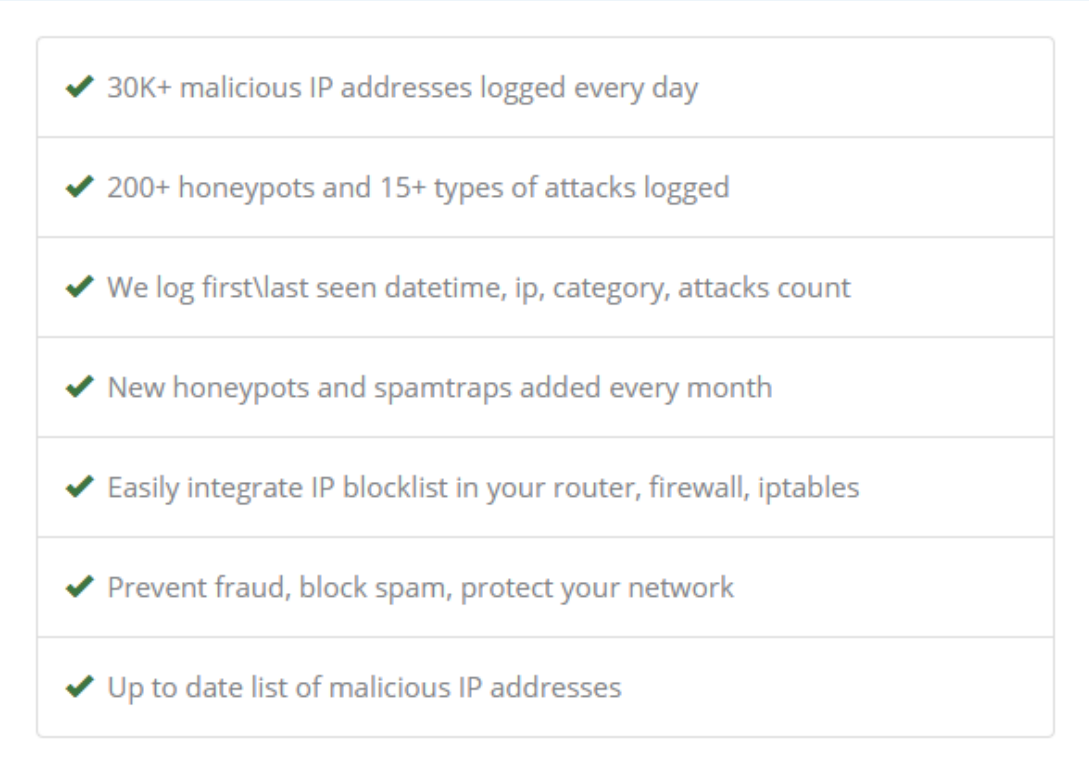
- Bank#1 decides to share this IP address with other organizations.
- They publish a list with this IP and other IPs that can be used to detect similar malicious activity.

- Bank#1 just published a ***threat intelligence feed***.

Creating Threat Intelligence

- Honeypots
- Logs – network, proxy, database, application, etc
- Alerts – IDS/IPS, firewall, endpoint services, etc
- Threat hunting, investigations
- Malware analysis – dynamic, static, etc
- Enriching existing threat intelligence

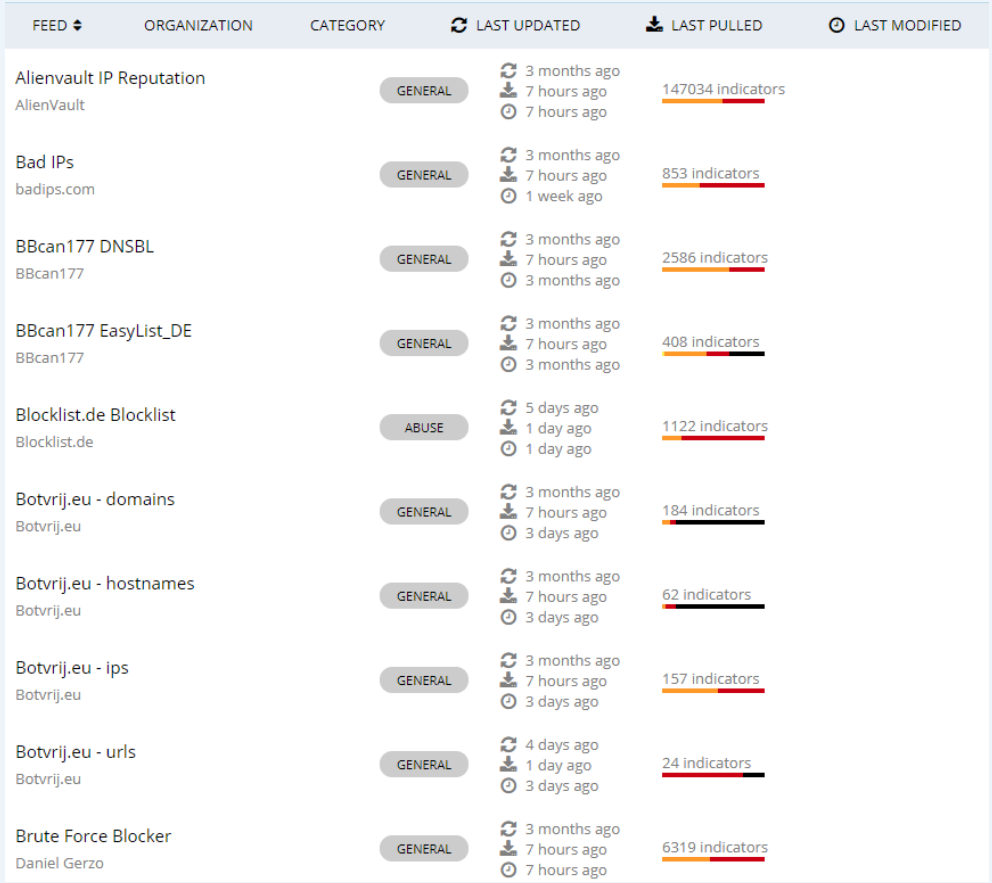
Many established security organizations have a dedicated team for threat intelligence, or are looking to create one.



IPSPamList, a NoVirusThanks service, collects malicious IP addresses using the above methods

It helps to have dedicated people creating threat intelligence

Collecting Threat Intelligence



FEED	ORGANIZATION	CATEGORY	LAST UPDATED	LAST PULLED	LAST MODIFIED
Alienvault IP Reputation	AlienVault	GENERAL	3 months ago	7 hours ago	7 hours ago	147034 indicators
Bad IPs	badips.com	GENERAL	3 months ago	7 hours ago	1 week ago	853 indicators
BBcan177 DNSBL	BBcan177	GENERAL	3 months ago	7 hours ago	3 months ago	2586 indicators
BBcan177 EasyList_DE	BBcan177	GENERAL	3 months ago	7 hours ago	3 months ago	408 indicators
Blocklist.de Blocklist	Blocklist.de	ABUSE	5 days ago	1 day ago	1 day ago	1122 indicators
Botvrij.eu - domains	Botvrij.eu	GENERAL	3 months ago	7 hours ago	3 days ago	184 indicators
Botvrij.eu - hostnames	Botvrij.eu	GENERAL	3 months ago	7 hours ago	3 days ago	62 indicators
Botvrij.eu - ips	Botvrij.eu	GENERAL	3 months ago	7 hours ago	3 days ago	157 indicators
Botvrij.eu - urls	Botvrij.eu	GENERAL	4 days ago	1 day ago	3 days ago	24 indicators
Brute Force Blocker	Daniel Gerzo	GENERAL	3 months ago	7 hours ago	7 hours ago	6319 indicators

Pulsedive is consuming around 40 open-source feeds

- Hundreds of free feeds from websites of non-profits or security firms
- Paid feeds from threat intelligence services and security vendors
- Free/premium mailing lists and community orgs
  - FS-ISAC, real-estate, health, retail, etc

Formats

- Structured data – CSV, XML, JSON, STIX
- Unstructured data – PDF reports, mailing lists
- Sharing protocols – TAXII
- Data models – OpenIOC, CybOX, VERIS

```
version="1.1.1" timestamp="2017-07-07T00:00:00">
    <!-- SOURCE: FED -->
    <stix:STIX_Header>
        <stix:Title>TA17-163B</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators
        </stix:Package_Intent>
        <stix:Description>Crash Override</stix:Description>
        <stix:Handling>
            <marking:Marking>
                <marking:Controlled_Structure>//node() | //@*</marking:Controlled_Structure>
                <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType"
                color="WHITE"/>
                    <marking:Marking_Structure xsi:type=
                    "TOUMarking:TermsOfUseMarkingStructureType">
                        <TOUMarking:Terms_Of_Use>DISCLAIMER: This report is provided "as
                        is" for informational purposes only. The Department of Homeland
                        Security (DHS) does not provide any warranties of any kind
                        regarding any information contained within. The DHS does not
                        endorse any commercial product or service, referenced in this
                        bulletin or otherwise. This document is distributed as TLP:WHITE:
                        Disclosure is not limited. For more information on the Traffic
                        Light Protocol, see http://www.us-cert.gov/tlp.
                        </TOUMarking:Terms_Of_Use>
                    </marking:Marking_Structure>
            </marking:Marking>
        </stix:Handling>
        <stix:Information_Source>
            <stixCommon:Time>
                <cyboxCommon:Produced_Time>2017-07-07T00:00:00</cyboxCommon:Produced_Time>
            </stixCommon:Time>
        </stix:Information_Source>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator id="NCCIC:indicator-ef6cacb0-6336-11e7-b0f9-eccd6dca154b" xsi:type=
        "indicator:IndicatorType">
            <indicator:Title>Malicious IPv4 Indicator</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist
            </indicator:Type>
            <indicator:Observable id=
            "NCCIC:Observable-ef6cacb2-6336-11e7-99da-eccd6dca154b">
                <cybox:Object id="NCCIC:Object-ef6cacb1-6336-11e7-892e-eccd6dca154b">
                    <cybox:Properties xsi:type="AddressObj:AddressObjectType" category=
                    "ipv4-addr" is_spoofed="false">
                        <AddressObj:Address_Value condition="Equals">195.16.88.6
                        </AddressObj:Address_Value>
                    </cybox:Properties>
                </cybox:Object>
```

STIX IOC format example

Attempts to standardize made things worse ☹

Why is it important?

- Can be tailored to industry and company
- Can be disseminated and integrated very quickly
- Peer-reviewed
- Can be used to detect emerging threats shortly after they're observed
- Can reduce "linger time" for new threats
- Not affected by AV/system updates

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA17-181A)
Petya Ransomware

More Alerts

Original release date: July 01, 2017 | Last revised: July 28, 2017

Print | Tweet | Send | Share

Systems Affected

Microsoft Windows operating systems

Overview

This Alert has been updated to reflect the National Cybersecurity and Communications Integration Center's (NCCIC) analysis of the "NotPetya" malware variant.

The scope of this Alert's analysis is limited to the newest Petya malware variant that surfaced on June 27, 2017. This malware is referred to as "NotPetya" throughout this Alert.

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list. Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods.

The NCCIC Code Analysis Team produced a Malware Initial Findings Report (MIFR) to provide in-depth technical analysis of the malware. In coordination with public and private sector partners, NCCIC is also providing additional indicators of compromise (IOCs) in comma-separated-value (CSV) form for information sharing purposes.

Available Files:

- MIFR-10130295.pdf
- MIFR-10130295_stix.xml
- TA-17-181B_IOCs.csv

Description

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

- PsExec - a legitimate Windows administration tool
- WMI - Windows Management Instrumentation, a legitimate Windows component
- EternalBlue - the same Windows SMBv1 exploit used by WannaCry
- EternalRomance - another Windows SMBv1 exploit

Microsoft released a security update for the MS17-010 SMB vulnerability on March 14, 2017, which addressed the EternalBlue and EternalRomance lateral movement techniques.

US-CERT alert regarding Petya Ransomware
Threat intelligence can be disseminated quickly

Good vs Bad IOCs

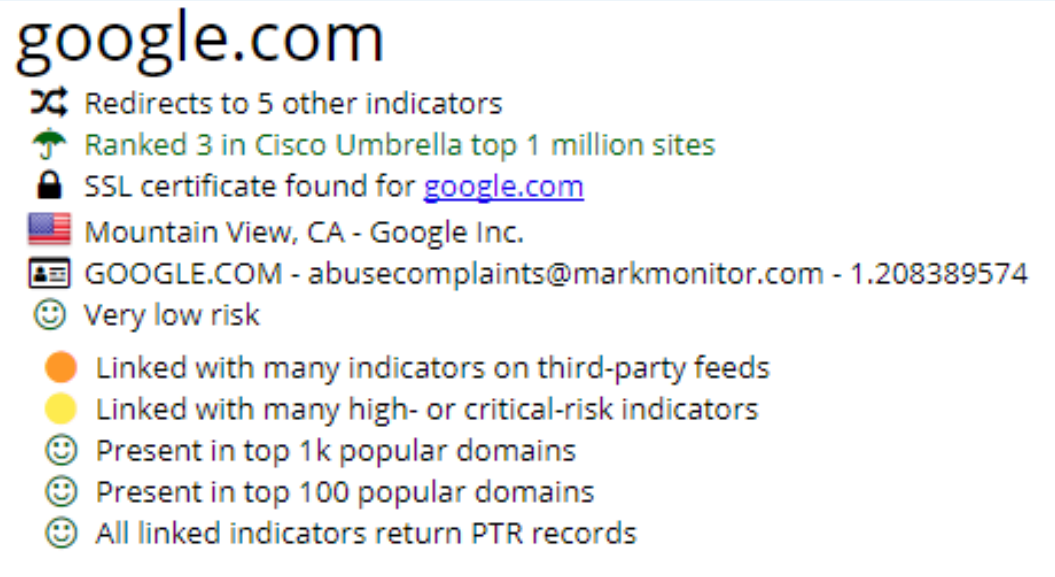
Good

- Unique to malicious activity
- Less specific
  - Domain is preferred over URL
- Not too general either
  - Maybe a netblock or small IP range
- Relevant for longer
  - Behavioral data like unique HTTP header or WHOIS registrant

Bad

- Detects both normal and bad activity
- Too specific
  - Dozens of unique URLs and query strings vs one domain
- Too general
  - An entire ISP, top-level domain, or country
- Changes often
  - Fast flux domain, compromised IP

Vetting



We can use third-party services to vet threat intelligence

- Indicators from third-parties may not be vetted, or may be completely inaccurate
- Vetting indicators using additional services can reduce false positives
- Cisco Umbrella/Alexa top million sites, VirusTotal, WHOIS, and other services can help
- Malicious indicators can be hosted on clean domains… context is important!

Threat Intelligence Platforms

- Used to consume feeds and enrich, correlate, and manage threat intelligence
- There are also companies that provide the intelligence but might not offer a platform
  - RecordedFuture sells human and social intelligence

Integration

- Threat intelligence platform for management
- Upload IOCs (CSV, signatures, etc) to SIEM/Splunk/IDS/IPS/firewall for alerting and detection
- Intelligence from threat hunting, alerts, and investigations can be added back into threat intelligence platform

```
################################################################################
# abuse.ch ZeuS IP blocklist for Snort                                         #
#                                                                              #
# For questions please refer to https://zeustracker.abuse.ch/blocklist.php     #
################################################################################

alert udp $HOME_NET any -> any 53 (msg:"ZeuS Tracker: ZeuS CnC DNS lookup:
0if1nl6.org"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|07|0if1nl6|03|org|00|"; fast_pattern; nocase; threshold: type limit, track
by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004002; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ZeuS Tracker: ZeuS botnet
CnC Traffic detected"; flow:established,to_server; content:"|0d 0a|Host:
0if1nl6.org|0d 0a|"; http_header; fast_pattern; nocase; threshold: type limit, track
by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004003; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"ZeuS Tracker: ZeuS CnC DNS lookup: 0x.x.gg";
content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|02|0x|01|x|02|gg|00|"; fast_pattern; nocase; threshold: type limit, track
by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004004; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ZeuS Tracker: ZeuS botnet
CnC Traffic detected"; flow:established,to_server; content:"|0d 0a|Host: 0x.x.gg|0d
0a|"; http_header; fast_pattern; nocase; threshold: type limit, track by_src, seconds
60, count 1; classtype:trojan-activity; sid:900004005; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"ZeuS Tracker: ZeuS CnC DNS lookup: 54g35546-
5g6hbggffhb.tk"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|14|54g35546-5g6hbggffhb|02|tk|00|"; fast_pattern; nocase; threshold: type
limit, track by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004006;
rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ZeuS Tracker: ZeuS botnet
CnC Traffic detected"; flow:established,to_server; content:"|0d 0a|Host: 54g35546-
5g6hbggffhb.tk|0d 0a|"; http_header; fast_pattern; nocase; threshold: type limit,
track by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004007; rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"ZeuS Tracker: ZeuS CnC DNS lookup:
76tguy6hh6tgftrt7tg.su"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10;
offset:2; content:"|13|76tguy6hh6tgftrt7tg|02|su|00|"; fast_pattern; nocase;
threshold: type limit, track by_src, seconds 60, count 1; classtype:trojan-activity;
sid:900004008; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ZeuS Tracker: ZeuS botnet
CnC Traffic detected"; flow:established,to_server; content:"|0d 0a|Host:
76tguy6hh6tgftrt7tg.su|0d 0a|"; http_header; fast_pattern; nocase; threshold: type
limit, track by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004009;
rev:1;)
alert udp $HOME_NET any -> any 53 (msg:"ZeuS Tracker: ZeuS CnC DNS lookup:
afobal.cl"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|06|afobal|02|cl|00|"; fast_pattern; nocase; threshold: type limit, track
by_src, seconds 60, count 1; classtype:trojan-activity; sid:900004010; rev:1;)
```

Zeus IOCs in Snort rule format

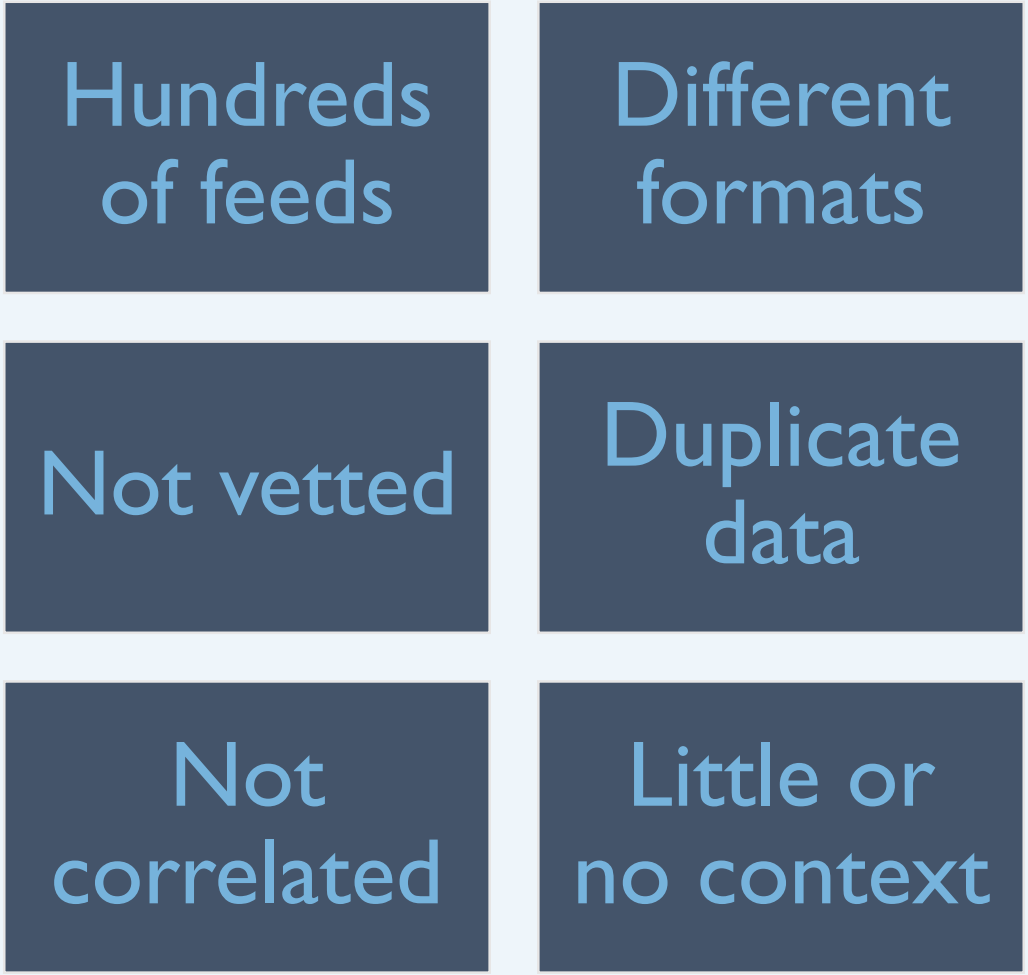
Some feeds already provide rules for blocking, or a threat intelligence platform can create some for you

Problems with Threat Intelligence

- You or another org need to have seen the threat already
- Existing feeds probably don't help much
- Standards add to the mess
- A ton of threat intelligence out there…

How do businesses make threat intelligence actionable?

It can be useful, but the industry hasn't quite figured it all out yet.



Resources

- http://iplists.firehol.org/ – consolidated threat intelligence feed
- https://github.com/hslatman/awesome-threat-intelligence – list of threat intelligence resources and tools
- https://www.sans.org/course/cyber-threat-intelligence – SANS FOR578 Cyber Threat Intelligence certification
- https://pulsedive.com – free community threat intelligence platform

Pulsedive Demo

Thank you!

https://pulsedive.com

@pulsedive

dan@pulsedive.com

LinkedIn