The TIP of the Stinger:

Efficiently Using Threat Intelligence With TheHive

Matthew Gracie
Information Security Engineer

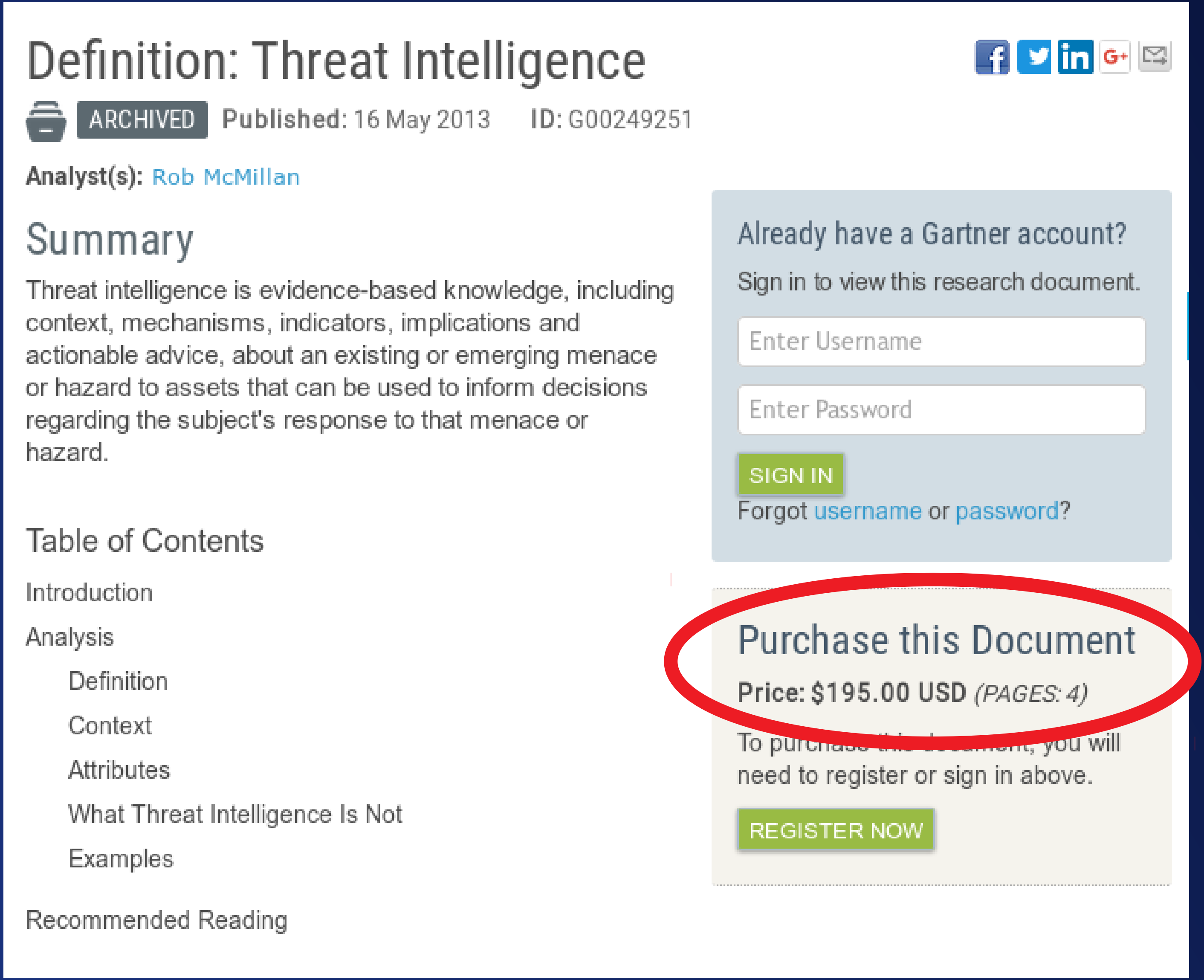
BlueCross BlueShield of Western New York

Who Am I And What Am I Talking About?

What is Threat Intelligence?

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.” --Gartner *

* https://www.gartner.com/doc/2487216/definition-threat-intelligence



Definition: Threat Intelligence

ARCHIVED **Published:** 16 May 2013 **ID:** G00249251

Analyst(s): Rob McMillan

Summary

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Table of Contents

Already have a Gartner account?

Sign in to view this research document.

Enter Username

Enter Password

SIGN IN

Forgot username or password?

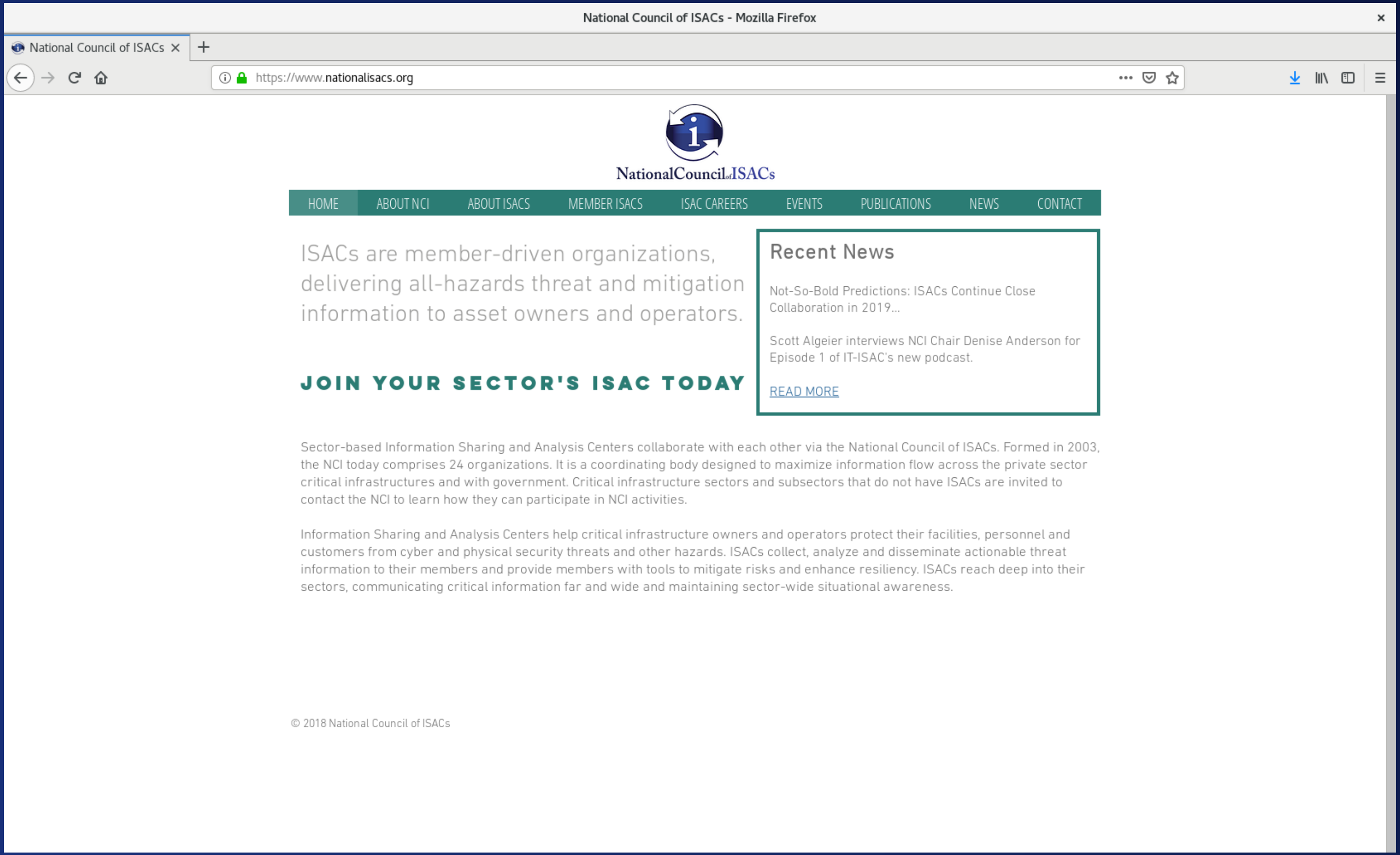
Purchase this Document

Price: $195.00 USD *(PAGES: 4)*

To purchase this document, you will need to register or sign in above.

REGISTER NOW

WHERE DOES HE GET THOSE WONDERFUL IOCS?
imgflip.com



ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.

JOIN YOUR SECTOR'S ISAC TODAY

Recent News

Not-So-Bold Predictions: ISACs Continue Close Collaboration in 2019...

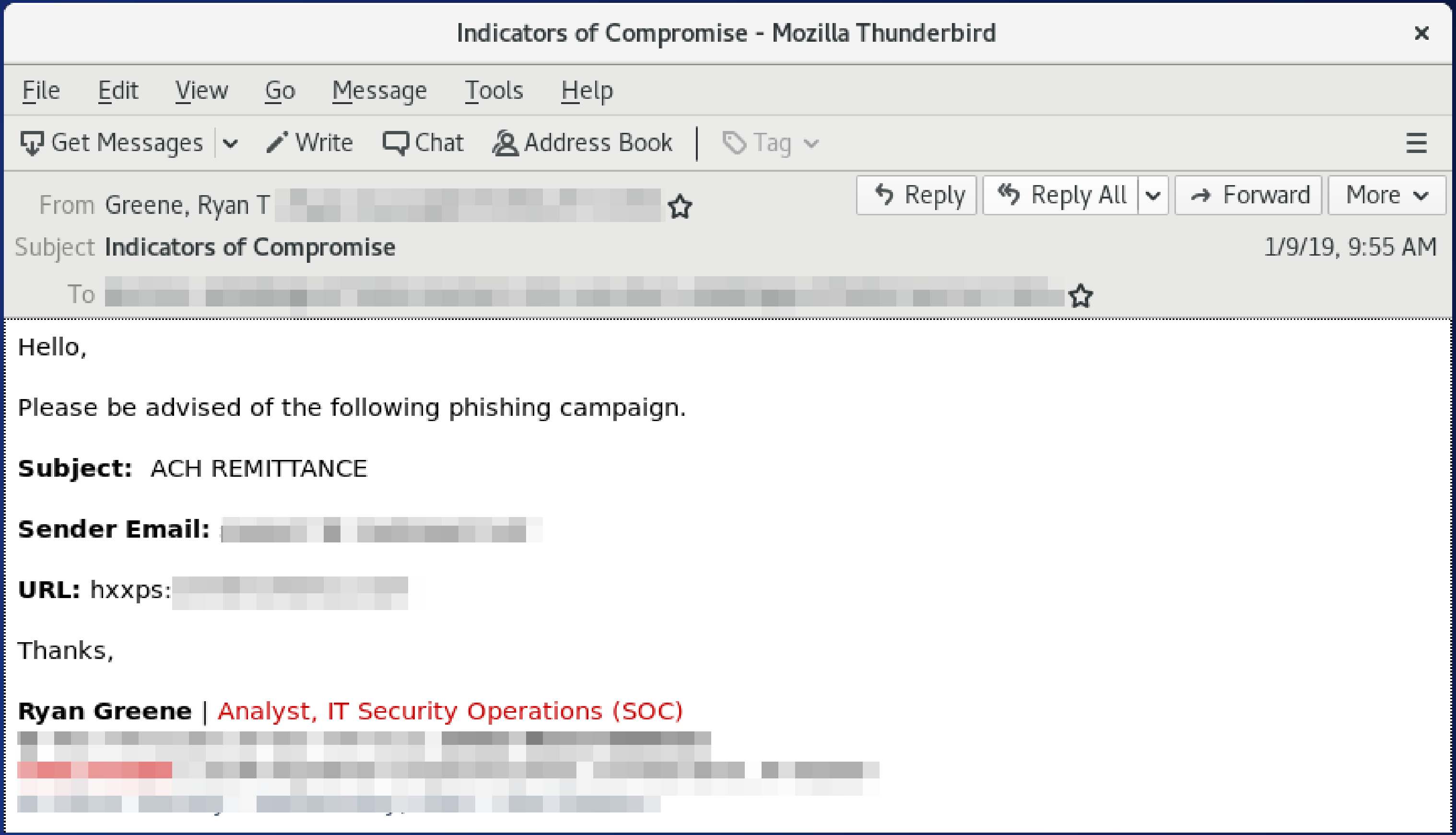
Scott Algeier interviews NCI Chair Denise Anderson for Episode 1 of IT-ISAC's new podcast.

READ MORE

Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 24 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities.

Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

© 2018 National Council of ISACs



From Greene, Ryan T [redacted]

Subject **Indicators of Compromise**

1/9/19, 9:55 AM

To [redacted]

Hello,

Please be advised of the following phishing campaign.

Subject: ACH REMITTANCE

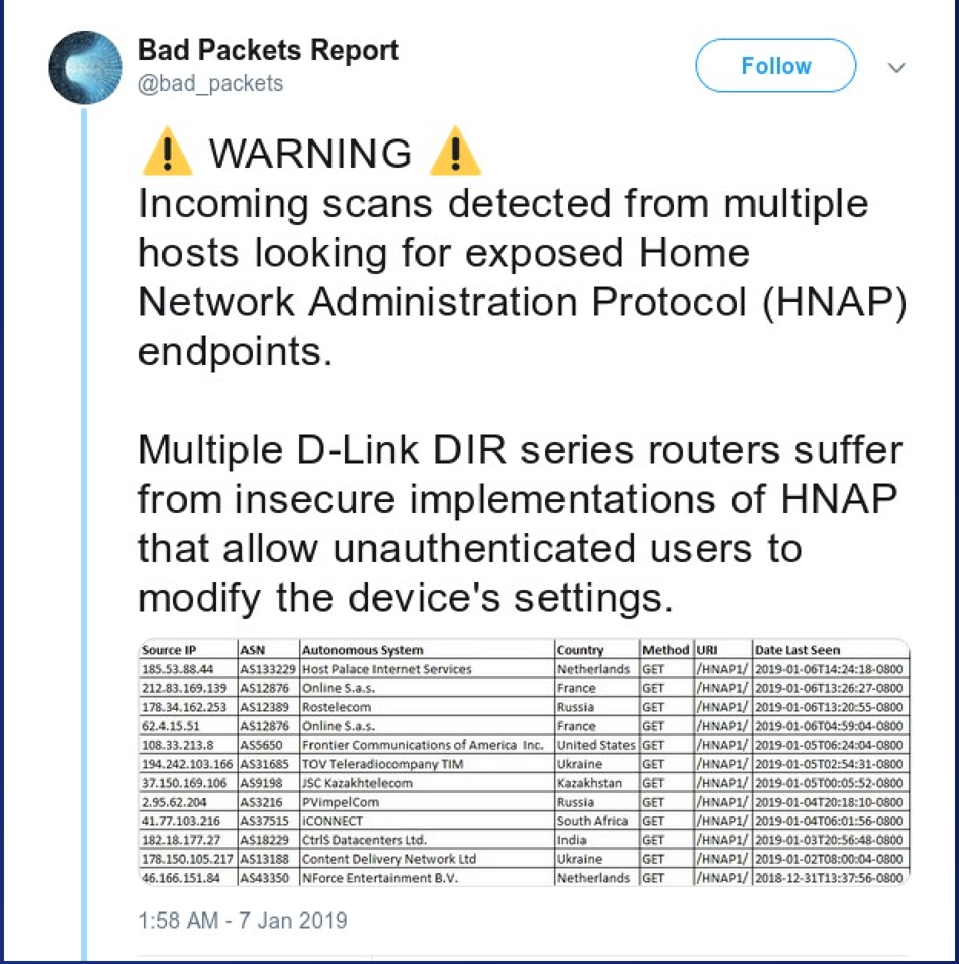
Sender Email: [redacted]

URL: hxxps:[redacted]

Thanks,

Ryan Greene | Analyst, IT Security Operations (SOC)

[redacted]



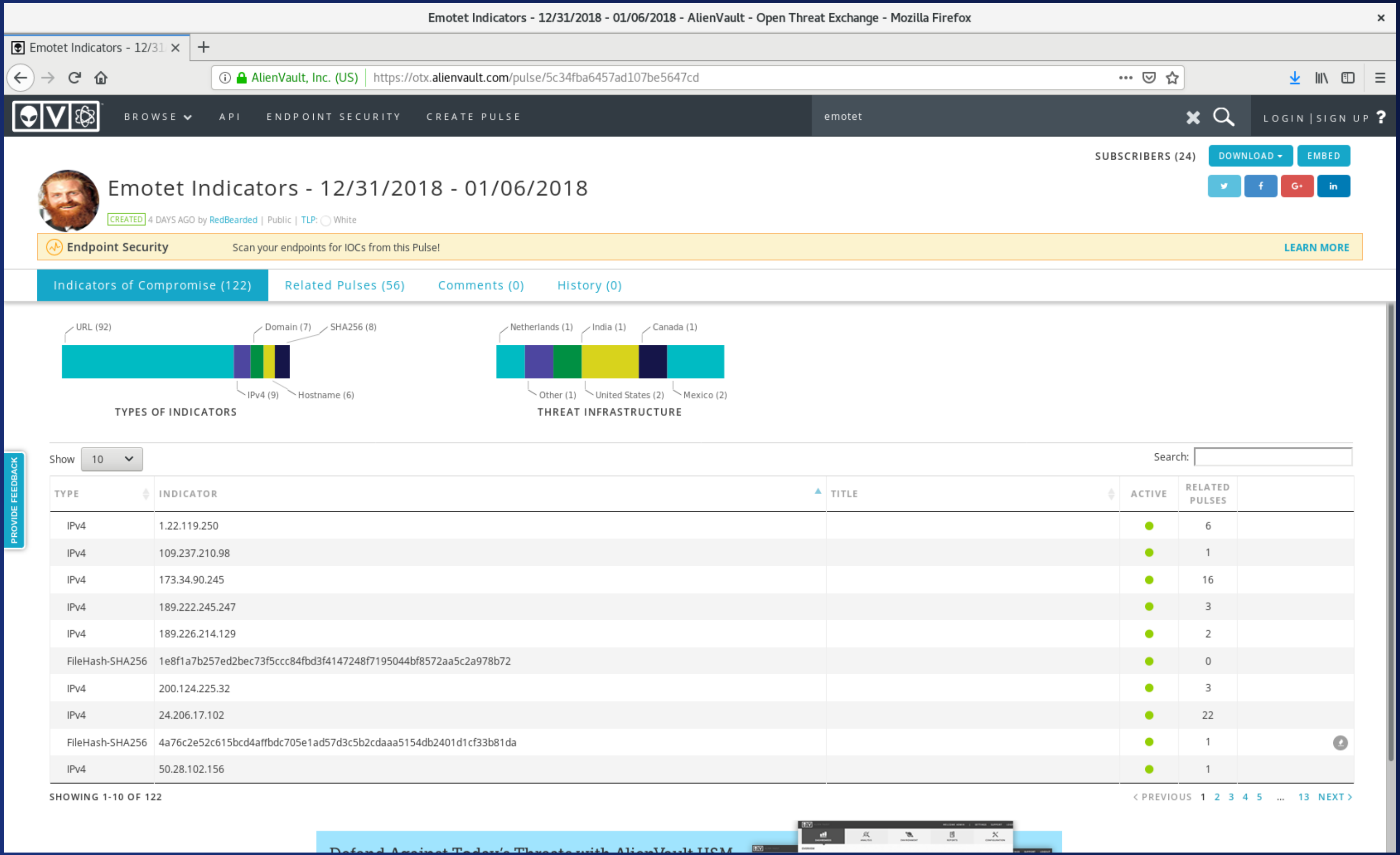
Bad Packets Report
@bad_packets

⚠️ WARNING ⚠️
Incoming scans detected from multiple hosts looking for exposed Home Network Administration Protocol (HNAP) endpoints.

Multiple D-Link DIR series routers suffer from insecure implementations of HNAP that allow unauthenticated users to modify the device's settings.

Source IP	ASN	Autonomous System	Country	Method	URI	Date Last Seen
185.53.88.44	AS133229	Host Palace Internet Services	Netherlands	GET	/HNAP1/	2019-01-06T14:24:18-0800
212.83.169.139	AS12876	Online S.a.s.	France	GET	/HNAP1/	2019-01-06T13:26:27-0800
178.34.162.253	AS12389	Rostelecom	Russia	GET	/HNAP1/	2019-01-06T13:20:55-0800
62.4.15.51	AS12876	Online S.a.s.	France	GET	/HNAP1/	2019-01-06T04:59:04-0800
108.33.213.8	AS5650	Frontier Communications of America Inc.	United States	GET	/HNAP1/	2019-01-05T06:24:04-0800
194.242.103.166	AS31685	TOV Teleradiocompany TIM	Ukraine	GET	/HNAP1/	2019-01-05T02:54:31-0800
37.150.169.106	AS9198	JSC Kazakhtelecom	Kazakhstan	GET	/HNAP1/	2019-01-05T00:05:52-0800
2.95.62.204	AS3216	PVimpelCom	Russia	GET	/HNAP1/	2019-01-04T20:18:10-0800
41.77.103.216	AS37515	iCONNECT	South Africa	GET	/HNAP1/	2019-01-04T06:01:56-0800
182.18.177.27	AS18229	CtrlS Datacenters Ltd.	India	GET	/HNAP1/	2019-01-03T20:56:48-0800
178.150.105.217	AS13188	Content Delivery Network Ltd	Ukraine	GET	/HNAP1/	2019-01-02T08:00:04-0800
46.166.151.84	AS43350	NForce Entertainment B.V.	Netherlands	GET	/HNAP1/	2018-12-31T13:37:56-0800

1:58 AM - 7 Jan 2019



Emotet Indicators - 12/31/2018 - 01/06/2018

CREATED 4 DAYS AGO by RedBearded | Public | TLP: ○ White

Endpoint Security Scan your endpoints for IOCs from this Pulse! LEARN MORE

Indicators of Compromise (122) | Related Pulses (56) | Comments (0) | History (0)

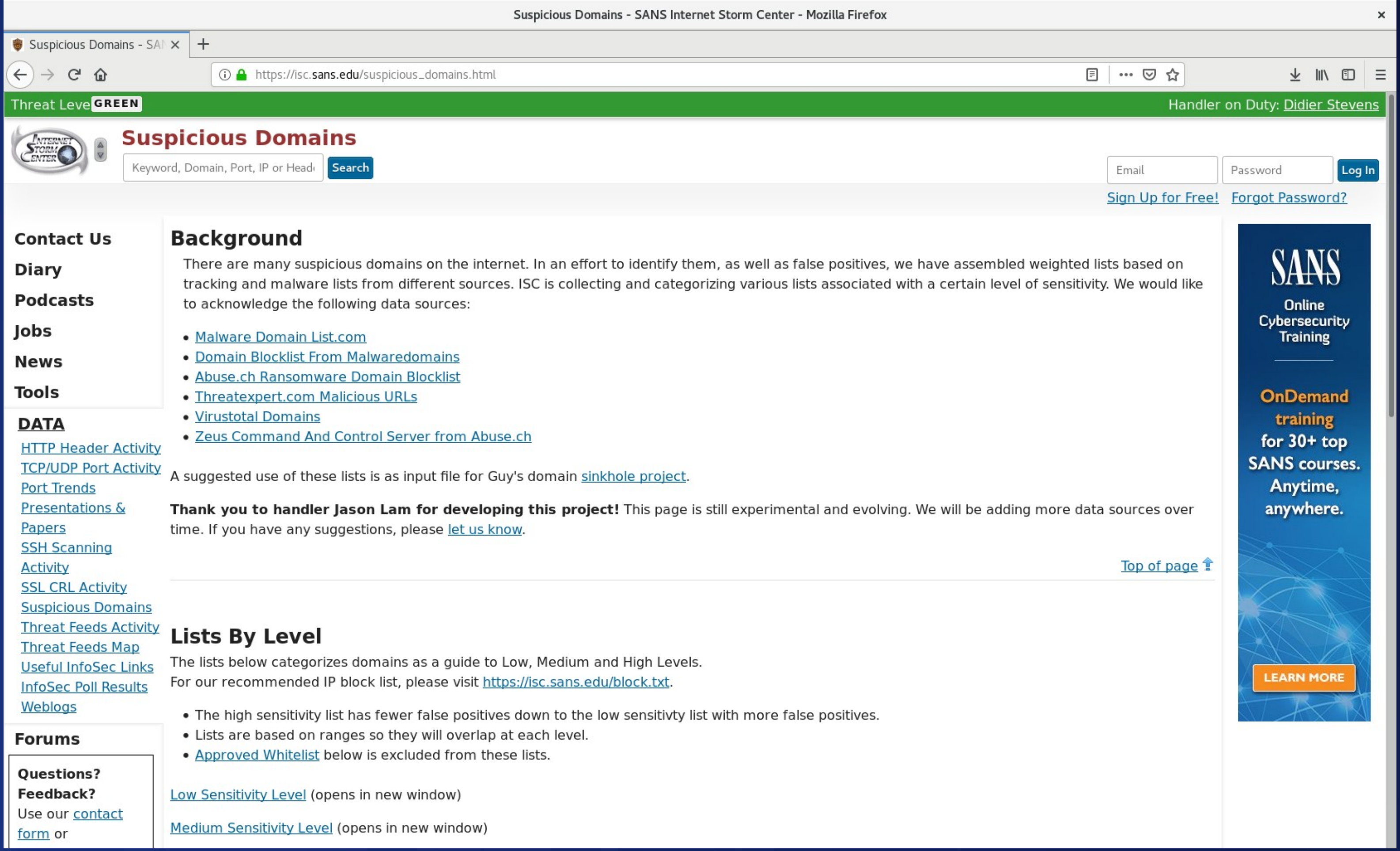
Show 10

Search:

TYPE	INDICATOR	TITLE	ACTIVE	RELATED PULSES
IPv4	1.22.119.250		●	6
IPv4	109.237.210.98		●	1
IPv4	173.34.90.245		●	16
IPv4	189.222.245.247		●	3
IPv4	189.226.214.129		●	2
FileHash-SHA256	1e8f1a7b257ed2bec73f5ccc84fbd3f4147248f7195044bf8572aa5c2a978b72		●	0
IPv4	200.124.225.32		●	3
IPv4	24.206.17.102		●	22
FileHash-SHA256	4a76c2e52c615bcd4affbdc705e1ad57d3c5b2cdaaa5154db2401d1cf33b81da		●	1
IPv4	50.28.102.156		●	1

SHOWING 1-10 OF 122

< PREVIOUS 1 2 3 4 5 ... 13 NEXT >



Suspicious Domains - SANS Internet Storm Center - Mozilla Firefox
Suspicious Domains - SA
https://isc.sans.edu/suspicious_domains.html
Threat Leve GREEN
Handler on Duty: Didier Stevens

Suspicious Domains

Keyword, Domain, Port, IP or Head
Search
Email
Password
Log In
Sign Up for Free!
Forgot Password?

Contact Us
Diary
Podcasts
Jobs
News
Tools

DATA

HTTP Header Activity
TCP/UDP Port Activity
Port Trends
Presentations & Papers
SSH Scanning Activity
SSL CRL Activity
Suspicious Domains
Threat Feeds Activity
Threat Feeds Map
Useful InfoSec Links
InfoSec Poll Results
Weblogs

Forums

Questions? Feedback? Use our contact form or

Background

There are many suspicious domains on the internet. In an effort to identify them, as well as false positives, we have assembled weighted lists based on tracking and malware lists from different sources. ISC is collecting and categorizing various lists associated with a certain level of sensitivity. We would like to acknowledge the following data sources:

- Malware Domain List.com
- Domain Blocklist From Malwaredomains
- Abuse.ch Ransomware Domain Blocklist
- Threatexpert.com Malicious URLs
- Virustotal Domains
- Zeus Command And Control Server from Abuse.ch

A suggested use of these lists is as input file for Guy's domain sinkhole project.

Thank you to handler Jason Lam for developing this project! This page is still experimental and evolving. We will be adding more data sources over time. If you have any suggestions, please let us know.

Top of page

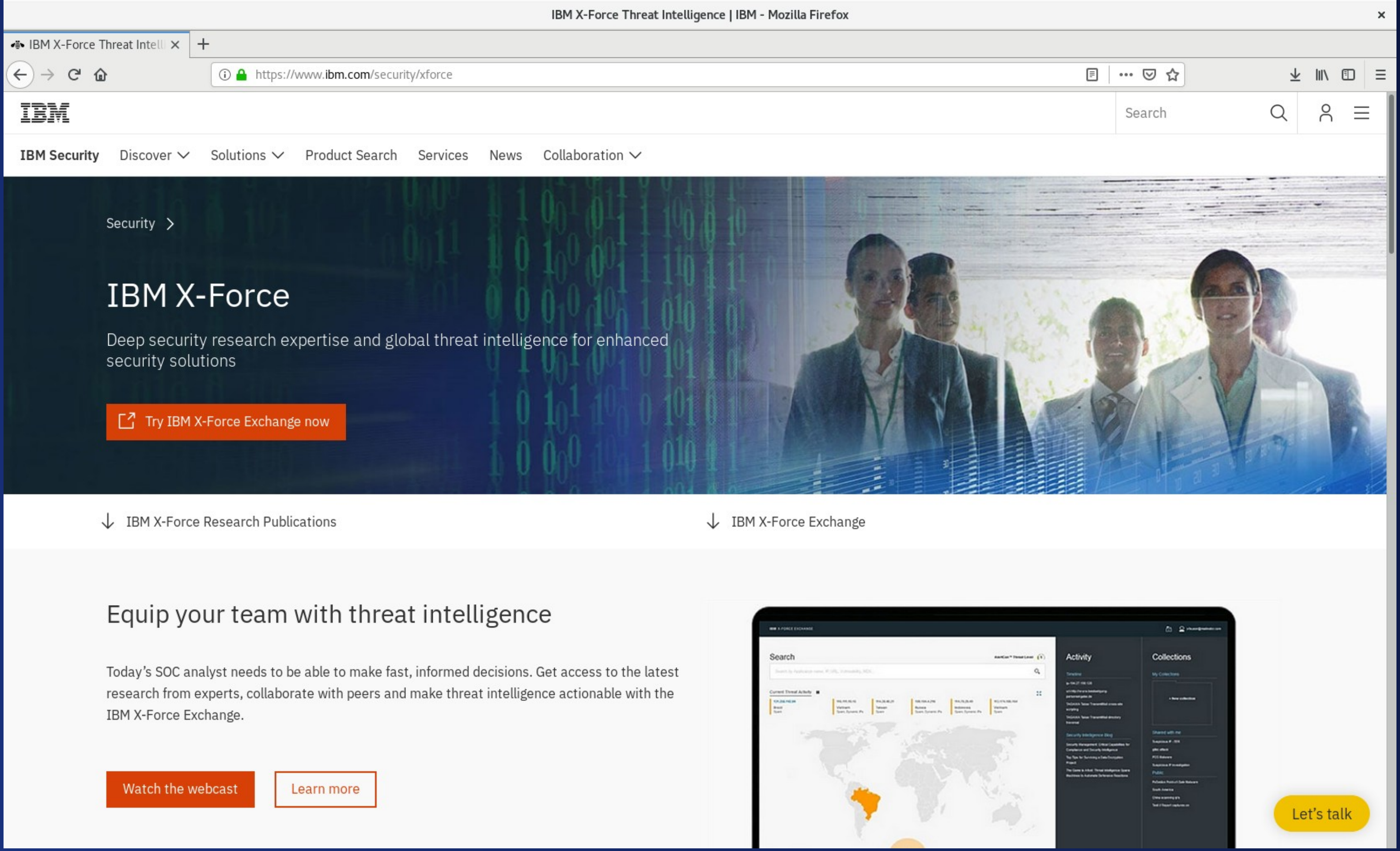
Lists By Level

The lists below categorizes domains as a guide to Low, Medium and High Levels.
For our recommended IP block list, please visit https://isc.sans.edu/block.txt.

- The high sensitivity list has fewer false positives down to the low sensitivty list with more false positives.
- Lists are based on ranges so they will overlap at each level.
- Approved Whitelist below is excluded from these lists.

Low Sensitivity Level (opens in new window)

Medium Sensitivity Level (opens in new window)



IBM X-Force

Deep security research expertise and global threat intelligence for enhanced security solutions

Try IBM X-Force Exchange now

IBM X-Force Research Publications

IBM X-Force Exchange

Equip your team with threat intelligence

Today's SOC analyst needs to be able to make fast, informed decisions. Get access to the latest research from experts, collaborate with peers and make threat intelligence actionable with the IBM X-Force Exchange.

Watch the webcast

Learn more

So How Do We Use It?

MISP

- MISP is an open source Threat Intel Platform
- Collects, sanitizes, and disseminates IOCs
- Supports tagging, TLP, galaxies, taxonomies, and much more
- Robust import and export capabilities
- This is an excellent “system of record”

Getting Data Into MISP

- Manual entry in web console
- Import local MISP JSON or CSV files
- Share data with other MISP instances
- Import .IOC files, Threatconnect, PDF, etc.
- Many third party extensions and add-ons

How Does MISP Structure Data?

- Events
- Attributes
- Tags
- Threat and Analysis Level
- Distribution

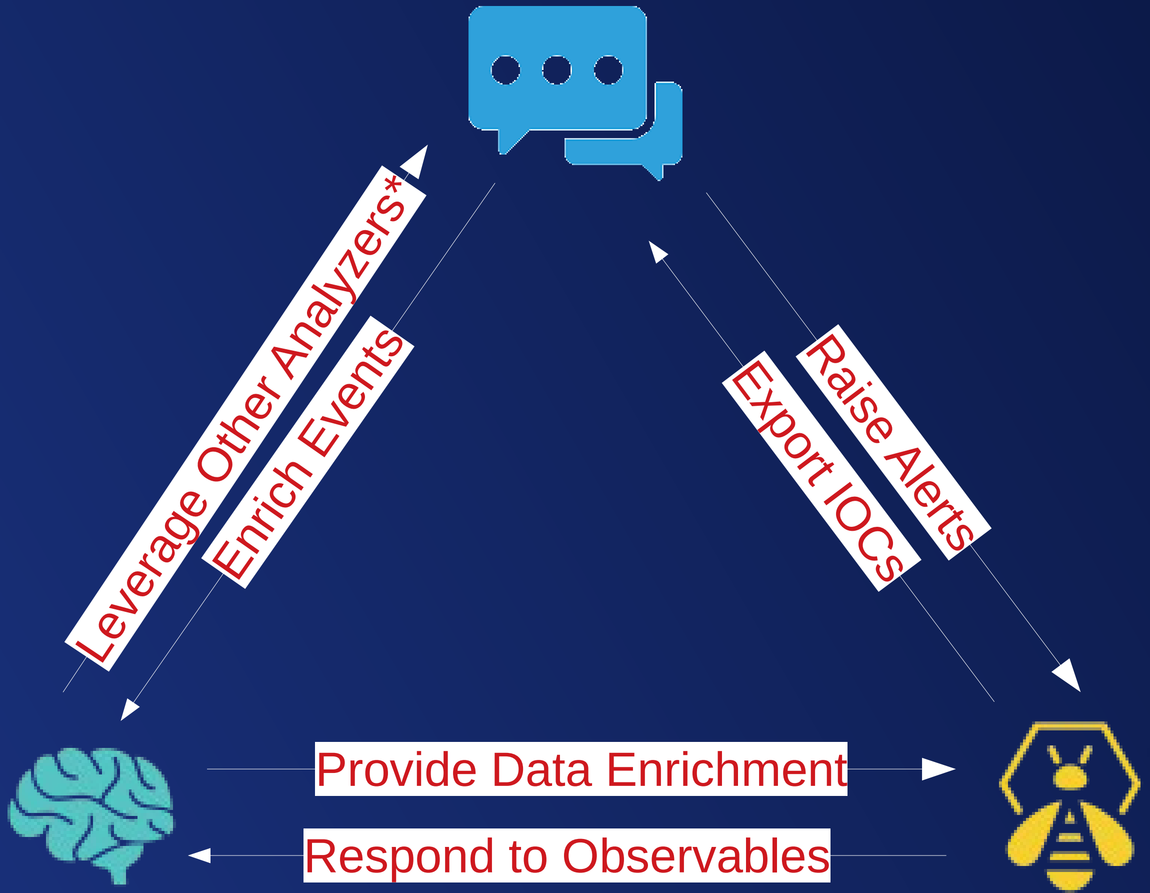
TheHive

- TheHive is an open source SOAR platform
- Allows real-time IR collaboration
- Dashboards and reporting
- Integrates with MISP for threat intel functions
- Alerts, Cases, and Case Templates
- New observables can export back to MISP

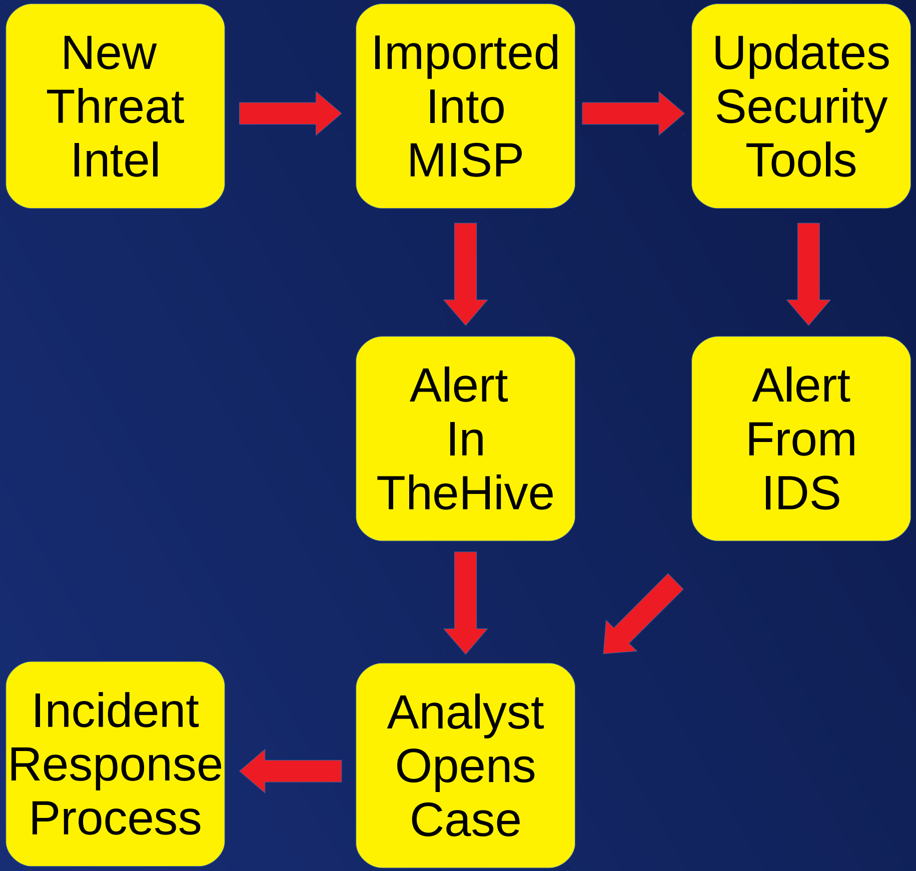
Cortex

- Cortex is an IR automation solution
- “Analyzers” allow enrichment of IOC data
- “Responders” allow scripted responses
- Integrates tightly with TheHive and MISP

Integration



Workflow



New Threat Intel

Imported Into MISP

Updates Security Tools

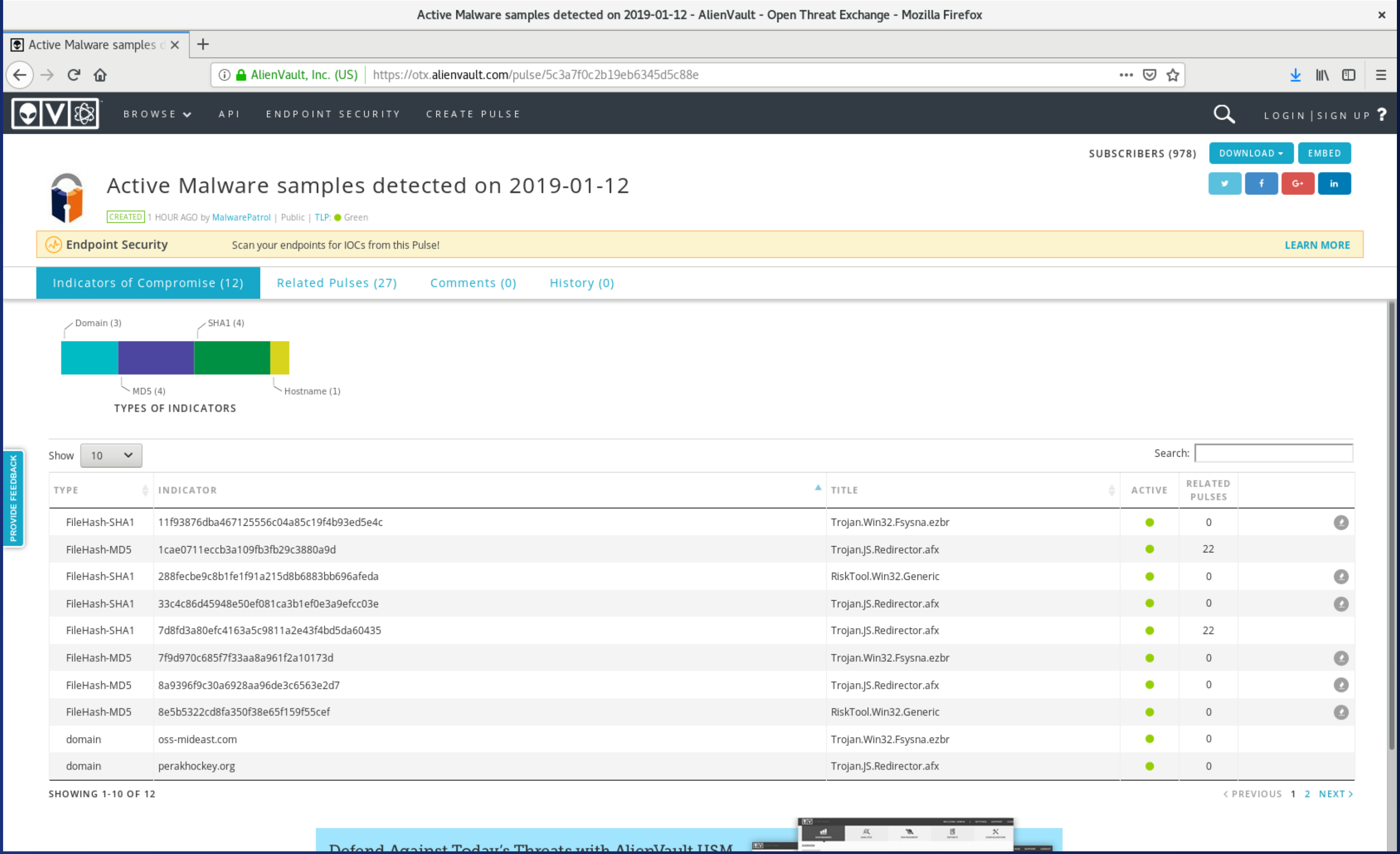
Alert In TheHive

Alert From IDS

Analyst Opens Case

Incident Response Process

Demonstration


Active Malware samples detected on 2019-01-12 - AlienVault - Open Threat Exchange - Mozilla Firefox
Active Malware samples c
AlienVault, Inc. (US)
https://otx.alienvault.com/pulse/5c3a7f0c2b19eb6345d5c88e
BROWSE
API
ENDPOINT SECURITY
CREATE PULSE
LOGIN | SIGN UP
SUBSCRIBERS (978)
DOWNLOAD
EMBED
PROVIDE FEEDBACK

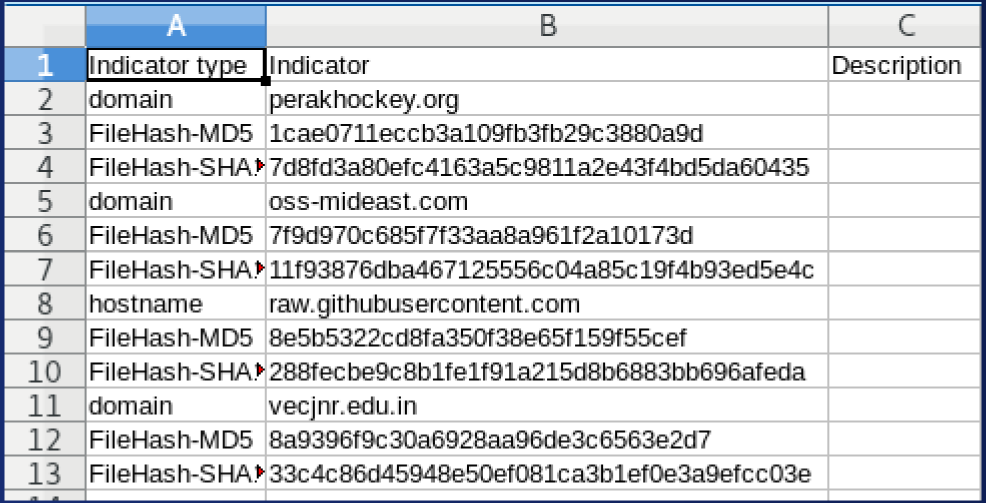
Active Malware samples detected on 2019-01-12

CREATED 1 HOUR AGO by MalwarePatrol | Public | TLP: ● Green

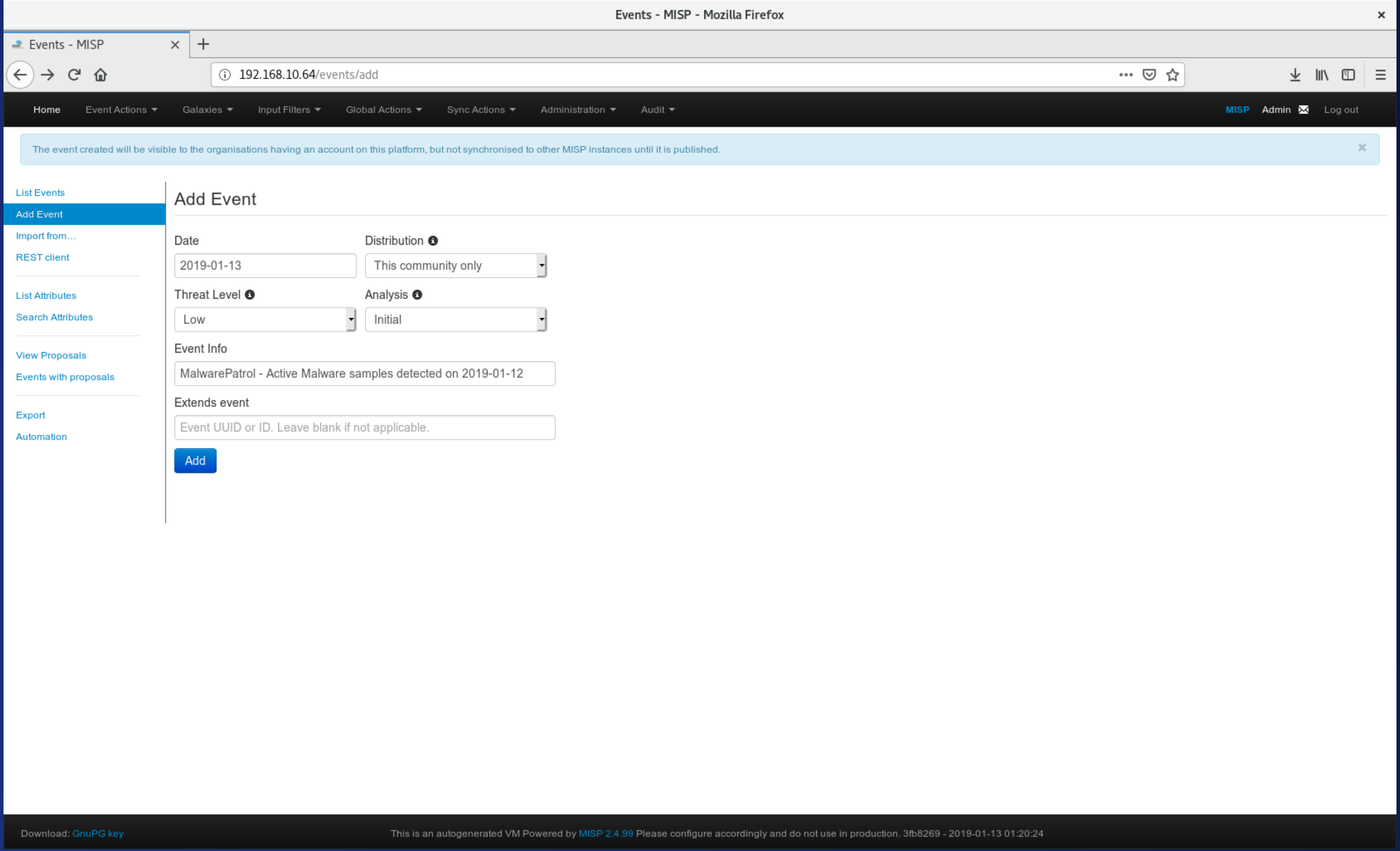
Endpoint Security Scan your endpoints for IOCs from this Pulse! LEARN MORE

TYPE	INDICATOR	TITLE	ACTIVE	RELATED PULSES
FileHash-SHA1	11f93876dba467125556c04a85c19f4b93ed5e4c	Trojan.Win32.Fsysna.ezbr	●	0
FileHash-MD5	1cae0711eccb3a109fb3fb29c3880a9d	Trojan.JS.Redirector.afx	●	22
FileHash-SHA1	288fecbe9c8b1fe1f91a215d8b6883bb696afeda	RiskTool.Win32.Generic	●	0
FileHash-SHA1	33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e	Trojan.JS.Redirector.afx	●	0
FileHash-SHA1	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435	Trojan.JS.Redirector.afx	●	22
FileHash-MD5	7f9d970c685f7f33aa8a961f2a10173d	Trojan.Win32.Fsysna.ezbr	●	0
FileHash-MD5	8a9396f9c30a6928aa96de3c6563e2d7	Trojan.JS.Redirector.afx	●	0
FileHash-MD5	8e5b5322cd8fa350f38e65f159f55cef	RiskTool.Win32.Generic	●	0
domain	oss-mideast.com	Trojan.Win32.Fsysna.ezbr	●	0
domain	perakhockey.org	Trojan.JS.Redirector.afx	●	0

SHOWING 1-10 OF 12



	A	B	C
1	Indicator type	Indicator	Description
2	domain	perakhockey.org	
3	FileHash-MD5	1cae0711eccb3a109fb3fb29c3880a9d	
4	FileHash-SHA	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435	
5	domain	oss-mideast.com	
6	FileHash-MD5	7f9d970c685f7f33aa8a961f2a10173d	
7	FileHash-SHA	11f93876dba467125556c04a85c19f4b93ed5e4c	
8	hostname	raw.githubusercontent.com	
9	FileHash-MD5	8e5b5322cd8fa350f38e65f159f55cef	
10	FileHash-SHA	288fecbe9c8b1fe1f91a215d8b6883bb696afeda	
11	domain	vecjnr.edu.in	
12	FileHash-MD5	8a9396f9c30a6928aa96de3c6563e2d7	
13	FileHash-SHA	33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e	



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.

Add Event

Date: 2019-01-13

Distribution: This community only

Threat Level: Low

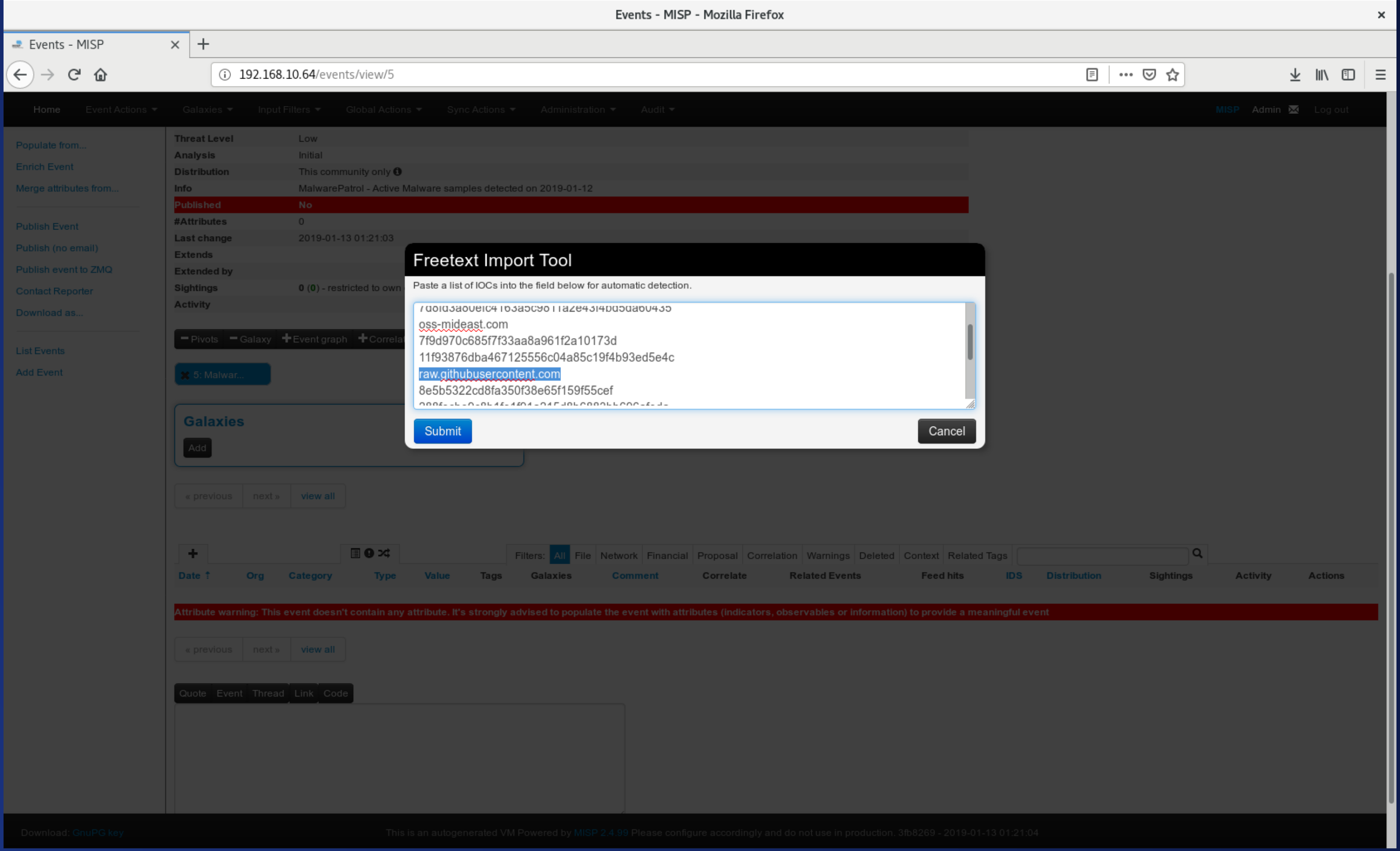
Analysis: Initial

Event Info: MalwarePatrol - Active Malware samples detected on 2019-01-12

Extends event: Event UUID or ID. Leave blank if not applicable.

Download: GnuPG key

This is an autogenerated VM Powered by MISP 2.4.99 Please configure accordingly and do not use in production. 3fb8269 - 2019-01-13 01:20:24



Threat Level	Low
Analysis	Initial
Distribution	This community only
Info	MalwarePatrol - Active Malware samples detected on 2019-01-12
Published	No
#Attributes	0
Last change	2019-01-13 01:21:03
Extends	
Extended by	
Sightings	0 (0) - restricted to own
Activity	

Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event

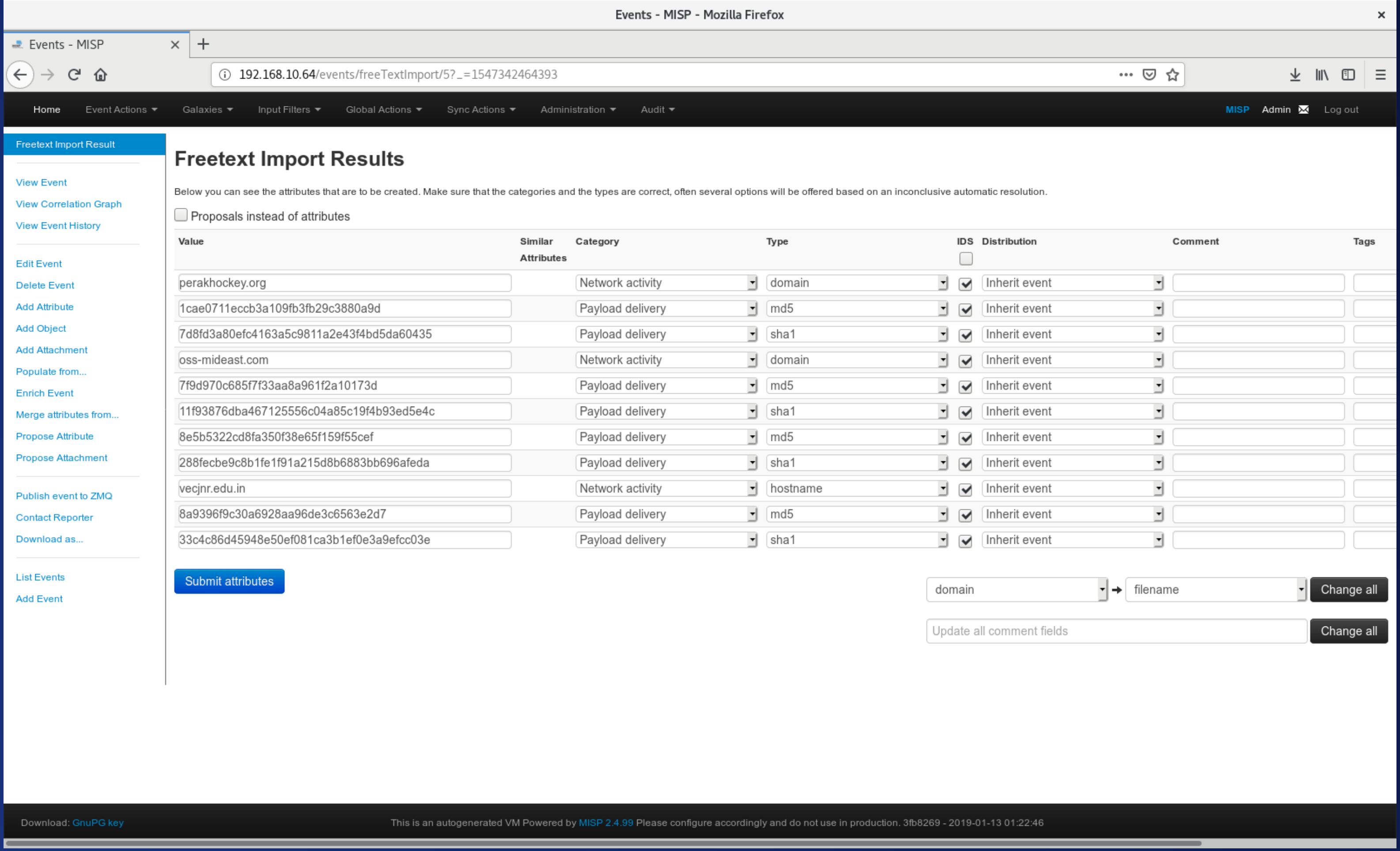
Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

```
oss-mideast.com
7f9d970c685f7f33aa8a961f2a10173d
11f93876dba467125556c04a85c19f4b93ed5e4c
raw.githubusercontent.com
8e5b5322cd8fa350f38e65f159f55cef
```

Download: GnuPG key

This is an autogenerated VM Powered by MISP 2.4.99 Please configure accordingly and do not use in production. 3fb8269 - 2019-01-13 01:21:04



Freetext Import Results

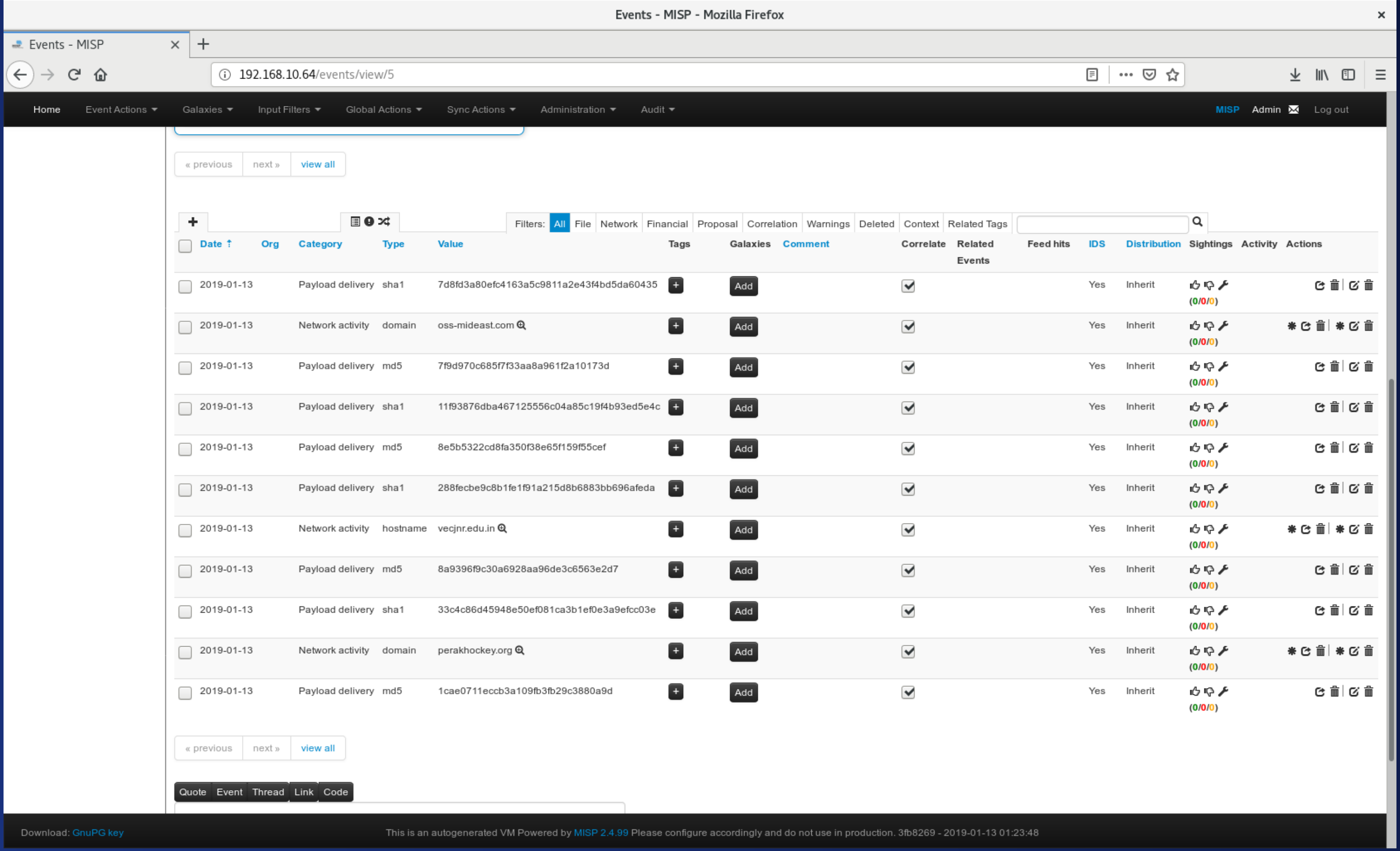
Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

□ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS □	Distribution	Comment	Tags
perakhockey.org		Network activity	domain	☑	Inherit event		
1cae0711eccb3a109fb3fb29c3880a9d		Payload delivery	md5	☑	Inherit event		
7d8fd3a80efc4163a5c9811a2e43f4bd5da60435		Payload delivery	sha1	☑	Inherit event		
oss-mideast.com		Network activity	domain	☑	Inherit event		
7f9d970c685f7f33aa8a961f2a10173d		Payload delivery	md5	☑	Inherit event		
11f93876dba467125556c04a85c19f4b93ed5e4c		Payload delivery	sha1	☑	Inherit event		
8e5b5322cd8fa350f38e65f159f55cef		Payload delivery	md5	☑	Inherit event		
288fecbe9c8b1fe1f91a215d8b6883bb696afeda		Payload delivery	sha1	☑	Inherit event		
vecjnr.edu.in		Network activity	hostname	☑	Inherit event		
8a9396f9c30a6928aa96de3c6563e2d7		Payload delivery	md5	☑	Inherit event		
33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e		Payload delivery	sha1	☑	Inherit event		

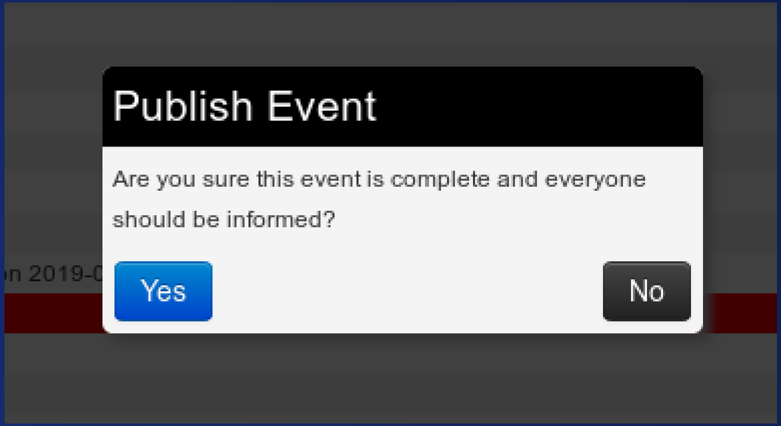
Download: GnuPG key

This is an autogenerated VM Powered by MISP 2.4.99 Please configure accordingly and do not use in production. 3fb8269 - 2019-01-13 01:22:46



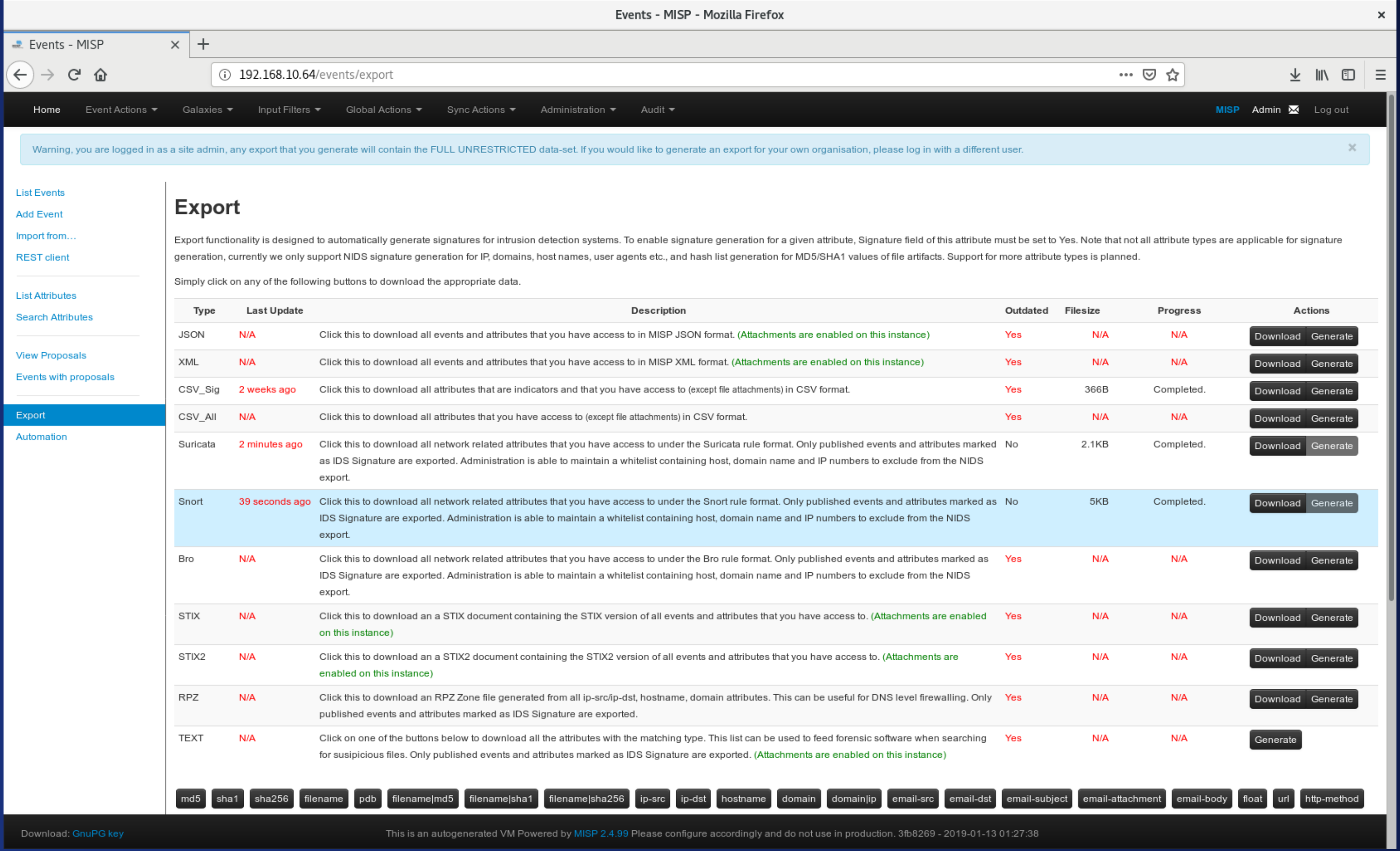
□	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2019-01-13		Payload delivery	sha1	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Network activity	domain	oss-mideast.com	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	md5	7f9d970c685f7f33aa8a961f2a10173d	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	sha1	11f93876dba467125556c04a85c19f4b93ed5e4c	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	md5	8e5b5322cd8fa350f38e65f159f55cef	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	sha1	288fecbe9c8b1fe1f91a215d8b6883bb696afeda	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Network activity	hostname	vecjnr.edu.in	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	md5	8a9396f9c30a6928aa96de3c6563e2d7	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	sha1	33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Network activity	domain	perakhockey.org	+	Add		☑			Yes	Inherit	(0/0/0)		
□	2019-01-13		Payload delivery	md5	1cae0711eccb3a109fb3fb29c3880a9d	+	Add		☑			Yes	Inherit	(0/0/0)		

This is an autogenerated VM Powered by MISP 2.4.99 Please configure accordingly and do not use in production. 3fb8269 - 2019-01-13 01:23:48



Publish Event

Are you sure this event is complete and everyone should be informed?



Warning, you are logged in as a site admin, any export that you generate will contain the FULL UNRESTRICTED data-set. If you would like to generate an export for your own organisation, please log in with a different user.

Export

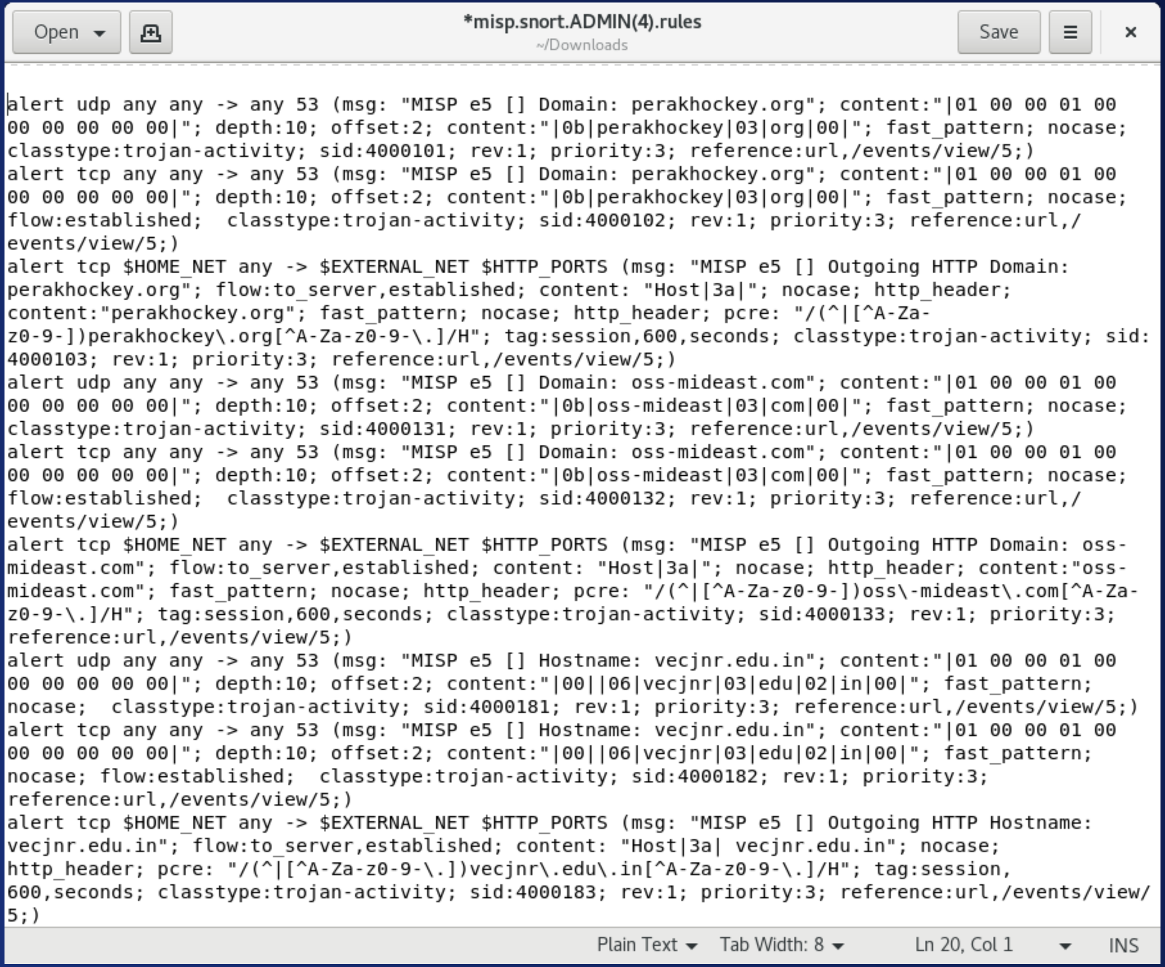
Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

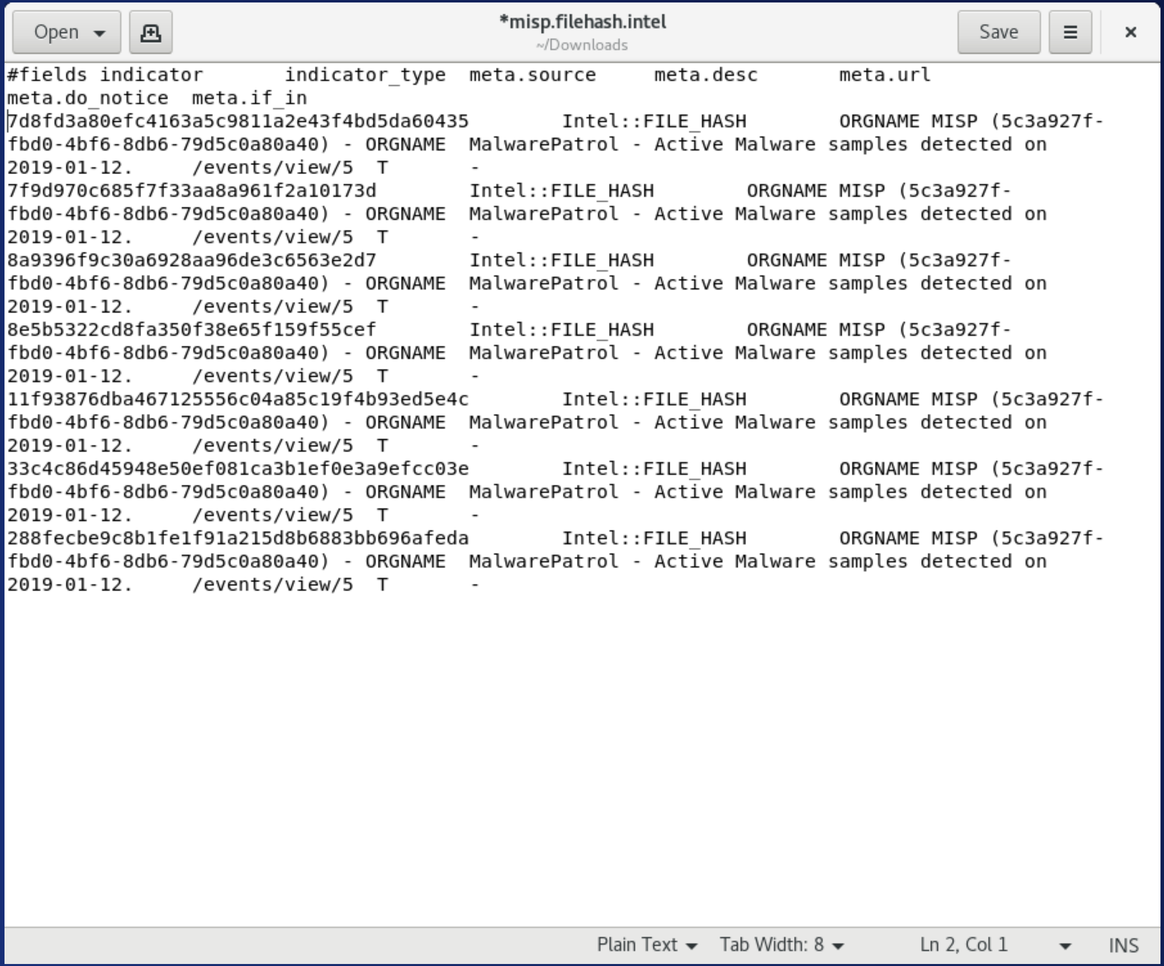
Type	Last Update	Description	Outdated	Filesize	Progress	Actions
JSON	N/A	Click this to download all events and attributes that you have access to in MISP JSON format. (Attachments are enabled on this instance)	Yes	N/A	N/A	Download Generate
XML	N/A	Click this to download all events and attributes that you have access to in MISP XML format. (Attachments are enabled on this instance)	Yes	N/A	N/A	Download Generate
CSV_Sig	2 weeks ago	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	366B	Completed.	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	N/A	N/A	Download Generate
Suricata	2 minutes ago	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	No	2.1KB	Completed.	Download Generate
Snort	39 seconds ago	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	No	5KB	Completed.	Download Generate
Bro	N/A	Click this to download all network related attributes that you have access to under the Bro rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
STIX	N/A	Click this to download an a STIX document containing the STIX version of all events and attributes that you have access to. (Attachments are enabled on this instance)	Yes	N/A	N/A	Download Generate
STIX2	N/A	Click this to download an a STIX2 document containing the STIX2 version of all events and attributes that you have access to. (Attachments are enabled on this instance)	Yes	N/A	N/A	Download Generate
RPZ	N/A	Click this to download an RPZ Zone file generated from all ip-src/ip-dst, hostname, domain attributes. This can be useful for DNS level firewalling. Only published events and attributes marked as IDS Signature are exported.	Yes	N/A	N/A	Download Generate
TEXT	N/A	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked as IDS Signature are exported. (Attachments are enabled on this instance)	Yes	N/A	N/A	Generate

Download: GnuPG key

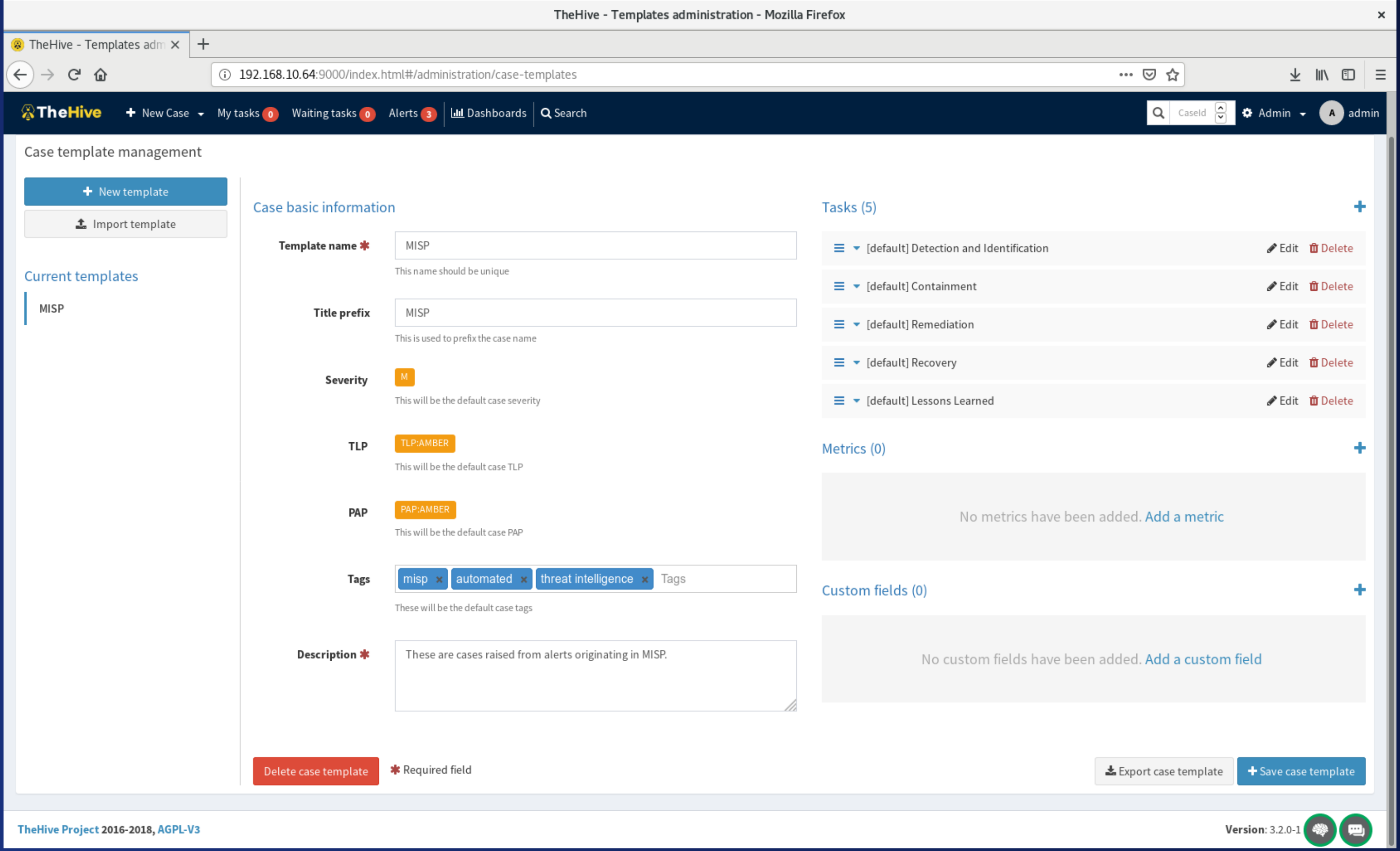
This is an autogenerated VM Powered by MISP 2.4.99 Please configure accordingly and do not use in production. 3fb8269 - 2019-01-13 01:27:38



```
alert udp any any -> any 53 (msg: "MISP e5 [] Domain: perakhockey.org"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|0b|perakhockey|03|org|00|"; fast_pattern; nocase;
classtype:trojan-activity; sid:4000101; rev:1; priority:3; reference:url,/events/view/5;)
alert tcp any any -> any 53 (msg: "MISP e5 [] Domain: perakhockey.org"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|0b|perakhockey|03|org|00|"; fast_pattern; nocase;
flow:established;  classtype:trojan-activity; sid:4000102; rev:1; priority:3; reference:url,/
events/view/5;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e5 [] Outgoing HTTP Domain:
perakhockey.org"; flow:to_server,established; content: "Host|3a|"; nocase; http_header;
content:"perakhockey.org"; fast_pattern; nocase; http_header; pcre: "/(^|[^A-Za-
z0-9-])perakhockey\.org[^A-Za-z0-9-\.]/H"; tag:session,600,seconds; classtype:trojan-activity; sid:
4000103; rev:1; priority:3; reference:url,/events/view/5;)
alert udp any any -> any 53 (msg: "MISP e5 [] Domain: oss-mideast.com"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|0b|oss-mideast|03|com|00|"; fast_pattern; nocase;
classtype:trojan-activity; sid:4000131; rev:1; priority:3; reference:url,/events/view/5;)
alert tcp any any -> any 53 (msg: "MISP e5 [] Domain: oss-mideast.com"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|0b|oss-mideast|03|com|00|"; fast_pattern; nocase;
flow:established;  classtype:trojan-activity; sid:4000132; rev:1; priority:3; reference:url,/
events/view/5;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e5 [] Outgoing HTTP Domain: oss-
mideast.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; content:"oss-
mideast.com"; fast_pattern; nocase; http_header; pcre: "/(^|[^A-Za-z0-9-])oss\-mideast\.com[^A-Za-
z0-9-\.]/H"; tag:session,600,seconds; classtype:trojan-activity; sid:4000133; rev:1; priority:3;
reference:url,/events/view/5;)
alert udp any any -> any 53 (msg: "MISP e5 [] Hostname: vecjnr.edu.in"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|00||06|vecjnr|03|edu|02|in|00|"; fast_pattern;
nocase;  classtype:trojan-activity; sid:4000181; rev:1; priority:3; reference:url,/events/view/5;)
alert tcp any any -> any 53 (msg: "MISP e5 [] Hostname: vecjnr.edu.in"; content:"|01 00 00 01 00
00 00 00 00 00|"; depth:10; offset:2; content:"|00||06|vecjnr|03|edu|02|in|00|"; fast_pattern;
nocase; flow:established;  classtype:trojan-activity; sid:4000182; rev:1; priority:3;
reference:url,/events/view/5;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e5 [] Outgoing HTTP Hostname:
vecjnr.edu.in"; flow:to_server,established; content: "Host|3a| vecjnr.edu.in"; nocase;
http_header; pcre: "/(^|[^A-Za-z0-9-\.])vecjnr\.edu\.in[^A-Za-z0-9-\.]/H"; tag:session,
600,seconds; classtype:trojan-activity; sid:4000183; rev:1; priority:3; reference:url,/events/view/
5;)
```



```
#fields indicator       indicator_type  meta.source     meta.desc       meta.url
meta.do_notice  meta.if_in
7d8fd3a80efc4163a5c9811a2e43f4bd5da60435        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
7f9d970c685f7f33aa8a961f2a10173d        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
8a9396f9c30a6928aa96de3c6563e2d7        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
8e5b5322cd8fa350f38e65f159f55cef        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
11f93876dba467125556c04a85c19f4b93ed5e4c        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
288fecbe9c8b1fe1f91a215d8b6883bb696afeda        Intel::FILE_HASH        ORGNAME MISP (5c3a927f-
fbd0-4bf6-8db6-79d5c0a80a40) - ORGNAME  MalwarePatrol - Active Malware samples detected on
2019-01-12.     /events/view/5  T       -
```



Case template management

Current templates

MISP

Case basic information

Template name * MISP
This name should be unique

Title prefix MISP
This is used to prefix the case name

Severity M
This will be the default case severity

TLP TLP:AMBER
This will be the default case TLP

PAP PAP:AMBER
This will be the default case PAP

Tags misp × automated × threat intelligence × Tags
These will be the default case tags

Description * These are cases raised from alerts originating in MISP.

* Required field

Tasks (5)

- [default] Detection and Identification — Edit Delete
- [default] Containment — Edit Delete
- [default] Remediation — Edit Delete
- [default] Recovery — Edit Delete
- [default] Lessons Learned — Edit Delete

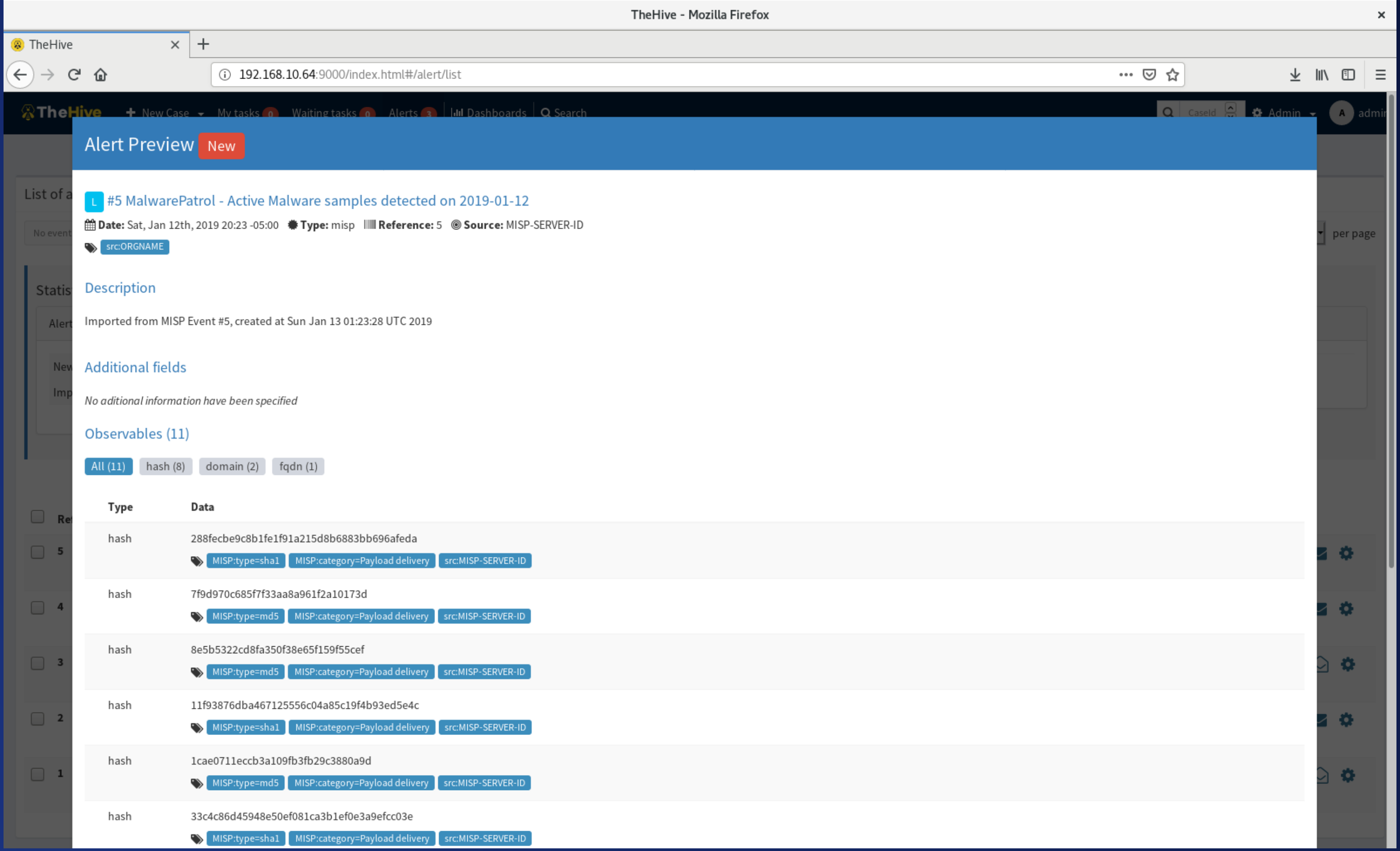
Metrics (0)

No metrics have been added. Add a metric

Custom fields (0)

No custom fields have been added. Add a custom field

TheHive Project 2016-2018, AGPL-V3



Alert Preview New

L #5 MalwarePatrol - Active Malware samples detected on 2019-01-12

Date: Sat, Jan 12th, 2019 20:23 -05:00 **Type:** misp **Reference:** 5 **Source:** MISP-SERVER-ID

src:ORGNAME

Description

Imported from MISP Event #5, created at Sun Jan 13 01:23:28 UTC 2019

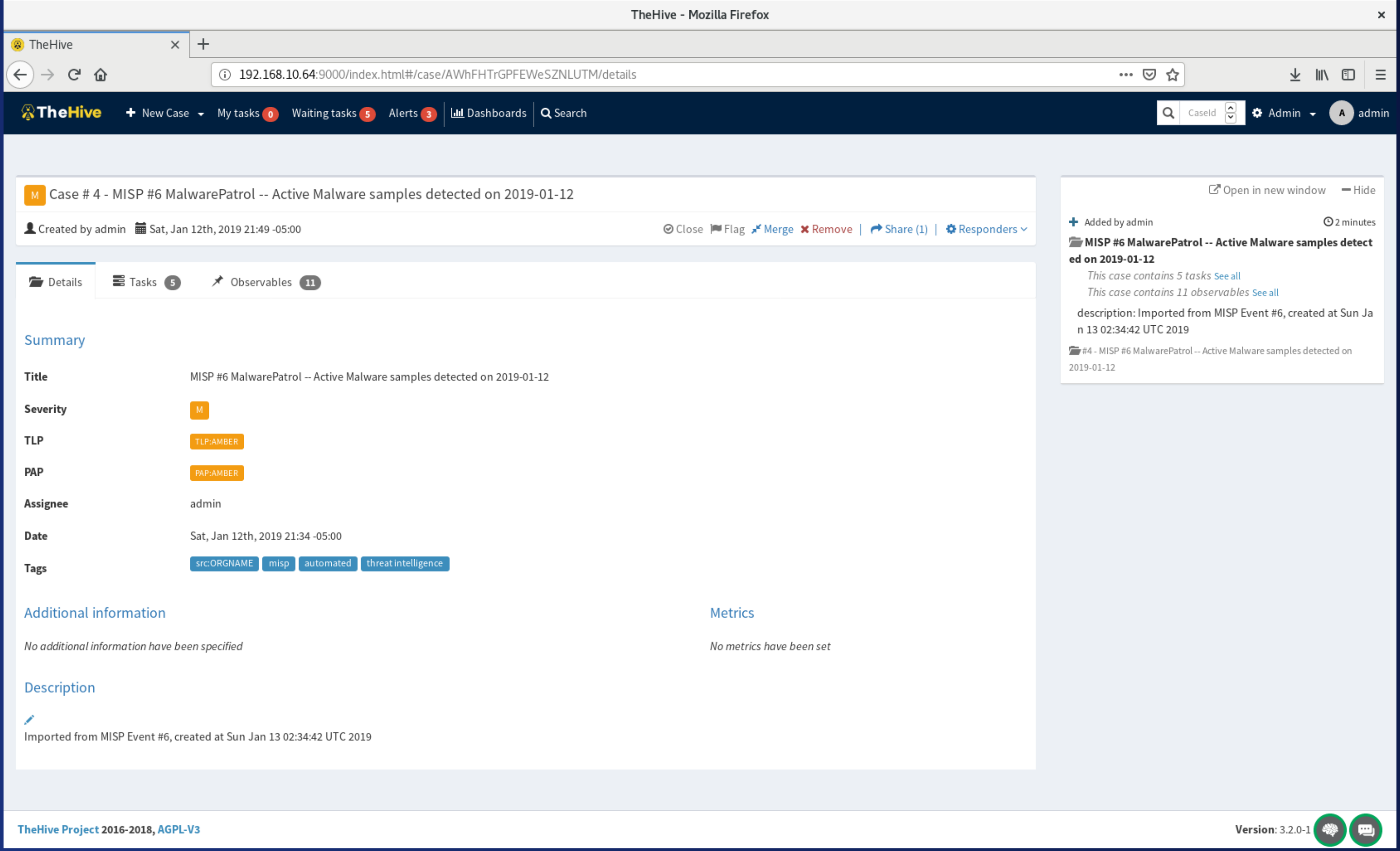
Additional fields

No aditional information have been specified

Observables (11)

All (11) hash (8) domain (2) fqdn (1)

Type	Data
hash	288fecbe9c8b1fe1f91a215d8b6883bb696afeda MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID
hash	7f9d970c685f7f33aa8a961f2a10173d MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID
hash	8e5b5322cd8fa350f38e65f159f55cef MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID
hash	11f93876dba467125556c04a85c19f4b93ed5e4c MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID
hash	1cae0711eccb3a109fb3fb29c3880a9d MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID
hash	33c4c86d45948e50ef081ca3b1ef0e3a9efcc03e MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID



M Case # 4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

Created by admin Sat, Jan 12th, 2019 21:49 -05:00

Summary

Title	MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12
Severity	M
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	admin
Date	Sat, Jan 12th, 2019 21:34 -05:00
Tags	src:ORGNAME misp automated threat intelligence

Additional information

No additional information have been specified

Metrics

No metrics have been set

Description

Imported from MISP Event #6, created at Sun Jan 13 02:34:42 UTC 2019

Added by admin 2 minutes

MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

This case contains 5 tasks See all

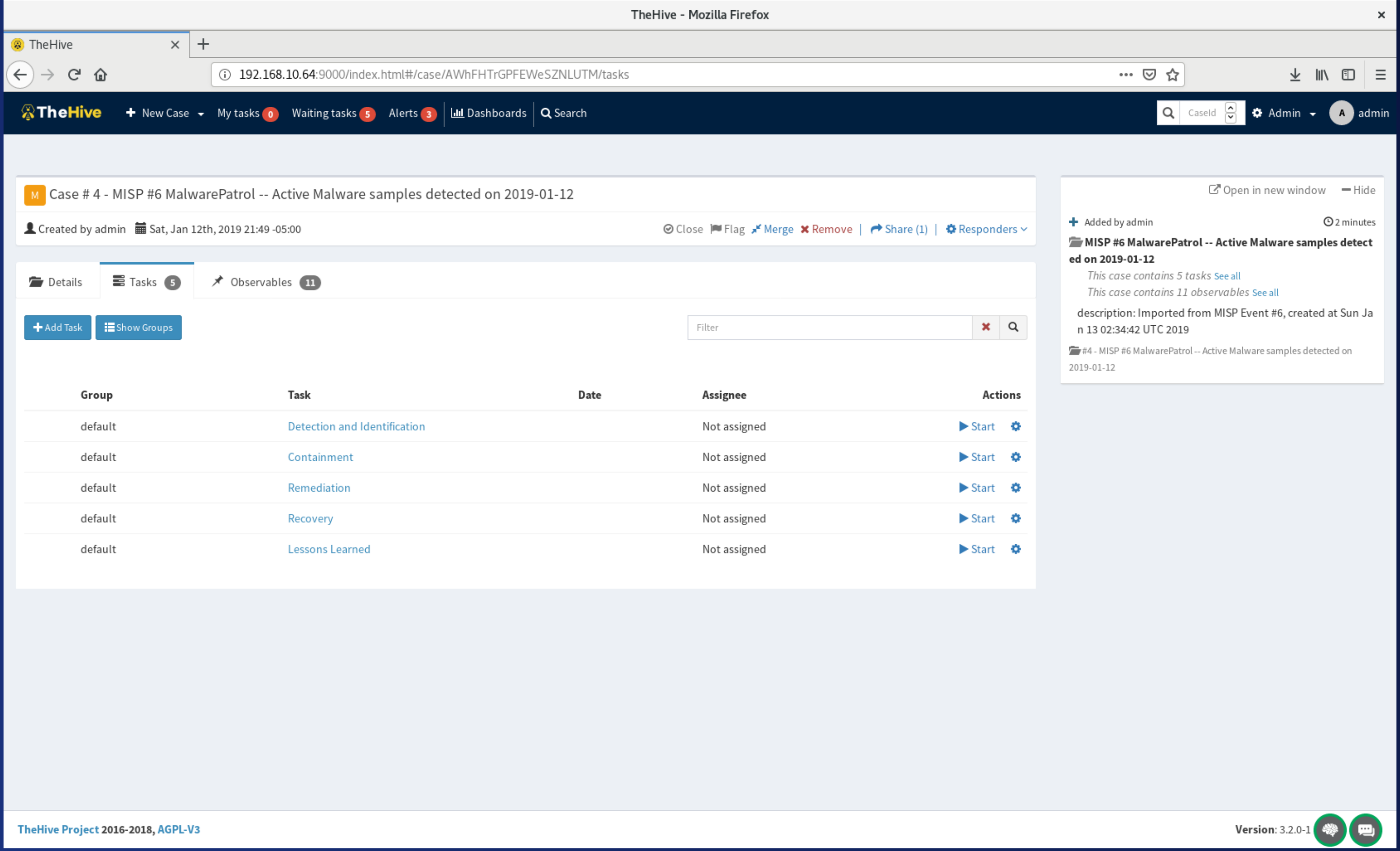
This case contains 11 observables See all

description: Imported from MISP Event #6, created at Sun Jan 13 02:34:42 UTC 2019

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

TheHive Project 2016-2018, AGPL-V3

Version: 3.2.0-1


TheHive - Mozilla Firefox
TheHive
192.168.10.64:9000/index.html#/case/AWhFHTrGPFEWeSZNLUTM/tasks
TheHive
New Case
My tasks 0
Waiting tasks 5
Alerts 3
Dashboards
Search
CaseId
Admin
admin

M Case # 4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

Created by admin Sat, Jan 12th, 2019 21:49 -05:00

Group	Task	Date	Assignee	Actions
default	Detection and Identification		Not assigned	Start
default	Containment		Not assigned	Start
default	Remediation		Not assigned	Start
default	Recovery		Not assigned	Start
default	Lessons Learned		Not assigned	Start

Added by admin 2 minutes

MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

This case contains 5 tasks See all

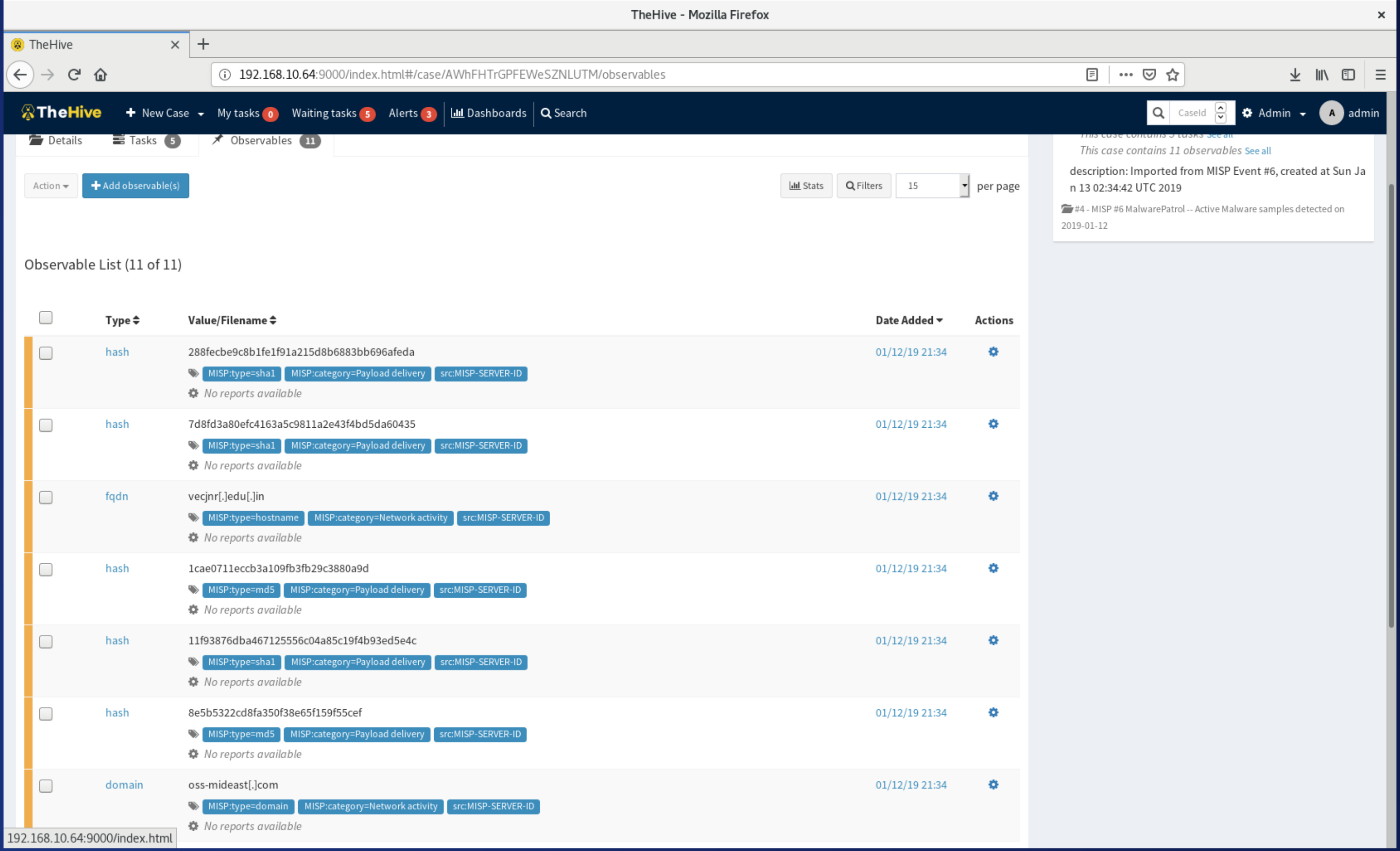
This case contains 11 observables See all

description: Imported from MISP Event #6, created at Sun Jan 13 02:34:42 UTC 2019

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

TheHive Project 2016-2018, AGPL-V3

Version: 3.2.0-1



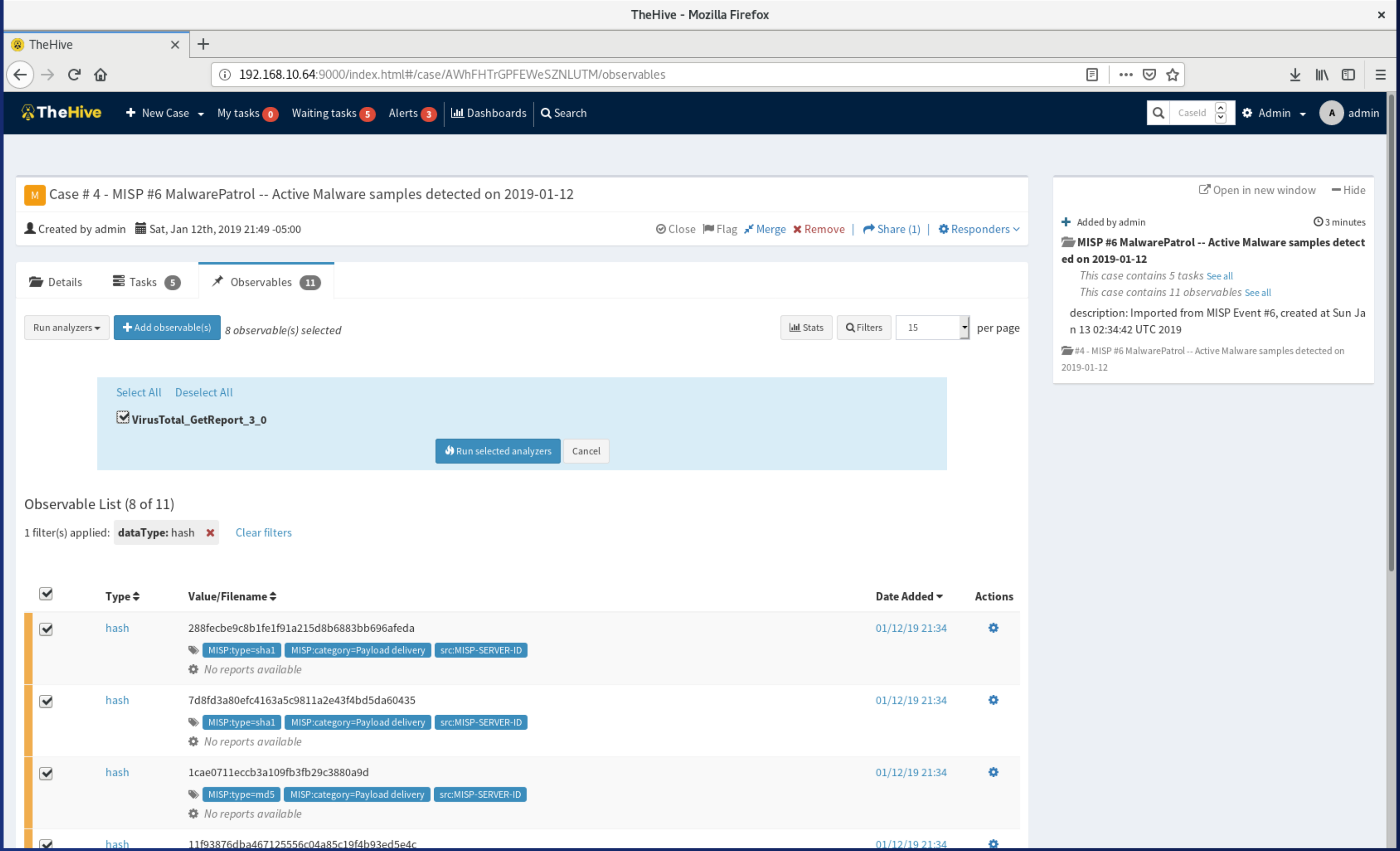
This case contains 11 observables See all

description: Imported from MISP Event #6, created at Sun Jan 13 02:34:42 UTC 2019

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

Observable List (11 of 11)

□	Type	Value/Filename	Date Added	Actions
□	hash	288fecbe9c8b1fe1f91a215d8b6883bb696afeda MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435 MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	fqdn	vecjnr[.]edu[.]in MISP:type=hostname MISP:category=Network activity src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	1cae0711eccb3a109fb3fb29c3880a9d MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	11f93876dba467125556c04a85c19f4b93ed5e4c MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	8e5b5322cd8fa350f38e65f159f55cef MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	domain	oss-mideast[.]com MISP:type=domain MISP:category=Network activity src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙



TheHive - Mozilla Firefox
TheHive
192.168.10.64:9000/index.html#/case/AWhFHTrGPFEWeSZNLUTM/observables
TheHive
New Case
My tasks 0
Waiting tasks 5
Alerts 3
Dashboards
Search
CaseId
Admin
admin

Case # 4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

Created by admin Sat, Jan 12th, 2019 21:49 -05:00

8 observable(s) selected

☑ VirusTotal_GetReport_3_0

Observable List (8 of 11)

1 filter(s) applied: **dataType:** hash

☑	Type	Value/Filename	Date Added	Actions
☑	hash	288fecbe9c8b1fe1f91a215d8b6883bb696afeda MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	
☑	hash	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435 MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	
☑	hash	1cae0711eccb3a109fb3fb29c3880a9d MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	
☑	hash	11f93876dba467125556c04a85c19f4b93ed5e4c	01/12/19 21:34	

Added by admin 3 minutes

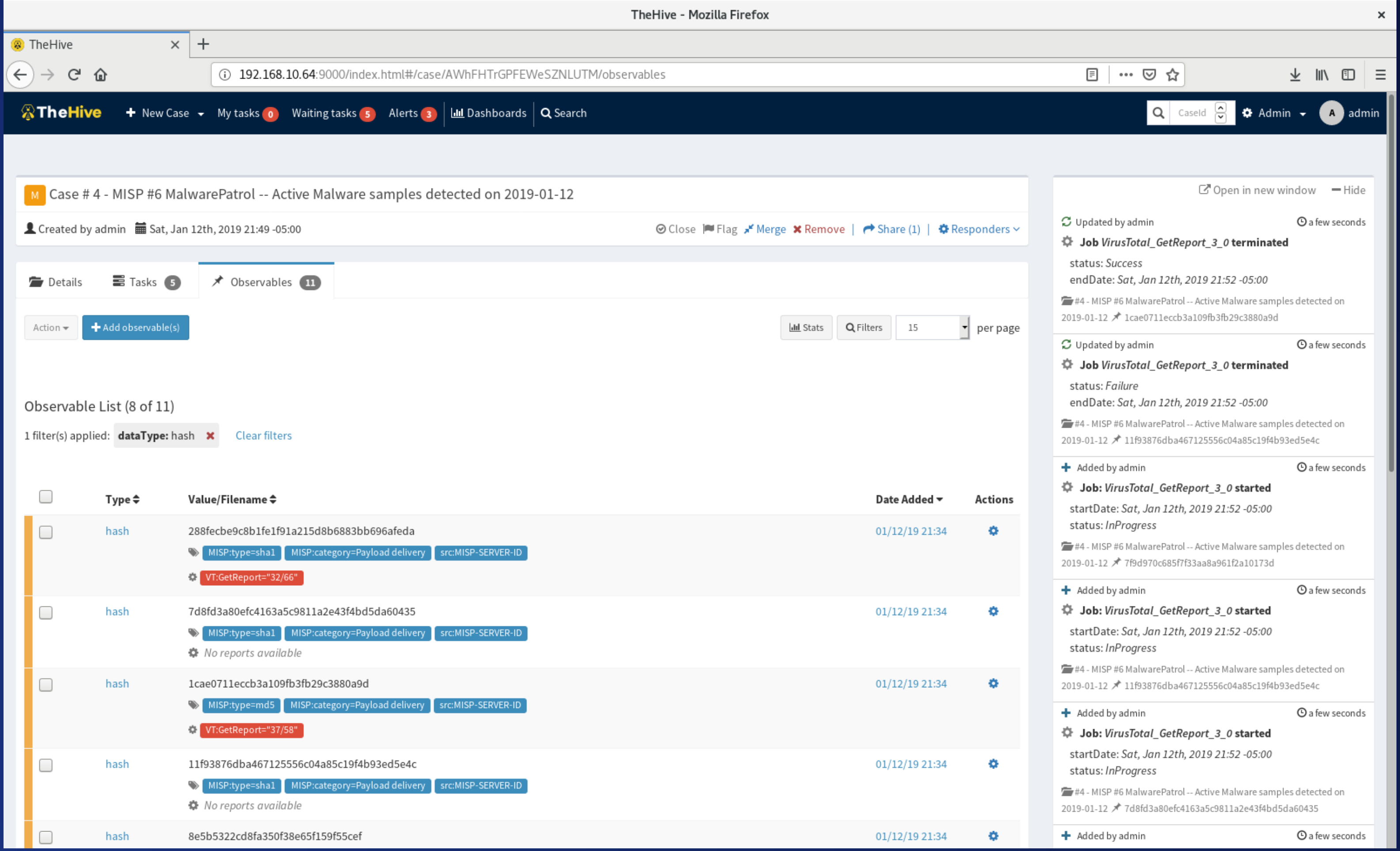
MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

This case contains 5 tasks See all

This case contains 11 observables See all

description: Imported from MISP Event #6, created at Sun Jan 13 02:34:42 UTC 2019

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12


TheHive - Mozilla Firefox
TheHive
192.168.10.64:9000/index.html#/case/AWhFHTrGPFEWeSZNLUTM/observables
TheHive
New Case
My tasks 0
Waiting tasks 5
Alerts 3
Dashboards
Search
CaseId
Admin
admin

M Case # 4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12

Created by admin Sat, Jan 12th, 2019 21:49 -05:00

Observable List (8 of 11)

1 filter(s) applied: **dataType:** hash ✖ Clear filters

□	Type	Value/Filename	Date Added	Actions
□	hash	288fecbe9c8b1fe1f91a215d8b6883bb696afeda MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID VT:GetReport="32/66"	01/12/19 21:34	⚙
□	hash	7d8fd3a80efc4163a5c9811a2e43f4bd5da60435 MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	1cae0711eccb3a109fb3fb29c3880a9d MISP:type=md5 MISP:category=Payload delivery src:MISP-SERVER-ID VT:GetReport="37/58"	01/12/19 21:34	⚙
□	hash	11f93876dba467125556c04a85c19f4b93ed5e4c MISP:type=sha1 MISP:category=Payload delivery src:MISP-SERVER-ID *No reports available*	01/12/19 21:34	⚙
□	hash	8e5b5322cd8fa350f38e65f159f55cef	01/12/19 21:34	⚙

Updated by admin a few seconds

Job *VirusTotal_GetReport_3_0* terminated

status: *Success*
endDate: *Sat, Jan 12th, 2019 21:52 -05:00*

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12 1cae0711eccb3a109fb3fb29c3880a9d

Updated by admin a few seconds

Job *VirusTotal_GetReport_3_0* terminated

status: *Failure*
endDate: *Sat, Jan 12th, 2019 21:52 -05:00*

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12 11f93876dba467125556c04a85c19f4b93ed5e4c

Added by admin a few seconds

Job: *VirusTotal_GetReport_3_0* started

startDate: *Sat, Jan 12th, 2019 21:52 -05:00*
status: *InProgress*

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12 7f9d970c685f7f33aa8a961f2a10173d

Added by admin a few seconds

Job: *VirusTotal_GetReport_3_0* started

startDate: *Sat, Jan 12th, 2019 21:52 -05:00*
status: *InProgress*

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12 11f93876dba467125556c04a85c19f4b93ed5e4c

Added by admin a few seconds

Job: *VirusTotal_GetReport_3_0* started

startDate: *Sat, Jan 12th, 2019 21:52 -05:00*
status: *InProgress*

#4 - MISP #6 MalwarePatrol -- Active Malware samples detected on 2019-01-12 7d8fd3a80efc4163a5c9811a2e43f4bd5da60435

Added by admin a few seconds

How Can I Play With This?

- There’s a MISP / TheHive / Cortex VM image available from the MISP team.
- https://www.circl.lu/misp-training-images/

Questions?

For More Information

@InfosecGoon

infosecgoon@roadflares.org

https://github.com/InfosecGoon/stinger/