Making a Day in the Life of a University Sys-Admin Easier

James Culverhouse | AusCERT General Manager

Mike Holm | Operations Manager

About AusCERT

- AusCERT is an operational cyber emergency response team based at the University of Queensland
- Helping organisations prevent, detect, respond to and mitigate cyber and Internet based attacks since 1993
- Independent and impartial
- Self-funded and not-for-profit
- National focus across government, education, research and industry

ISAC: Information Sharing & Analytics Centre

Share today, Save tomorrow

© Nick Soysa, AusCERT Senior Information Security Analyst

The University Of Queensland
AUSTRALIA

AusCERT

```
<li><a href="index.html">Home</a></li>
<li><a href="home-events.html">Home Events</a></li>
<li><a href="multi-col-menu.html">Multiple Column Menu on Larger Viewports
<li class="has-children"> <a href="#" class="current">Header Options</a>
  <ul>
    <li><a href="tall-button-header.html">Tall Button Header</a></li>
    <li><a href="image-logo.html">Image Logo</a></li>
    <li class="active"><a href="tall-logo.html">Tall Logo Image</a
  </ul>
</li>
<li class="has-children"> <a href="#">Carousels</a>
  <ul>
    <li><a href="variable-width-slider.html">Variable Image Wi
    <li><a href="testimonial-slider.html">Testimonial Slider<
    <li><a href="featured-work-slider.html">Featured Work Sli
    <li><a href="equal-column-slider.html">Equal Column Slid
    <li><a href="video-slider.html">Video Slider</a></li>
    <li><a href="mini-bootstrap-
```

© BBC
bbc.co.uk/doctorwho

What we’re all doing (hopefully):

- Your own security framework, for your environment
- Participate in your cybersecurity community of practice (eg QUDIT)
- QUDIT 10 ten initiatives
- …because you can’t go it alone!

Why an ISAC?

- Most organisations engage in threat intelligence sharing in an informal and unstructured manner
- Sharing channels: mail notifications, chat, phone, social media
- Sharing delay
- Persistent record of information (! Chat)
- Difficulty interpreting and actioning threat indicators

ISAC Functions

- Information Sharing and Analytics Centre
- Curation of data
- Support industry standard data formats (e.g. STIX, …)

Sharing modes

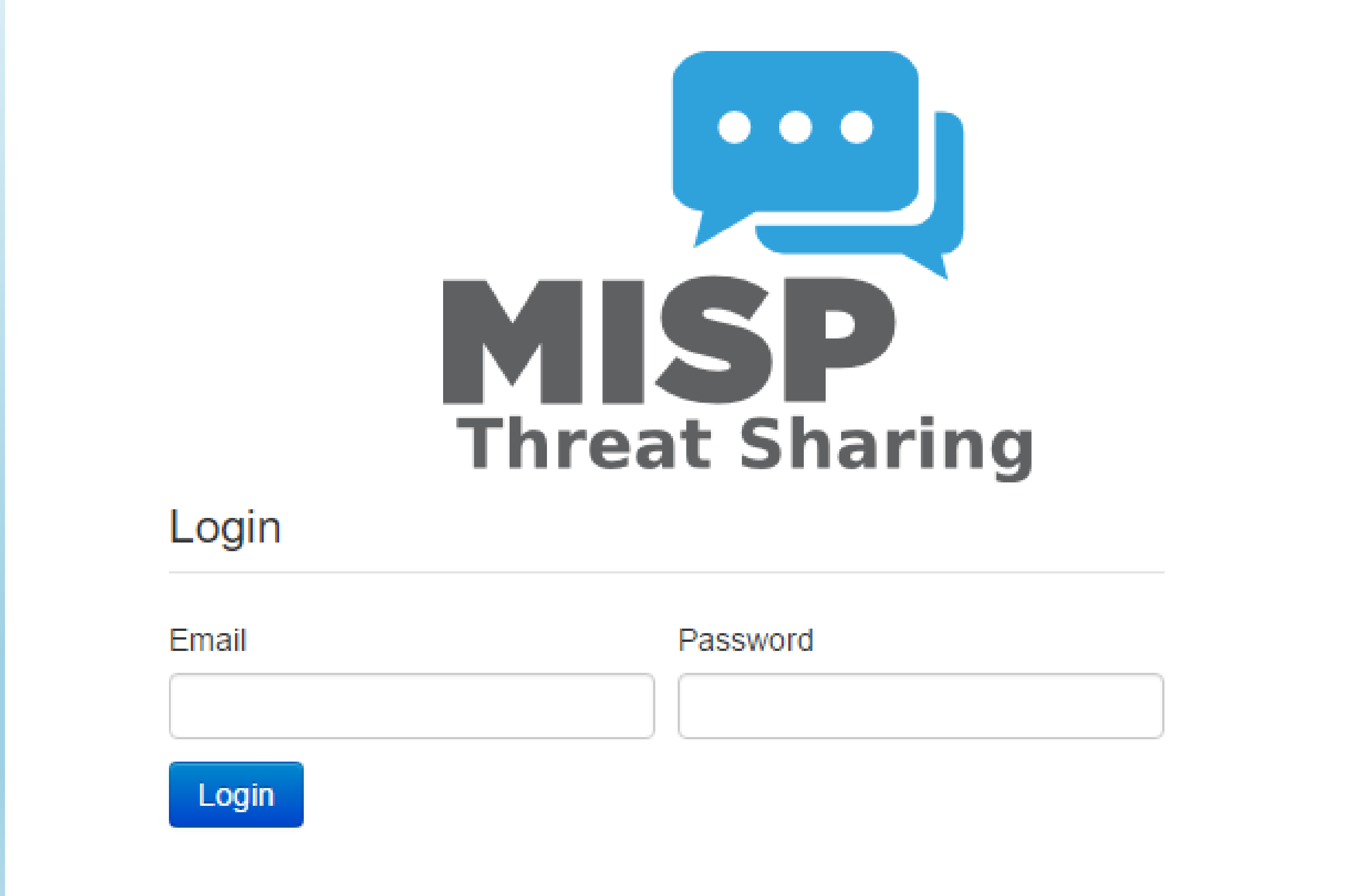
- **Human consumption**
  - Context important; bit more effort populating events
  - Ability to visualise relationships
  - Ability to interpret indicators, detect and report false positives

- **Machine consumption**
  - Context not important
  - Export in widely supported automation standards important
  - Careful curation absolutely important (~0 false positives)
  - Testing important

Introduction to MISP

- Free and Open Source threat intel sharing platform
- Developed and maintained by CERT Luxembourg
- Used by world recognised agencies: NSA, ….
- Ongoing integration with multiple security vendors and tools SIEMs, IDS, Mail filters, etc

MISP: Welcome Page

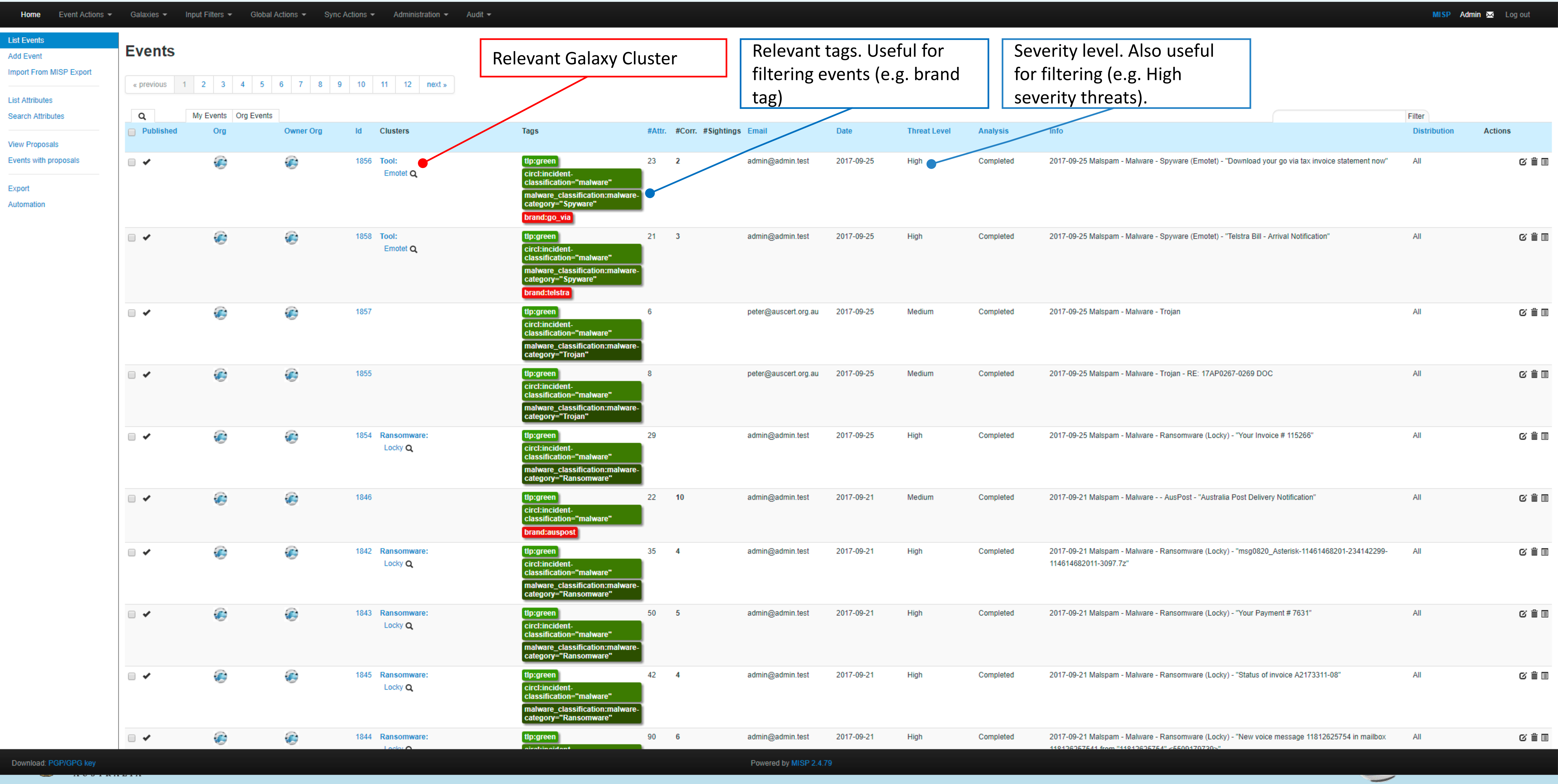


Login

Email

Password

MISP: Home page



Relevant Galaxy Cluster

Relevant tags. Useful for filtering events (e.g. brand tag)

Severity level. Also useful for filtering (e.g. High severity threats).

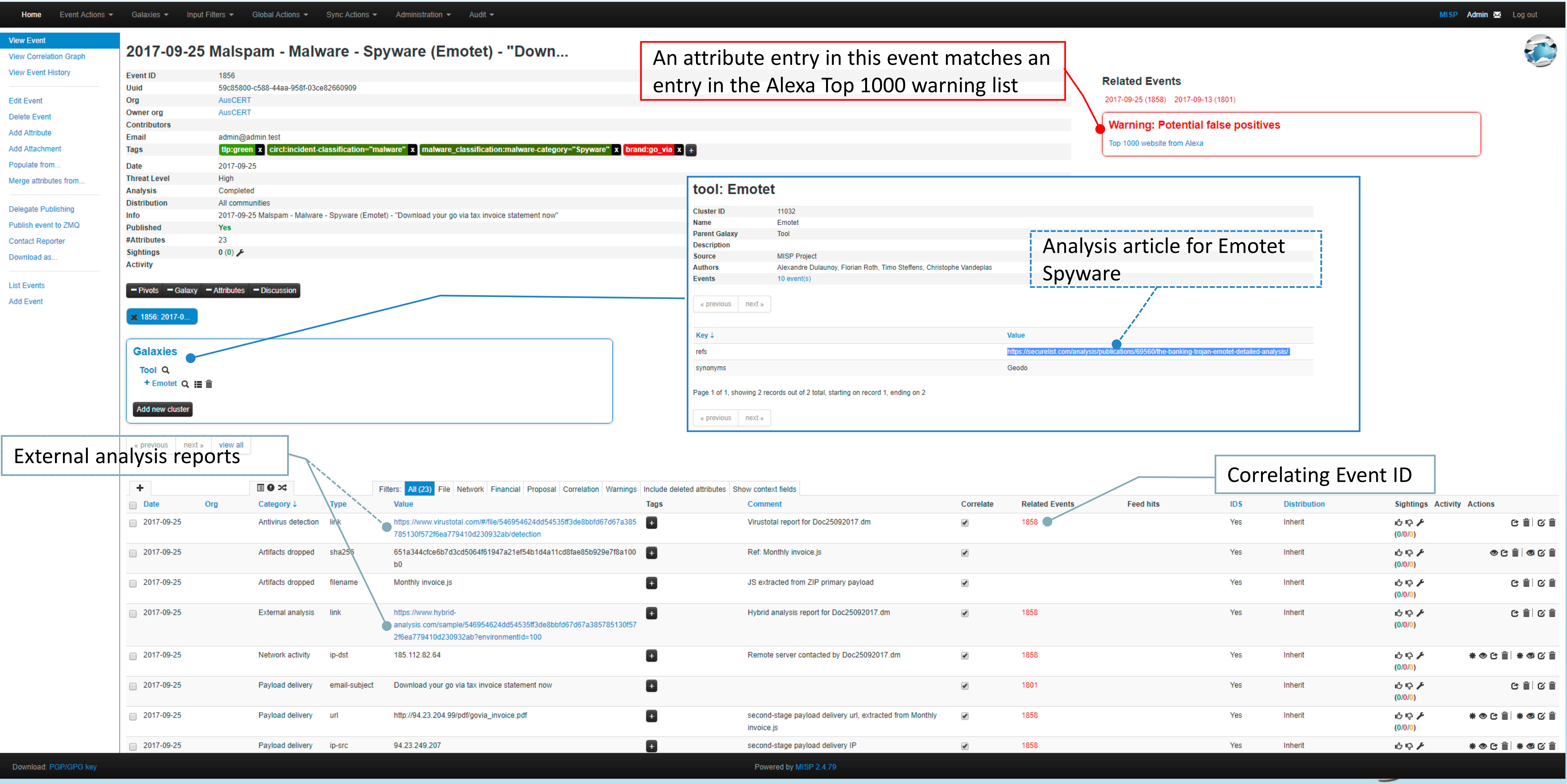
Events

Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	#Corr.	#Sightings	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓			1856	Tool: Emotet	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Spyware" brand:go_via	23	2		admin@admin.test	2017-09-25	High	Completed	2017-09-25 Malspam - Malware - Spyware (Emotet) - "Download your go via tax invoice statement now"	All	
✓			1858	Tool: Emotet	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Spyware" brand:telstra	21	3		admin@admin.test	2017-09-25	High	Completed	2017-09-25 Malspam - Malware - Spyware (Emotet) - "Telstra Bill - Arrival Notification"	All	
✓			1857		tlp:green circl:incident-classification="malware" malware_classification:malware-category="Trojan"	6			peter@auscert.org.au	2017-09-25	Medium	Completed	2017-09-25 Malspam - Malware - Trojan	All	
✓			1855		tlp:green circl:incident-classification="malware" malware_classification:malware-category="Trojan"	8			peter@auscert.org.au	2017-09-25	Medium	Completed	2017-09-25 Malspam - Malware - Trojan - RE: 17AP0267-0269 DOC	All	
✓			1854	Ransomware: Locky	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Ransomware"	29			admin@admin.test	2017-09-25	High	Completed	2017-09-25 Malspam - Malware - Ransomware (Locky) - "Your Invoice # 115266"	All	
✓			1846		tlp:green circl:incident-classification="malware" brand:auspost	22	10		admin@admin.test	2017-09-21	Medium	Completed	2017-09-21 Malspam - Malware - - AusPost - "Australia Post Delivery Notification"	All	
✓			1842	Ransomware: Locky	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Ransomware"	35	4		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "msg0820_Asterisk-11461468201-234142299-114614682011-3097.7z"	All	
✓			1843	Ransomware: Locky	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Ransomware"	50	5		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "Your Payment # 7631"	All	
✓			1845	Ransomware: Locky	tlp:green circl:incident-classification="malware" malware_classification:malware-category="Ransomware"	42	4		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "Status of invoice A2173311-08"	All	
✓			1844	Ransomware: Locky	tlp:green circl:incident-	90	6		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "New voice message 11812625754 in mailbox 118126257541 from "11812625754" <5509179720>"	All	

Download: PGP/GPG key

Powered by MISP 2.4.79

MISP: Event page – part 1



2017-09-25 Malspam - Malware - Spyware (Emotet) - "Down...

Event ID	1856
Uuid	59c85800-c588-44aa-958f-03ce82660909
Org	AusCERT
Owner org	AusCERT
Contributors	
Email	admin@admin.test
Tags	tlp:green x circl:incident-classification="malware" x malware_classification:malware-category="Spyware" x brand:go_via x +
Date	2017-09-25
Threat Level	High
Analysis	Completed
Distribution	All communities
Info	2017-09-25 Malspam - Malware - Spyware (Emotet) - "Download your go via tax invoice statement now"
Published	Yes
#Attributes	23
Sightings	0 (0)
Activity	

An attribute entry in this event matches an entry in the Alexa Top 1000 warning list

Related Events

2017-09-25 (1858) 2017-09-13 (1801)

Warning: Potential false positives

Top 1000 website from Alexa

Galaxies

Tool

+ Emotet

tool: Emotet

Cluster ID	11032
Name	Emotet
Parent Galaxy	Tool
Description	
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Timo Steffens, Christophe Vandeplas
Events	10 event(s)

« previous next »

Key ↓	Value
refs	https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
synonyms	Geodo

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous next »

Analysis article for Emotet Spyware

External analysis reports

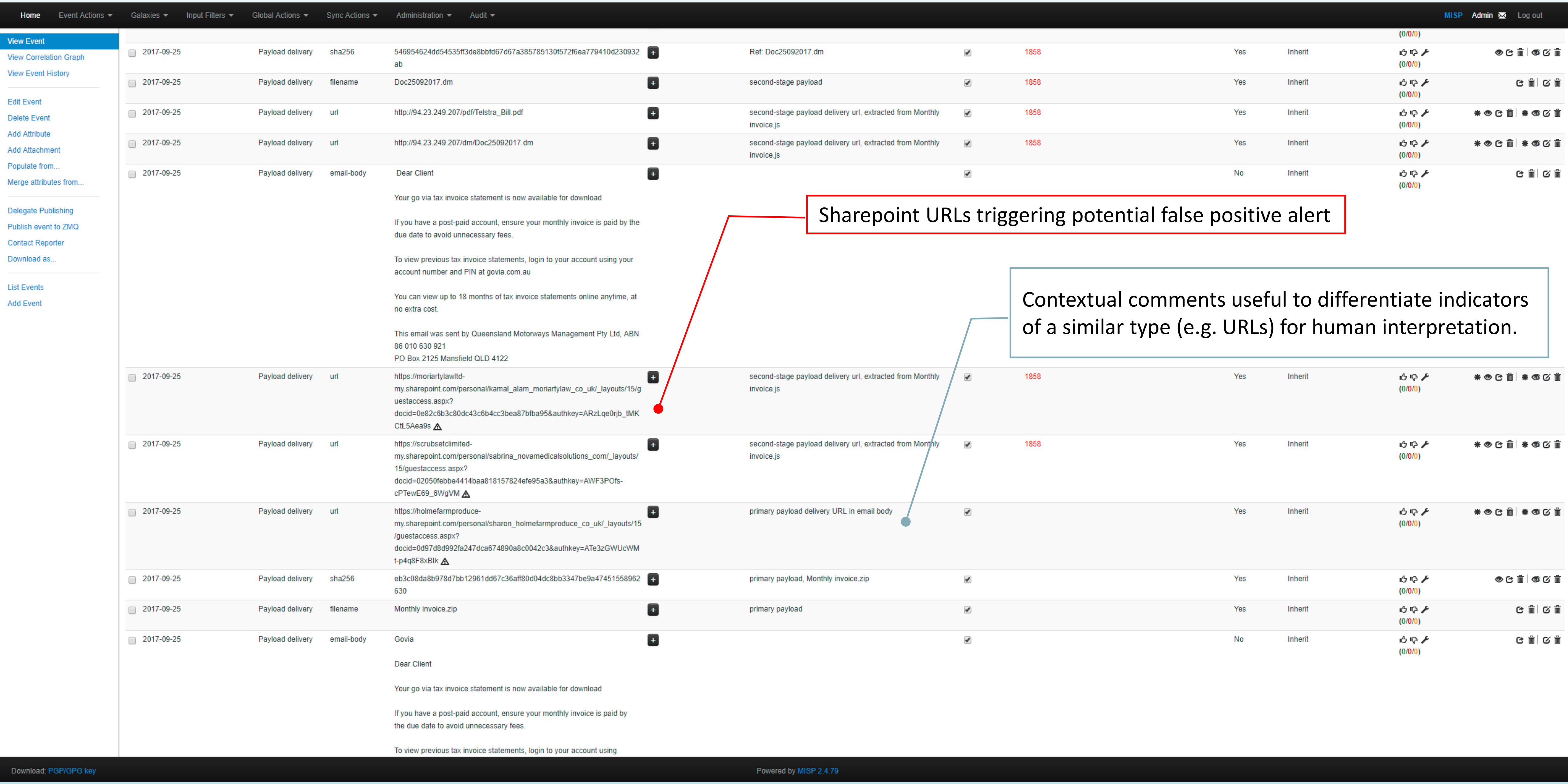
Correlating Event ID

Date	Org	Category ↓	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2017-09-25		Antivirus detection	link	https://www.virustotal.com/#/file/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab/detection	+	Virustotal report for Doc25092017.dm	☑	1858		Yes	Inherit	(0/0/0)		
2017-09-25		Artifacts dropped	sha256	651a344cfce6b7d3cd5064f61947a21ef54b1d4a11cd8fae85b929e7f8a100b0	+	Ref: Monthly invoice.js	☑			Yes	Inherit	(0/0/0)		
2017-09-25		Artifacts dropped	filename	Monthly invoice.js	+	JS extracted from ZIP primary payload	☑			Yes	Inherit	(0/0/0)		
2017-09-25		External analysis	link	https://www.hybrid-analysis.com/sample/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab?environmentId=100	+	Hybrid analysis report for Doc25092017.dm	☑	1858		Yes	Inherit	(0/0/0)		
2017-09-25		Network activity	ip-dst	185.112.82.64	+	Remote server contacted by Doc25092017.dm	☑	1858		Yes	Inherit	(0/0/0)		
2017-09-25		Payload delivery	email-subject	Download your go via tax invoice statement now	+		☑	1801		Yes	Inherit	(0/0/0)		
2017-09-25		Payload delivery	url	http://94.23.204.99/pdf/govia_invoice.pdf	+	second-stage payload delivery url, extracted from Monthly invoice.js	☑	1858		Yes	Inherit	(0/0/0)		
2017-09-25		Payload delivery	ip-src	94.23.249.207	+	second-stage payload delivery IP	☑	1858		Yes	Inherit			

Download: PGP/GPG key

Powered by MISP 2.4.79

MISP: Event page – part 2

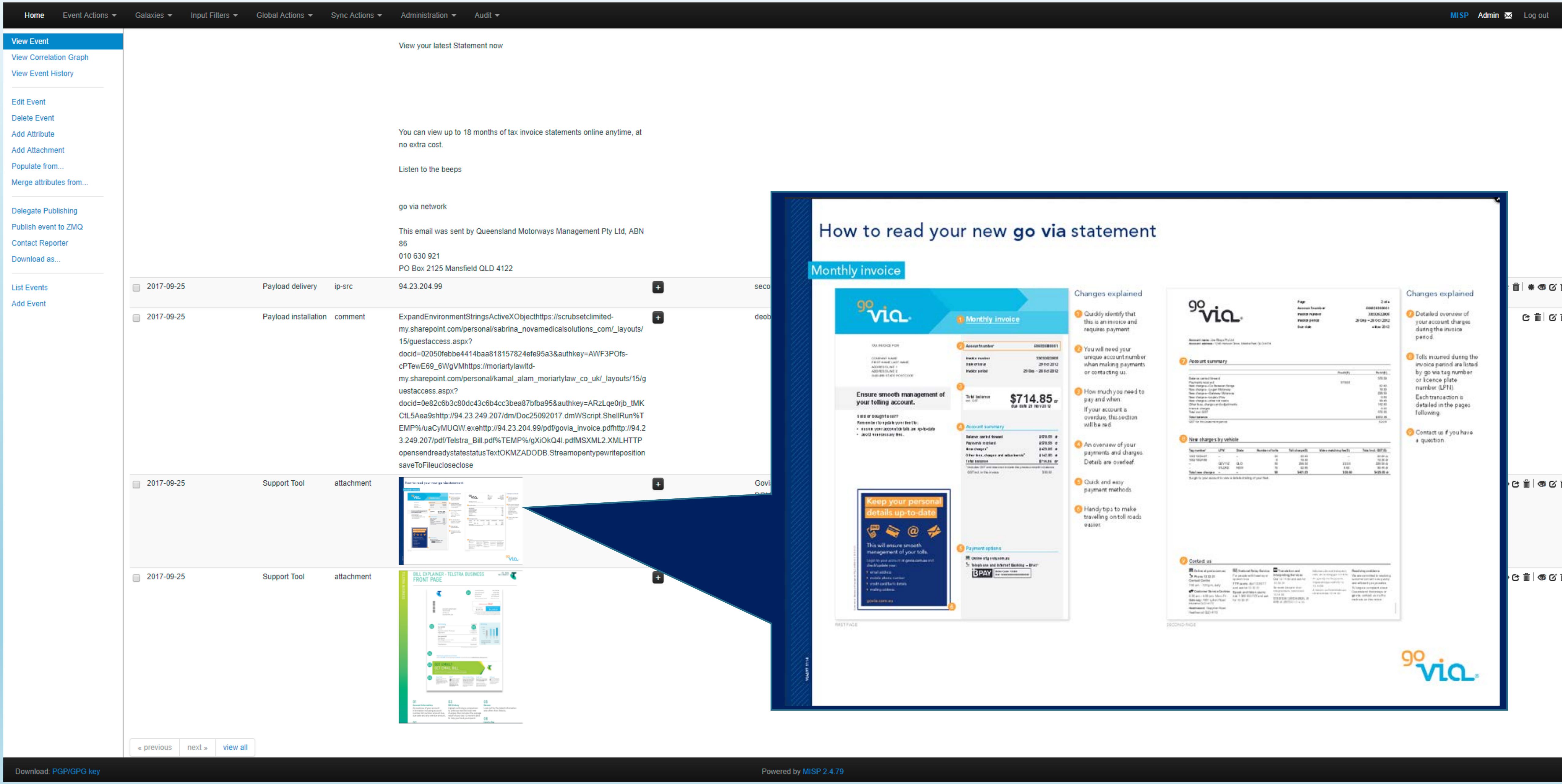


											(0/0/0)
□	2017-09-25	Payload delivery	sha256	546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab	+	Ref: Doc25092017.dm	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	filename	Doc25092017.dm	+	second-stage payload	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	url	http://94.23.249.207/pdf/Telstra_Bill.pdf	+	second-stage payload delivery url, extracted from Monthly invoice.js	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	url	http://94.23.249.207/dm/Doc25092017.dm	+	second-stage payload delivery url, extracted from Monthly invoice.js	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	email-body	Dear Client Your go via tax invoice statement is now available for download If you have a post-paid account, ensure your monthly invoice is paid by the due date to avoid unnecessary fees. To view previous tax invoice statements, login to your account using your account number and PIN at govia.com.au You can view up to 18 months of tax invoice statements online anytime, at no extra cost. This email was sent by Queensland Motorways Management Pty Ltd, ABN 86 010 630 921 PO Box 2125 Mansfield QLD 4122	+		☑		No	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	url	https://moriartylawltd-my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s ⚠	+	second-stage payload delivery url, extracted from Monthly invoice.js	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	url	https://scrubsetclimited-my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVM ⚠	+	second-stage payload delivery url, extracted from Monthly invoice.js	☑	1858	Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	url	https://holmefarmproduce-my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/_layouts/15/guestaccess.aspx?docid=0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-p4q8F8xBlk ⚠	+	primary payload delivery URL in email body	☑		Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	sha256	eb3c08da8b978d7bb12961dd67c36aff80d04dc8bb3347be9a47451558962630	+	primary payload, Monthly invoice.zip	☑		Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	filename	Monthly invoice.zip	+	primary payload	☑		Yes	Inherit	(0/0/0)
□	2017-09-25	Payload delivery	email-body	Govia Dear Client Your go via tax invoice statement is now available for download If you have a post-paid account, ensure your monthly invoice is paid by the due date to avoid unnecessary fees. To view previous tax invoice statements, login to your account using	+		☑		No	Inherit	(0/0/0)

Sharepoint URLs triggering potential false positive alert

Contextual comments useful to differentiate indicators of a similar type (e.g. URLs) for human interpretation.

MISP: Event page – part 3



View your latest Statement now

You can view up to 18 months of tax invoice statements online anytime, at no extra cost.

Listen to the beeps

go via network

This email was sent by Queensland Motorways Management Pty Ltd, ABN 86
010 630 921
PO Box 2125 Mansfield QLD 4122

2017-09-25	Payload delivery	ip-src	94.23.204.99	+	seco
2017-09-25	Payload installation	comment	ExpandEnvironmentStringsActiveXObjecthttps://scrubsetclimited-my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVMhttps://moriartylawltd-my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9shttp://94.23.249.207/dm/Doc25092017.dmWScript.ShellRun%TEMP%/uaCyMUQW.exehttp://94.23.204.99/pdf/govia_invoice.pdfhttp://94.23.249.207/pdf/Telstra_Bill.pdf%TEMP%/gXiOkQ4I.pdfMSXML2.XMLHTTPopensendreadystatestatusTextOKMZADODB.StreamopentypewritepositionsaveToFileuclosesclose	+	deob
2017-09-25	Support Tool	attachment		+	Govi
2017-09-25	Support Tool	attachment	BILL EXPLAINER - TELSTRA BUSINESS FRONT PAGE	+	

How to read your new **go via** statement

Monthly invoice

Ensure smooth management of your tolling account.

Total balance $714.85

Keep your personal details up-to-date

This will ensure smooth management of your tolls.

Changes explained

1 Quickly identify that this is an invoice and requires payment

2 You will need your unique account number when making payments or contacting us.

3 How much you need to pay and when.

If your account is overdue, this section will be red.

4 An overview of your payments and charges. Details are overleaf.

5 Quick and easy payment methods

6 Handy tips to make travelling on toll roads easier.

Changes explained

7 Detailed overview of your account charges during the invoice period.

8 Tolls incurred during the invoice period are listed by go via tag number or licence plate number (LPN).

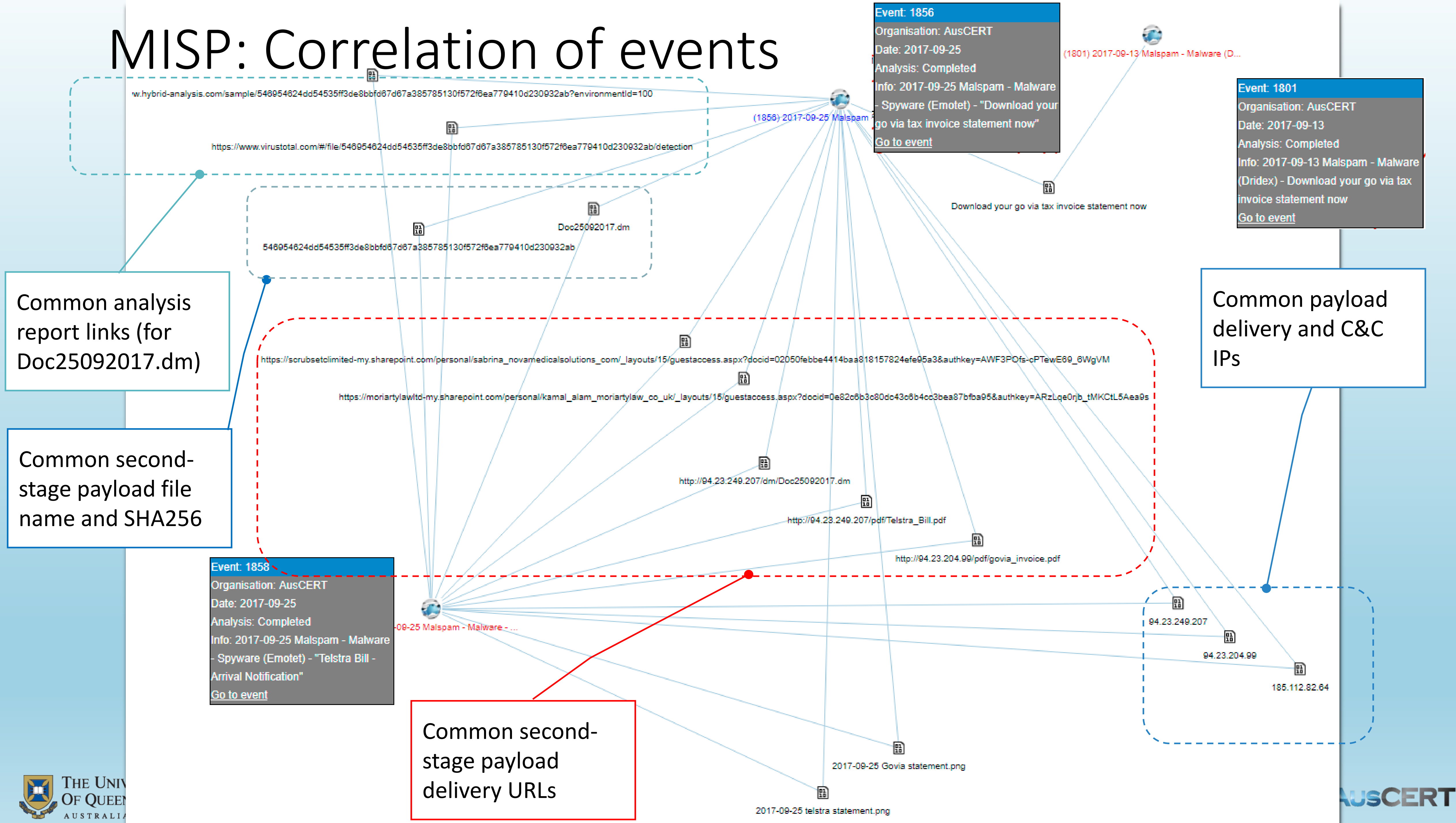
Each transaction is detailed in the pages following.

9 Contact us if you have a question.

Download: PGP/GPG key

Powered by MISP 2.4.79

MISP: Correlation of events



Event: 1856
Organisation: AusCERT
Date: 2017-09-25
Analysis: Completed
Info: 2017-09-25 Malspam - Malware - Spyware (Emotet) - "Download your go via tax invoice statement now"
Go to event

Event: 1801
Organisation: AusCERT
Date: 2017-09-13
Analysis: Completed
Info: 2017-09-13 Malspam - Malware (Dridex) - Download your go via tax invoice statement now
Go to event

Event: 1858
Organisation: AusCERT
Date: 2017-09-25
Analysis: Completed
Info: 2017-09-25 Malspam - Malware - Spyware (Emotet) - "Telstra Bill - Arrival Notification"
Go to event

(1801) 2017-09-13 Malspam - Malware (D...
(1856) 2017-09-25 Malspam
w.hybrid-analysis.com/sample/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab?environmentId=100
https://www.virustotal.com/#/file/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab/detection
Download your go via tax invoice statement now
Doc25092017.dm
546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab
https://scrubsetclimited-my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVM
https://moriartylawltd-my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s
http://94.23.249.207/dm/Doc25092017.dm
http://94.23.249.207/pdf/Telstra_Bill.pdf
http://94.23.204.99/pdf/govia_invoice.pdf
-09-25 Malspam - Malware - ...
94.23.249.207
94.23.204.99
185.112.82.64
2017-09-25 Govia statement.png
2017-09-25 telstra statement.png

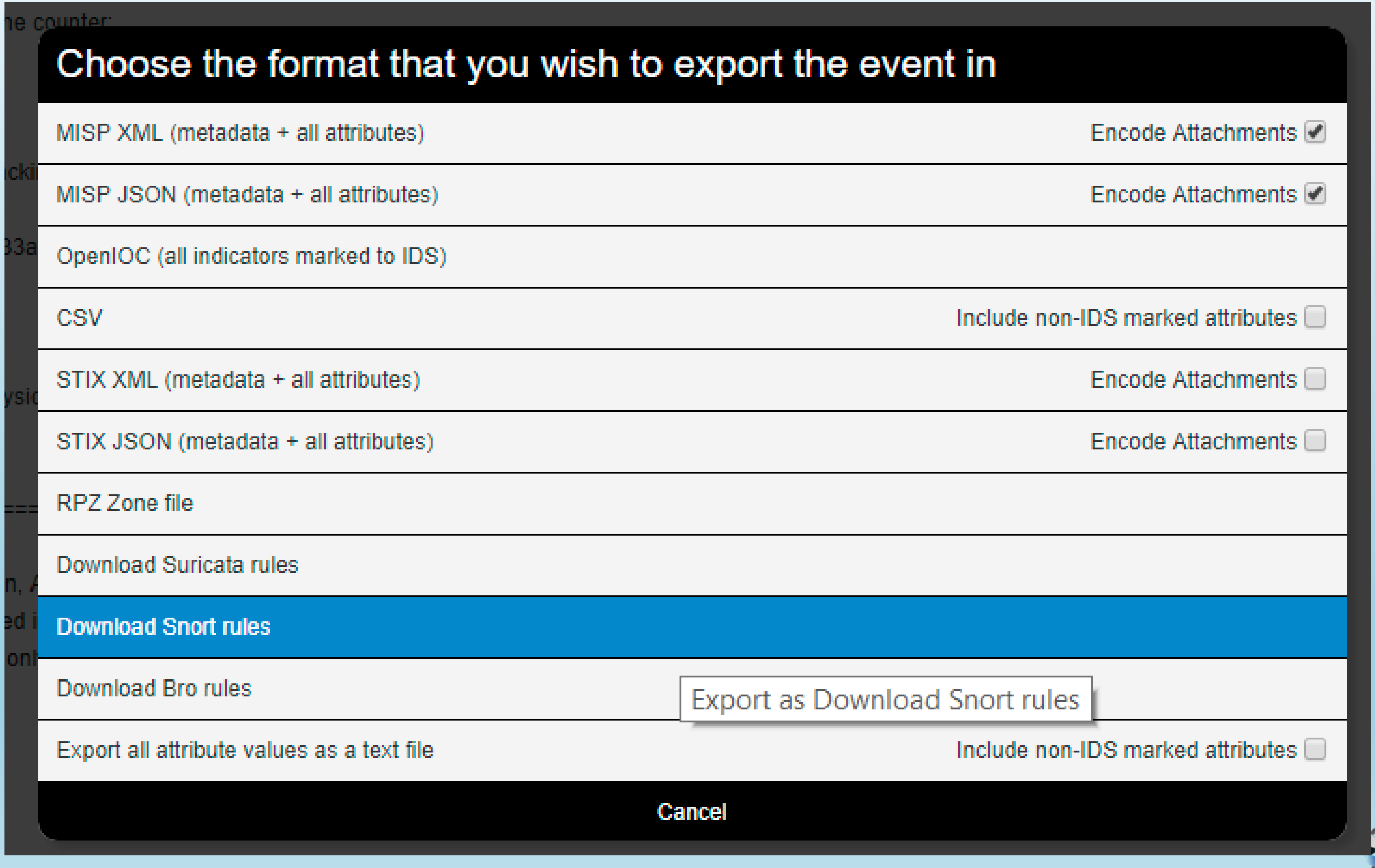
Common analysis report links (for Doc25092017.dm)

Common second-stage payload file name and SHA256

Common payload delivery and C&C IPs

Common second-stage payload delivery URLs

MISP: Downloading Indicators manually

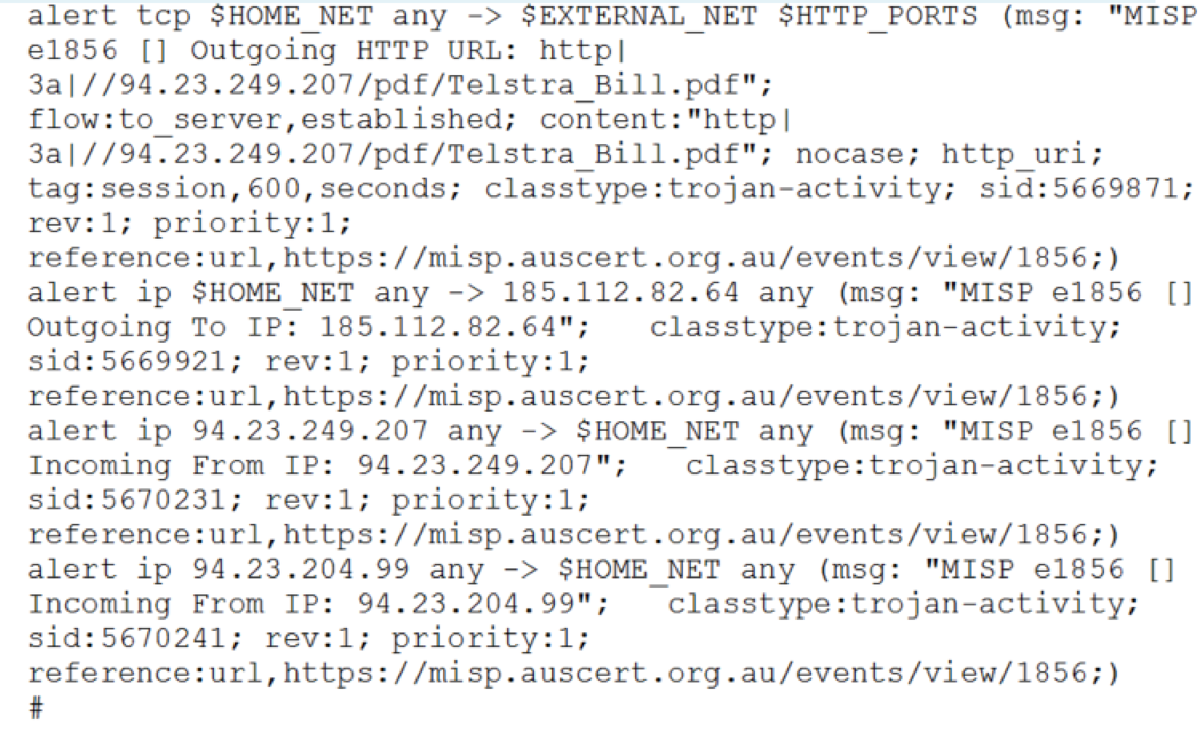


Choose the format that you wish to export the event in

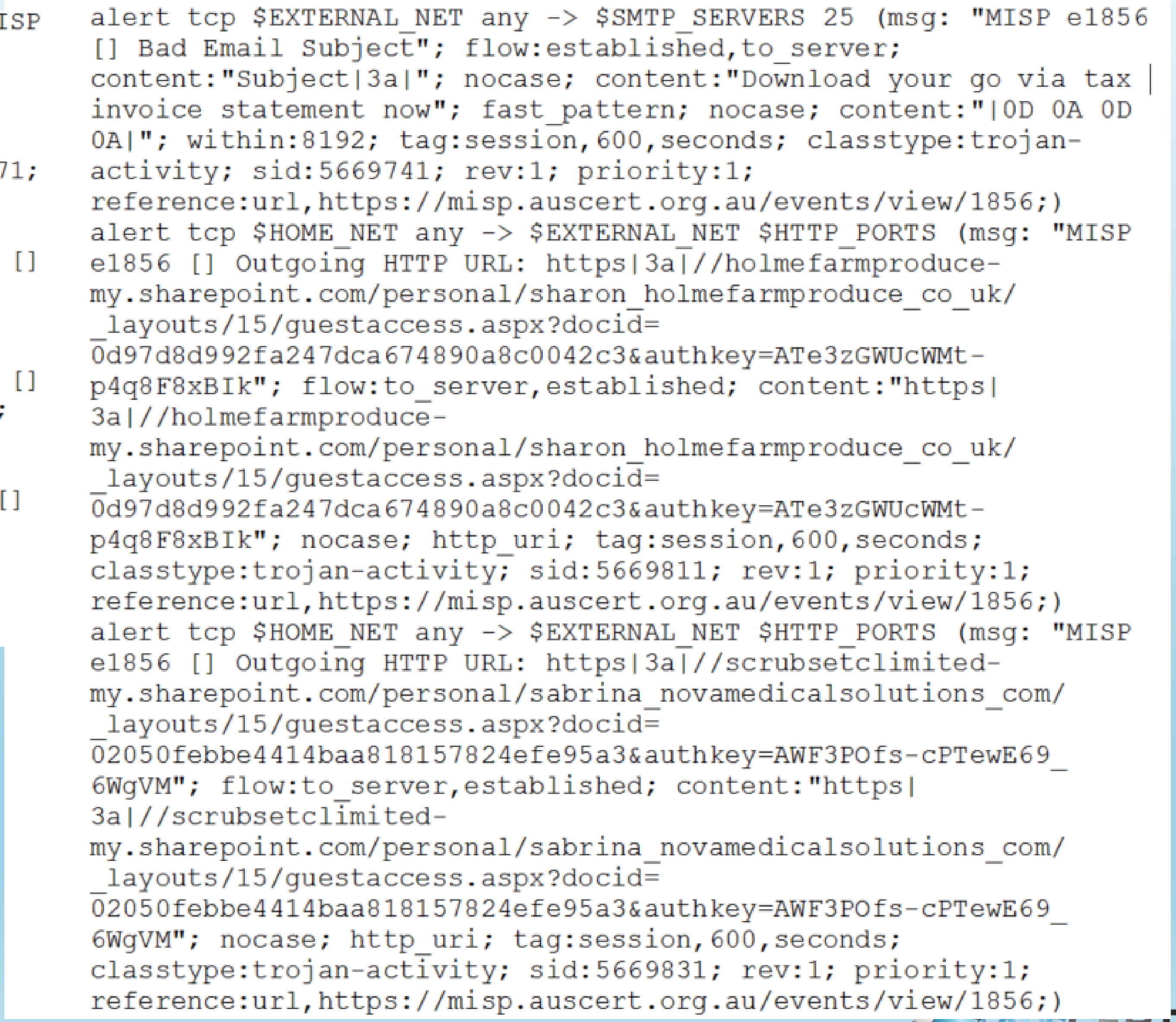
- MISP XML (metadata + all attributes) — Encode Attachments ☑
- MISP JSON (metadata + all attributes) — Encode Attachments ☑
- OpenIOC (all indicators marked to IDS)
- CSV — Include non-IDS marked attributes ☐
- STIX XML (metadata + all attributes) — Encode Attachments ☐
- STIX JSON (metadata + all attributes) — Encode Attachments ☐
- RPZ Zone file
- Download Suricata rules
- Download Snort rules
- Download Bro rules
- Export all attribute values as a text file — Include non-IDS marked attributes ☐

Export as Download Snort rules

Manually downloaded indicators: Snort rules for event 1856

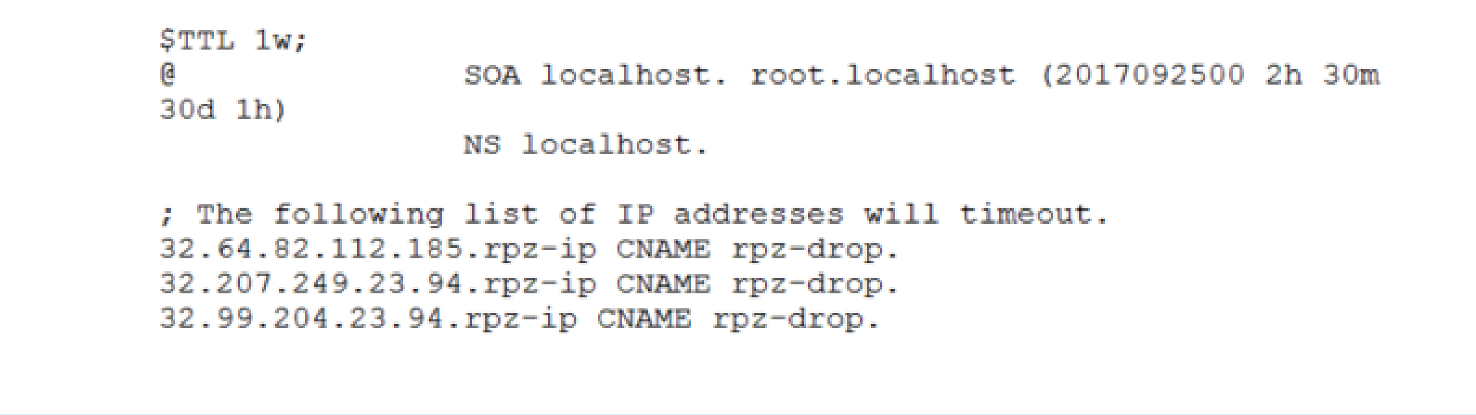


```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP
e1856 [] Outgoing HTTP URL: http|
3a|//94.23.249.207/pdf/Telstra_Bill.pdf";
flow:to_server,established; content:"http|
3a|//94.23.249.207/pdf/Telstra_Bill.pdf"; nocase; http_uri;
tag:session,600,seconds; classtype:trojan-activity; sid:5669871;
rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
alert ip $HOME_NET any -> 185.112.82.64 any (msg: "MISP e1856 []
Outgoing To IP: 185.112.82.64";   classtype:trojan-activity;
sid:5669921; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
alert ip 94.23.249.207 any -> $HOME_NET any (msg: "MISP e1856 []
Incoming From IP: 94.23.249.207";   classtype:trojan-activity;
sid:5670231; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
alert ip 94.23.204.99 any -> $HOME_NET any (msg: "MISP e1856 []
Incoming From IP: 94.23.204.99";   classtype:trojan-activity;
sid:5670241; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
#
```



```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg: "MISP e1856
[] Bad Email Subject"; flow:established,to_server;
content:"Subject|3a|"; nocase; content:"Download your go via tax
invoice statement now"; fast_pattern; nocase; content:"|0D 0A 0D
0A|"; within:8192; tag:session,600,seconds; classtype:trojan-
activity; sid:5669741; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP
e1856 [] Outgoing HTTP URL: https|3a|//holmefarmproduce-
my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/
_layouts/15/guestaccess.aspx?docid=
0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-
p4q8F8xBIk"; flow:to_server,established; content:"https|
3a|//holmefarmproduce-
my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/
_layouts/15/guestaccess.aspx?docid=
0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-
p4q8F8xBIk"; nocase; http_uri; tag:session,600,seconds;
classtype:trojan-activity; sid:5669811; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP
e1856 [] Outgoing HTTP URL: https|3a|//scrubsetclimited-
my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/
_layouts/15/guestaccess.aspx?docid=
02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_
6WgVM"; flow:to_server,established; content:"https|
3a|//scrubsetclimited-
my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/
_layouts/15/guestaccess.aspx?docid=
02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_
6WgVM"; nocase; http_uri; tag:session,600,seconds;
classtype:trojan-activity; sid:5669831; rev:1; priority:1;
reference:url,https://misp.auscert.org.au/events/view/1856;)
```

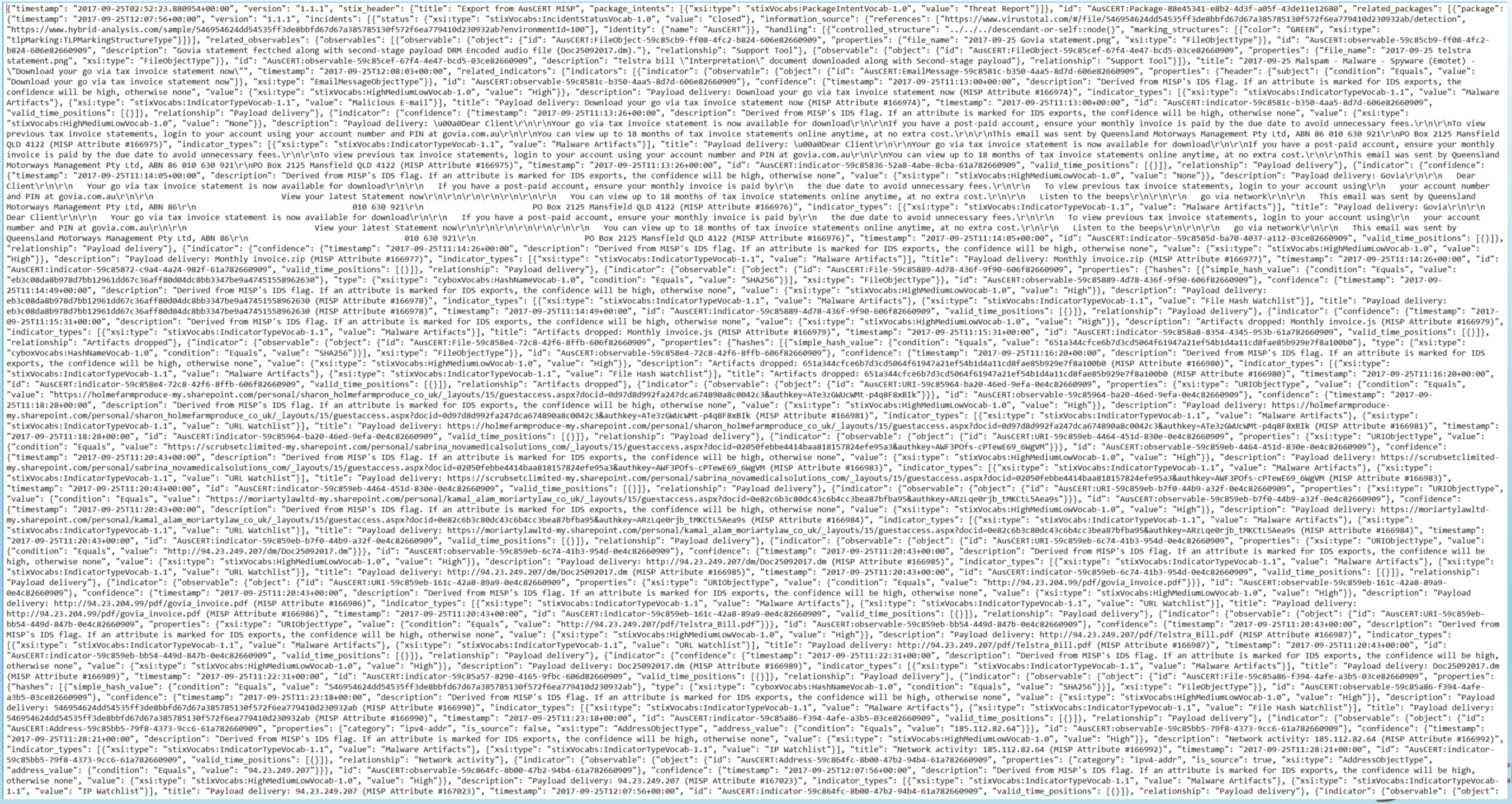
Manually downloaded indicators: RPZ for event 1856



```
$TTL 1w;
@               SOA localhost. root.localhost (2017092500 2h 30m
30d 1h)
                NS localhost.

; The following list of IP addresses will timeout.
32.64.82.112.185.rpz-ip CNAME rpz-drop.
32.207.249.23.94.rpz-ip CNAME rpz-drop.
32.99.204.23.94.rpz-ip CNAME rpz-drop.
```

Manually downloaded indicators: STIX JSON for event 1856



```
{"timestamp": "2017-09-25T02:52:23.880954+00:00", "version": "1.1.1", "stix_header": {"title": "Export from AusCERT MISP", "package_intents": [{"xsi:type": "stixVocabs:PackageIntentVocab-1.0", "value": "Threat Report"}]}, "id": "AusCERT:Package-88e45341-e8b2-4d3f-a05f-43de11e12680", "related_packages": [{"package":
{"timestamp": "2017-09-25T12:07:56+00:00", "version": "1.1.1", "incidents": [{"status": {"xsi:type": "stixVocabs:IncidentStatusVocab-1.0", "value": "Closed"}, "information_source": {"references": ["https://www.virustotal.com/#/file/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab/detection",
"https://www.hybrid-analysis.com/sample/546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab?environmentId=100"], "identity": {"name": "AusCERT"}}, "handling": [{"controlled_structure": "../../../descendant-or-self::node()", "marking_structures": [{"color": "GREEN", "xsi:type":
"tlpMarking:TLPMarkingStructureType"}]}], "related_observables": {"observables": [{"observable": {"object": {"id": "AusCERT:FileObject-59c85cb9-ff08-4fc2-b824-606e82660909", "properties": {"file_name": "2017-09-25 Govia statement.png", "xsi:type": "FileObjectType"}}, "id": "AusCERT:observable-59c85cb9-ff08-4fc2-
b824-606e82660909", "description": "Govia statement fectched along with second-stage payload DRM Encoded audio file (Doc25092017.dm)."}, "relationship": "Support Tool"}, {"observable": {"object": {"id": "AusCERT:FileObject-59c85cef-67f4-4e47-bcd5-03ce82660909", "properties": {"file_name": "2017-09-25 telstra
statement.png", "xsi:type": "FileObjectType"}}, "id": "AusCERT:observable-59c85cef-67f4-4e47-bcd5-03ce82660909", "description": "Telstra bill \"Interpretation\" document downloaded along with Second-stage payload"}, "relationship": "Support Tool"}]}, "title": "2017-09-25 Malspam - Malware - Spyware (Emotet) -
\"Download your go via tax invoice statement now\"", "timestamp": "2017-09-25T12:08:03+00:00", "related_indicators": {"indicators": [{"indicator": {"observable": {"object": {"id": "AusCERT:EmailMessage-59c8581c-b350-4aa5-8d7d-606e82660909", "properties": {"header": {"subject": {"condition": "Equals", "value":
"Download your go via tax invoice statement now"}}, "xsi:type": "EmailMessageObjectType"}}, "id": "AusCERT:observable-59c8581c-b350-4aa5-8d7d-606e82660909"}, "confidence": {"timestamp": "2017-09-25T11:13:00+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the
confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: Download your go via tax invoice statement now (MISP Attribute #166974)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware
Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malicious E-mail"}], "title": "Payload delivery: Download your go via tax invoice statement now (MISP Attribute #166974)", "timestamp": "2017-09-25T11:13:00+00:00", "id": "AusCERT:indicator-59c8581c-b350-4aa5-8d7d-606e82660909",
"valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"confidence": {"timestamp": "2017-09-25T11:13:26+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type":
"stixVocabs:HighMediumLowVocab-1.0", "value": "None"}}, "description": "Payload delivery: \u00a0Dear Client\r\n\r\nYour go via tax invoice statement is now available for download\r\n\r\nIf you have a post-paid account, ensure your monthly invoice is paid by the due date to avoid unnecessary fees.\r\n\r\nTo view
previous tax invoice statements, login to your account using your account number and PIN at govia.com.au\r\n\r\nYou can view up to 18 months of tax invoice statements online anytime, at no extra cost.\r\n\r\nThis email was sent by Queensland Motorways Management Pty Ltd, ABN 86 010 630 921\r\nPO Box 2125 Mansfield
QLD 4122 (MISP Attribute #166975)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}], "title": "Payload delivery: \u00a0Dear Client\r\n\r\nYour go via tax invoice statement is now available for download\r\n\r\nIf you have a post-paid account, ensure your monthly
invoice is paid by the due date to avoid unnecessary fees.\r\n\r\nTo view previous tax invoice statements, login to your account using your account number and PIN at govia.com.au\r\n\r\nYou can view up to 18 months of tax invoice statements online anytime, at no extra cost.\r\n\r\nThis email was sent by Queensland
Motorways Management Pty Ltd, ABN 86 010 630 921\r\nPO Box 2125 Mansfield QLD 4122 (MISP Attribute #166975)", "timestamp": "2017-09-25T11:13:26+00:00", "id": "AusCERT:indicator-59c85836-52a8-4abe-8cba-61a782660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"confidence":
{"timestamp": "2017-09-25T11:14:05+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "None"}}, "description": "Payload delivery: Govia\r\n\r\n   Dear
Client\r\n\r\n   Your go via tax invoice statement is now available for download\r\n\r\n   If you have a post-paid account, ensure your monthly invoice is paid by\r\n   the due date to avoid unnecessary fees.\r\n\r\n   To view previous tax invoice statements, login to your account using\r\n   your account number
and PIN at govia.com.au\r\n\r\n                    View your latest Statement now\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n   You can view up to 18 months of tax invoice statements online anytime, at no extra cost.\r\n\r\n   Listen to the beeps\r\n\r\n\r\n   go via network\r\n\r\n   This email was sent by Queensland
Motorways Management Pty Ltd, ABN 86\r\n                    010 630 921\r\n                    PO Box 2125 Mansfield QLD 4122 (MISP Attribute #166976)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}], "title": "Payload delivery: Govia\r\n\r\n
Dear Client\r\n\r\n   Your go via tax invoice statement is now available for download\r\n\r\n   If you have a post-paid account, ensure your monthly invoice is paid by\r\n   the due date to avoid unnecessary fees.\r\n\r\n   To view previous tax invoice statements, login to your account using\r\n   your account
number and PIN at govia.com.au\r\n\r\n                    View your latest Statement now\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n   You can view up to 18 months of tax invoice statements online anytime, at no extra cost.\r\n\r\n   Listen to the beeps\r\n\r\n\r\n   go via network\r\n\r\n   This email was sent by
Queensland Motorways Management Pty Ltd, ABN 86\r\n                    010 630 921\r\n                    PO Box 2125 Mansfield QLD 4122 (MISP Attribute #166976)", "timestamp": "2017-09-25T11:14:05+00:00", "id": "AusCERT:indicator-59c8585d-ba70-4037-a112-03ce82660909", "valid_time_positions": [{}]},
"relationship": "Payload delivery"}, {"indicator": {"confidence": {"timestamp": "2017-09-25T11:14:26+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value":
"High"}}, "description": "Payload delivery: Monthly invoice.zip (MISP Attribute #166977)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}], "title": "Payload delivery: Monthly invoice.zip (MISP Attribute #166977)", "timestamp": "2017-09-25T11:14:26+00:00", "id":
"AusCERT:indicator-59c85872-c9a4-4a24-982f-61a782660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:File-59c85889-4d78-436f-9f90-606f82660909", "properties": {"hashes": [{"simple_hash_value": {"condition": "Equals", "value":
"eb3c08da8b978d7bb12961dd67c36aff80d04dc8bb3347be9a47451558962630"}, "type": {"xsi:type": "cyboxVocabs:HashNameVocab-1.0", "condition": "Equals", "value": "SHA256"}}], "xsi:type": "FileObjectType"}}, "id": "AusCERT:observable-59c85889-4d78-436f-9f90-606f82660909"}, "confidence": {"timestamp": "2017-09-
25T11:14:49+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery:
eb3c08da8b978d7bb12961dd67c36aff80d04dc8bb3347be9a47451558962630 (MISP Attribute #166978)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "File Hash Watchlist"}], "title": "Payload delivery:
eb3c08da8b978d7bb12961dd67c36aff80d04dc8bb3347be9a47451558962630 (MISP Attribute #166978)", "timestamp": "2017-09-25T11:14:49+00:00", "id": "AusCERT:indicator-59c85889-4d78-436f-9f90-606f82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"confidence": {"timestamp": "2017-
09-25T11:15:31+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Artifacts dropped: Monthly invoice.js (MISP Attribute #166979)",
"indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}], "title": "Artifacts dropped: Monthly invoice.js (MISP Attribute #166979)", "timestamp": "2017-09-25T11:15:31+00:00", "id": "AusCERT:indicator-59c858a8-8354-4345-953b-61a782660909", "valid_time_positions": [{}]},
"relationship": "Artifacts dropped"}, {"indicator": {"observable": {"object": {"id": "AusCERT:File-59c858e4-72c8-42f6-8ffb-606f82660909", "properties": {"hashes": [{"simple_hash_value": {"condition": "Equals", "value": "651a344cfce6b7d3cd5064f61947a21ef54b1d4a11cd8fae85b929e7f8a100b0"}, "type": {"xsi:type":
"cyboxVocabs:HashNameVocab-1.0", "condition": "Equals", "value": "SHA256"}}], "xsi:type": "FileObjectType"}}, "id": "AusCERT:observable-59c858e4-72c8-42f6-8ffb-606f82660909"}, "confidence": {"timestamp": "2017-09-25T11:16:20+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS
exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Artifacts dropped: 651a344cfce6b7d3cd5064f61947a21ef54b1d4a11cd8fae85b929e7f8a100b0 (MISP Attribute #166980)", "indicator_types": [{"xsi:type":
"stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "File Hash Watchlist"}], "title": "Artifacts dropped: 651a344cfce6b7d3cd5064f61947a21ef54b1d4a11cd8fae85b929e7f8a100b0 (MISP Attribute #166980)", "timestamp": "2017-09-25T11:16:20+00:00",
"id": "AusCERT:indicator-59c858e4-72c8-42f6-8ffb-606f82660909", "valid_time_positions": [{}]}, "relationship": "Artifacts dropped"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c85964-ba20-46ed-9efa-0e4c82660909", "properties": {"xsi:type": "URIObjectType", "value": {"condition": "Equals",
"value": "https://holmefarmproduce-my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/_layouts/15/guestaccess.aspx?docid=0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-p4q8F8xBIk"}}}, "id": "AusCERT:observable-59c85964-ba20-46ed-9efa-0e4c82660909"}, "confidence": {"timestamp": "2017-09-
25T11:18:28+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: https://holmefarmproduce-
my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/_layouts/15/guestaccess.aspx?docid=0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-p4q8F8xBIk (MISP Attribute #166981)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type":
"stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery: https://holmefarmproduce-my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/_layouts/15/guestaccess.aspx?docid=0d97d8d992fa247dca674890a8c0042c3&authkey=ATe3zGWUcWMt-p4q8F8xBIk (MISP Attribute #166981)", "timestamp":
"2017-09-25T11:18:28+00:00", "id": "AusCERT:indicator-59c85964-ba20-46ed-9efa-0e4c82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c859eb-4464-451d-830e-0e4c82660909", "properties": {"xsi:type": "URIObjectType", "value":
{"condition": "Equals", "value": "https://scrubsetclimited-my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVM"}}}, "id": "AusCERT:observable-59c859eb-4464-451d-830e-0e4c82660909"}, "confidence":
{"timestamp": "2017-09-25T11:20:43+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: https://scrubsetclimited-
my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVM (MISP Attribute #166983)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type":
"stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery: https://scrubsetclimited-my.sharepoint.com/personal/sabrina_novamedicalsolutions_com/_layouts/15/guestaccess.aspx?docid=02050febbe4414baa818157824efe95a3&authkey=AWF3POfs-cPTewE69_6WgVM (MISP Attribute #166983)",
"timestamp": "2017-09-25T11:20:43+00:00", "id": "AusCERT:indicator-59c859eb-4464-451d-830e-0e4c82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c859eb-b7f0-44b9-a32f-0e4c82660909", "properties": {"xsi:type": "URIObjectType",
"value": {"condition": "Equals", "value": "https://moriartylawltd-my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s"}}}, "id": "AusCERT:observable-59c859eb-b7f0-44b9-a32f-0e4c82660909"}, "confidence":
{"timestamp": "2017-09-25T11:20:43+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: https://moriartylawltd-
my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s (MISP Attribute #166984)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type":
"stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery: https://moriartylawltd-my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc43c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s (MISP Attribute #166984)", "timestamp":
"2017-09-25T11:20:43+00:00", "id": "AusCERT:indicator-59c859eb-b7f0-44b9-a32f-0e4c82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c859eb-6c74-41b3-954d-0e4c82660909", "properties": {"xsi:type": "URIObjectType", "value":
{"condition": "Equals", "value": "http://94.23.249.207/dm/Doc25092017.dm"}}}, "id": "AusCERT:observable-59c859eb-6c74-41b3-954d-0e4c82660909"}, "confidence": {"timestamp": "2017-09-25T11:20:43+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be
high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: http://94.23.249.207/dm/Doc25092017.dm (MISP Attribute #166985)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type":
"stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery: http://94.23.249.207/dm/Doc25092017.dm (MISP Attribute #166985)", "timestamp": "2017-09-25T11:20:43+00:00", "id": "AusCERT:indicator-59c859eb-6c74-41b3-954d-0e4c82660909", "valid_time_positions": [{}]}, "relationship":
"Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c859eb-161c-42a8-89a9-0e4c82660909", "properties": {"xsi:type": "URIObjectType", "value": {"condition": "Equals", "value": "http://94.23.204.99/pdf/govia_invoice.pdf"}}}, "id": "AusCERT:observable-59c859eb-161c-42a8-89a9-
0e4c82660909"}, "confidence": {"timestamp": "2017-09-25T11:20:43+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload
delivery: http://94.23.204.99/pdf/govia_invoice.pdf (MISP Attribute #166986)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery:
http://94.23.204.99/pdf/govia_invoice.pdf (MISP Attribute #166986)", "timestamp": "2017-09-25T11:20:43+00:00", "id": "AusCERT:indicator-59c859eb-161c-42a8-89a9-0e4c82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:URI-59c859eb-
bb54-449d-847b-0e4c82660909", "properties": {"xsi:type": "URIObjectType", "value": {"condition": "Equals", "value": "http://94.23.249.207/pdf/Telstra_Bill.pdf"}}}, "id": "AusCERT:observable-59c859eb-bb54-449d-847b-0e4c82660909"}, "confidence": {"timestamp": "2017-09-25T11:20:43+00:00", "description": "Derived from
MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: http://94.23.249.207/pdf/Telstra_Bill.pdf (MISP Attribute #166987)", "indicator_types":
[{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "URL Watchlist"}], "title": "Payload delivery: http://94.23.249.207/pdf/Telstra_Bill.pdf (MISP Attribute #166987)", "timestamp": "2017-09-25T11:20:43+00:00", "id":
"AusCERT:indicator-59c859eb-bb54-449d-847b-0e4c82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"confidence": {"timestamp": "2017-09-25T11:22:31+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: Doc25092017.dm (MISP Attribute #166989)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}], "title": "Payload delivery: Doc25092017.dm
(MISP Attribute #166989)", "timestamp": "2017-09-25T11:22:31+00:00", "id": "AusCERT:indicator-59c85a57-8290-4165-9fbc-606d82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id": "AusCERT:File-59c85a86-f394-4afe-a3b5-03ce82660909", "properties":
{"hashes": [{"simple_hash_value": {"condition": "Equals", "value": "546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab"}, "type": {"xsi:type": "cyboxVocabs:HashNameVocab-1.0", "condition": "Equals", "value": "SHA256"}}], "xsi:type": "FileObjectType"}}, "id": "AusCERT:observable-59c85a86-f394-4afe-
a3b5-03ce82660909"}, "confidence": {"timestamp": "2017-09-25T11:23:18+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload
delivery: 546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab (MISP Attribute #166990)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "File Hash Watchlist"}], "title": "Payload delivery:
546954624dd54535ff3de8bbfd67d67a385785130f572f6ea779410d230932ab (MISP Attribute #166990)", "timestamp": "2017-09-25T11:23:18+00:00", "id": "AusCERT:indicator-59c85a86-f394-4afe-a3b5-03ce82660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object": {"id":
"AusCERT:Address-59c85bb5-79f8-4373-9cc6-61a782660909", "properties": {"category": "ipv4-addr", "is_source": false, "xsi:type": "AddressObjectType", "address_value": {"condition": "Equals", "value": "185.112.82.64"}}}, "id": "AusCERT:observable-59c85bb5-79f8-4373-9cc6-61a782660909"}, "confidence": {"timestamp":
"2017-09-25T11:28:21+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high, otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Network activity: 185.112.82.64 (MISP Attribute #166992)",
"indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "IP Watchlist"}], "title": "Network activity: 185.112.82.64 (MISP Attribute #166992)", "timestamp": "2017-09-25T11:28:21+00:00", "id": "AusCERT:indicator-
59c85bb5-79f8-4373-9cc6-61a782660909", "valid_time_positions": [{}]}, "relationship": "Network activity"}, {"indicator": {"observable": {"object": {"id": "AusCERT:Address-59c864fc-8b00-47b2-94b4-61a782660909", "properties": {"category": "ipv4-addr", "is_source": true, "xsi:type": "AddressObjectType",
"address_value": {"condition": "Equals", "value": "94.23.249.207"}}}, "id": "AusCERT:observable-59c864fc-8b00-47b2-94b4-61a782660909"}, "confidence": {"timestamp": "2017-09-25T12:07:56+00:00", "description": "Derived from MISP's IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none", "value": {"xsi:type": "stixVocabs:HighMediumLowVocab-1.0", "value": "High"}}, "description": "Payload delivery: 94.23.249.207 (MISP Attribute #167023)", "indicator_types": [{"xsi:type": "stixVocabs:IndicatorTypeVocab-1.1", "value": "Malware Artifacts"}, {"xsi:type": "stixVocabs:IndicatorTypeVocab-
1.1", "value": "IP Watchlist"}], "title": "Payload delivery: 94.23.249.207 (MISP Attribute #167023)", "timestamp": "2017-09-25T12:07:56+00:00", "id": "AusCERT:indicator-59c864fc-8b00-47b2-94b4-61a782660909", "valid_time_positions": [{}]}, "relationship": "Payload delivery"}, {"indicator": {"observable": {"object":
```

Automatically retrieving indicators via the API

- Snort (NIDS) rule: *https://misp.auscert.org.au/events/nids/snort/download/1856*

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg: "MISP e1856 [] Bad Email Subject";
flow:established,to_server; content:"Subject|3a|"; nocase; content:"Download your go via tax invoice statement
now"; fast_pattern; nocase; content:"|0D 0A 0D 0A|"; within:8192; tag:session,600,seconds; classtype:trojan-activity;
sid:5669741; rev:1; priority:1; reference:url,https://misp.auscert.org.au/events/view/1856;)
```

Alert on inbound traffic to SMTP servers on standard SMTP port bearing mail subject: *“ Download your go via tax invoice statement now”*

- Snort (NIDS) rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e1856 [] Outgoing HTTP URL:
http|3a|//94.23.249.207/dm/Doc25092017.dm"; flow:to_server,established;
content:"http|3a|//94.23.249.207/dm/Doc25092017.dm"; nocase; http_uri; tag:session,600,seconds; classtype:trojan-
activity; sid:5669851; rev:1; priority:1; reference:url,https://misp.auscert.org.au/events/view/1856;)
```

Alert on outbound traffic to this url:
http://94.23.249.207/dm/Doc25092017.dm

Automatically retrieving indicators via the API

- Snort (NIDS) rule: *https://misp.auscert.org.au/events/nids/snort/download/1856*

```
alert ip $HOME_NET any -> 185.112.82.64 any (msg: "MISP e1856 [] Outgoing To IP: 185.112.82.64";   classtype:trojan-
activity; sid:5669921; rev:1; priority:1; reference:url,https://misp.auscert.org.au/events/view/1856;)
```

Alert on outbound traffic on any port to IP: *" 185.112.82.64". Contacted by Emotet Spyware.*

- Suricata (NIDS) rule: *https://misp.auscert.org.au/events/nids/suricata/download/1856*

```
alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg: "MISP e1856 [] Outgoing URL: https|3a|//moriartylawltd-
my.sharepoint.com/personal/kamal_alam_moriartylaw_co_uk/_layouts/15/guestaccess.aspx?docid=0e82c6b3c80dc4
3c6b4cc3bea87bfba95&authkey=ARzLqe0rjb_tMKCtL5Aea9s"; tls_cert_subject; content:"moriartylawltd-
my.sharepoint.com"; nocase; pcre:"/moriartylawltd-my.sharepoint.com$/"; tag:session,600,seconds; classtype:trojan-
activity; sid:5669841; rev:1; priority:1; reference:url,https://misp.auscert.org.au/events/view/1856;)
```

Alert on inbound traffic on port 443 for second-stage payload delivery URL

Automatically retrieving indicators via the API

- RPZ file – DNS firewalls: *https://misp.auscert.org.au/attributes/rpz/download/null/1856*

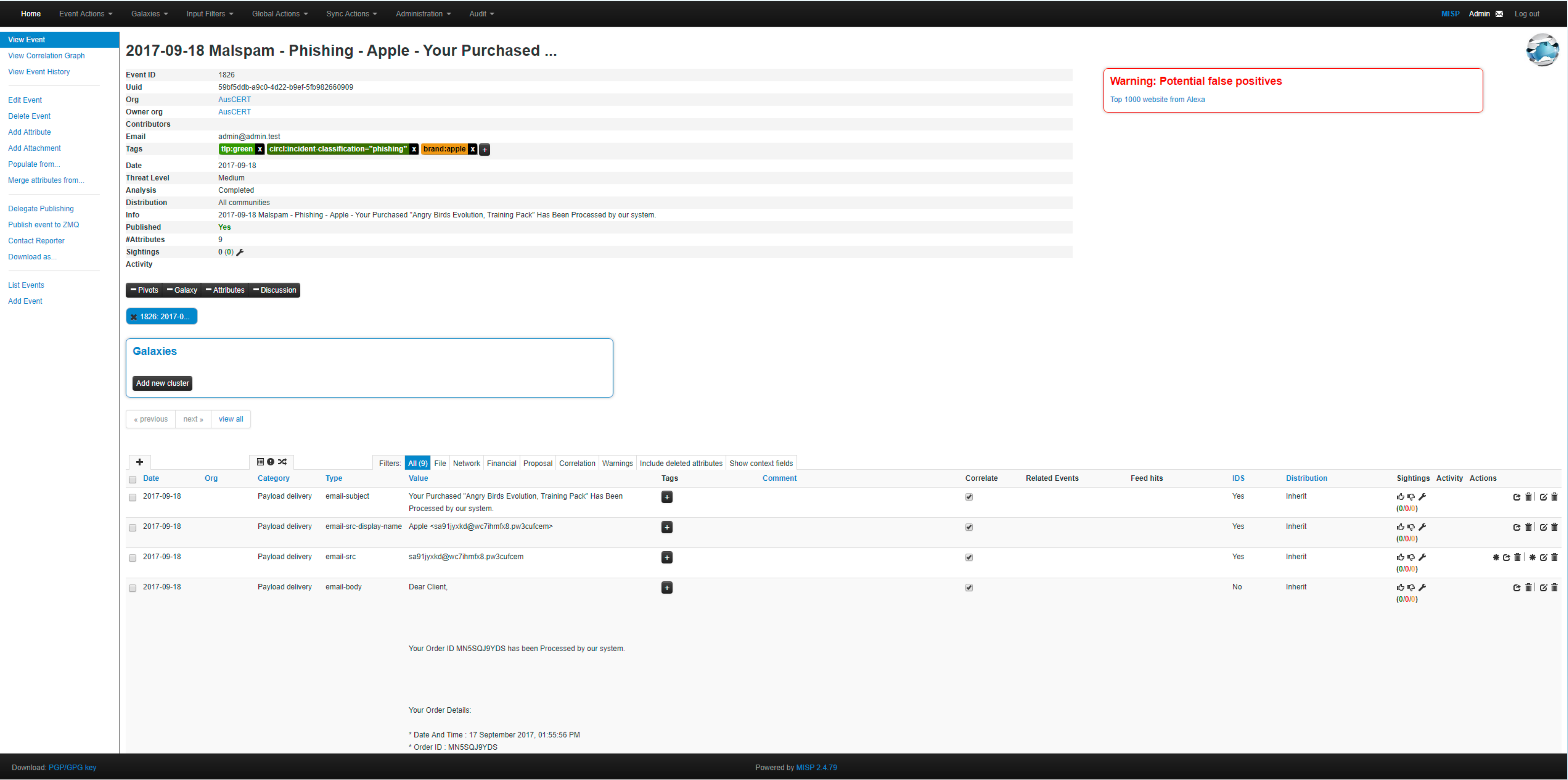
```
$TTL 1w;@            SOA localhost. root.localhost (2017092500 2h 30m 30d 1h)            NS localhost.; The following list
of IP addresses will timeout.32.64.82.112.185.rpz-ip CNAME rpz-drop.32.207.249.23.94.rpz-ip CNAME rpz-
drop.32.99.204.23.94.rpz-ip CNAME rpz-drop.
```

Timeout resolution attempts for IPs: 185.112.82.64, 94.23.249.207 and 94.23.204.99

- URL list (TXT file): *https://misp.auscert.org.au/attributes/text/download/url/null/1856*

```
http://94.23.204.99/pdf/govia_invoice.pdf
http://94.23.249.207/dm/Doc25092017.dm
http://94.23.249.207/pdf/Telstra_Bill.pdf
https://holmefarmproduce-
my.sharepoint.com/personal/sharon_holmefarmproduce_co_uk/_layouts/15/guestaccess.aspx?docid=0d97d8d992fa247dca674890a8c
0042c3&authkey=ATe3zGWUcWMt-p4q8F8xBIk
```

MISP: Phishing Event



2017-09-18 Malspam - Phishing - Apple - Your Purchased ...

Event ID	1826
Uuid	59bf5ddb-a9c0-4d22-b9ef-5fb982660909
Org	AusCERT
Owner org	AusCERT
Contributors	
Email	admin@admin.test
Tags	tlp:green x circl:incident-classification="phishing" x brand:apple x +
Date	2017-09-18
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	2017-09-18 Malspam - Phishing - Apple - Your Purchased "Angry Birds Evolution, Training Pack" Has Been Processed by our system.
Published	Yes
#Attributes	9
Sightings	0 (0)
Activity	

Warning: Potential false positives

Top 1000 website from Alexa

Galaxies

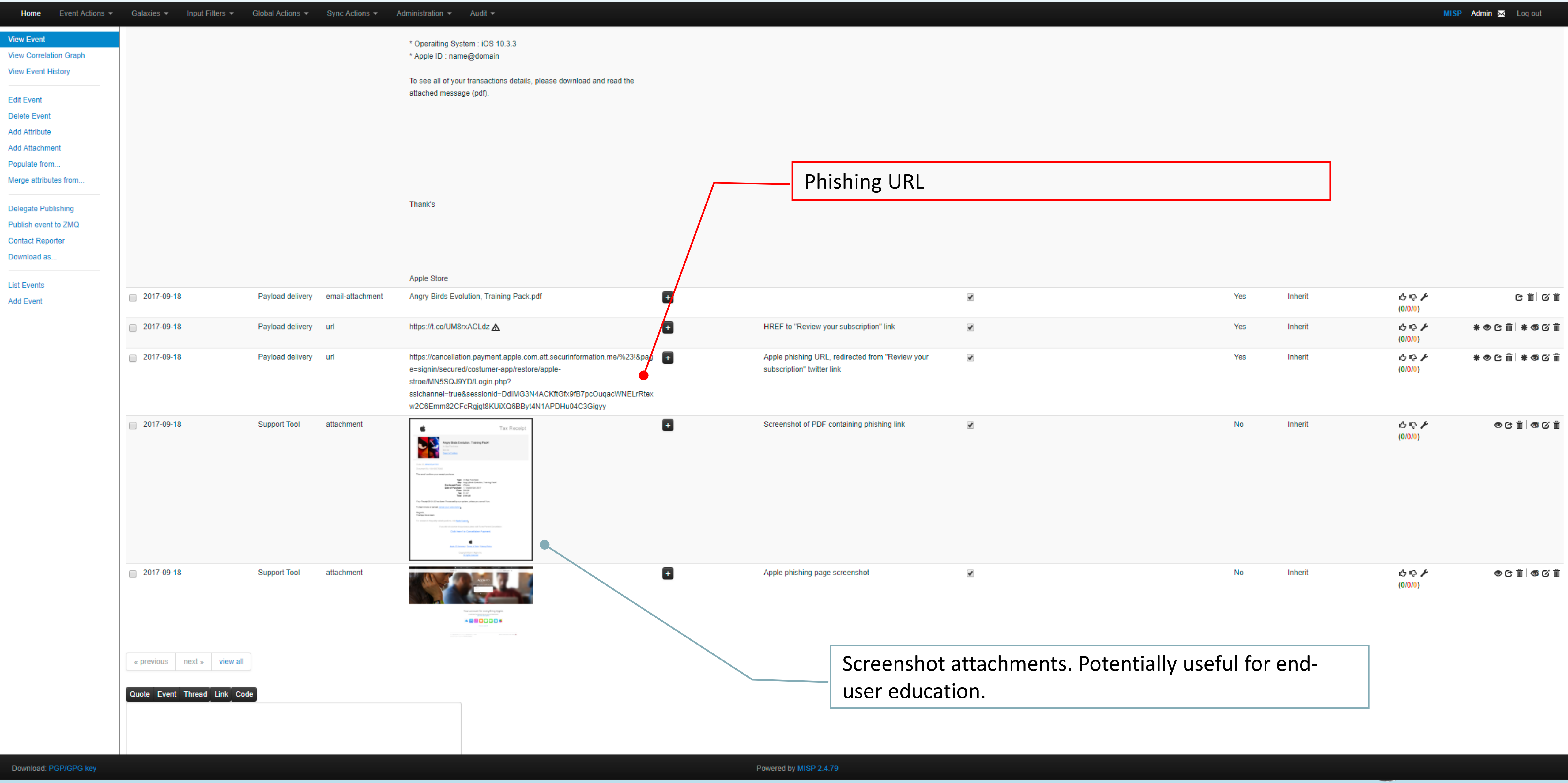
Filters: All (9) File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

□	Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2017-09-18		Payload delivery	email-subject	Your Purchased "Angry Birds Evolution, Training Pack" Has Been Processed by our system.	+		☑			Yes	Inherit	(0/0/0)		
□	2017-09-18		Payload delivery	email-src-display-name	Apple <sa91jyxkd@wc7ihmfx8.pw3cufcem>	+		☑			Yes	Inherit	(0/0/0)		
□	2017-09-18		Payload delivery	email-src	sa91jyxkd@wc7ihmfx8.pw3cufcem	+		☑			Yes	Inherit	(0/0/0)		
□	2017-09-18		Payload delivery	email-body	Dear Client, Your Order ID MN5SQJ9YDS has been Processed by our system. Your Order Details: * Date And Time : 17 September 2017, 01:55:56 PM * Order ID : MN5SQJ9YDS	+		☑			No	Inherit	(0/0/0)		

Download: PGP/GPG key

Powered by MISP 2.4.79

MISP: Phishing Event – part 2



* Operaiting System : iOS 10.3.3
* Apple ID : name@domain

To see all of your transactions details, please download and read the attached message (pdf).

Thank's

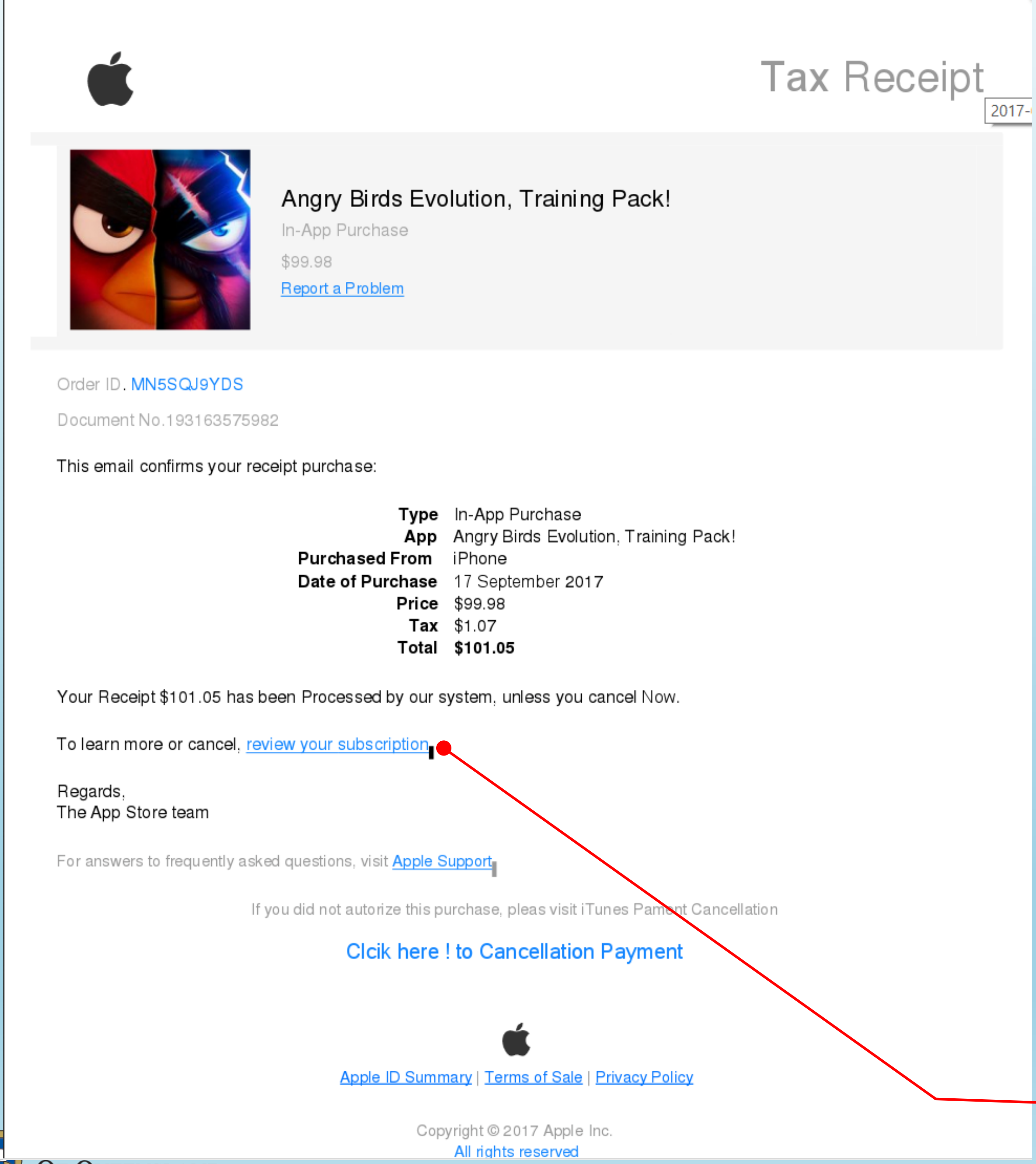
Apple Store

□	2017-09-18	Payload delivery	email-attachment	Angry Birds Evolution, Training Pack.pdf	+		☑	Yes	Inherit	(0/0/0)
□	2017-09-18	Payload delivery	url	https://t.co/UM8rxACLdz ⚠	+	HREF to "Review your subscription" link	☑	Yes	Inherit	(0/0/0)
□	2017-09-18	Payload delivery	url	https://cancellation.payment.apple.com.att.securinformation.me/%23!&pag e=signin/secured/costumer-app/restore/apple-stroe/MN5SQJ9YD/Login.php?sslchannel=true&sessionid=DdIMG3N4ACKftGfx9fB7pcOuqacWNELrRtexw2C6Emm82CFcRgjgt8KUiXQ6BByt4N1APDHu04C3Gigyy	+	Apple phishing URL, redirected from "Review your subscription" twitter link	☑	Yes	Inherit	(0/0/0)
□	2017-09-18	Support Tool	attachment	Tax Receipt	+	Screenshot of PDF containing phishing link	☑	No	Inherit	(0/0/0)
□	2017-09-18	Support Tool	attachment		+	Apple phishing page screenshot	☑	No	Inherit	(0/0/0)

Phishing URL

Screenshot attachments. Potentially useful for end-user education.

Phishing Event – part 3



Tax Receipt

2017-

Angry Birds Evolution, Training Pack!

In-App Purchase

$99.98

Report a Problem

Order ID. MN5SQJ9YDS

Document No.193163575982

This email confirms your receipt purchase:

Type	In-App Purchase
App	Angry Birds Evolution, Training Pack!
Purchased From	iPhone
Date of Purchase	17 September 2017
Price	$99.98
Tax	$1.07
Total	**$101.05**

Your Receipt $101.05 has been Processed by our system, unless you cancel Now.

To learn more or cancel, review your subscription

Regards,
The App Store team

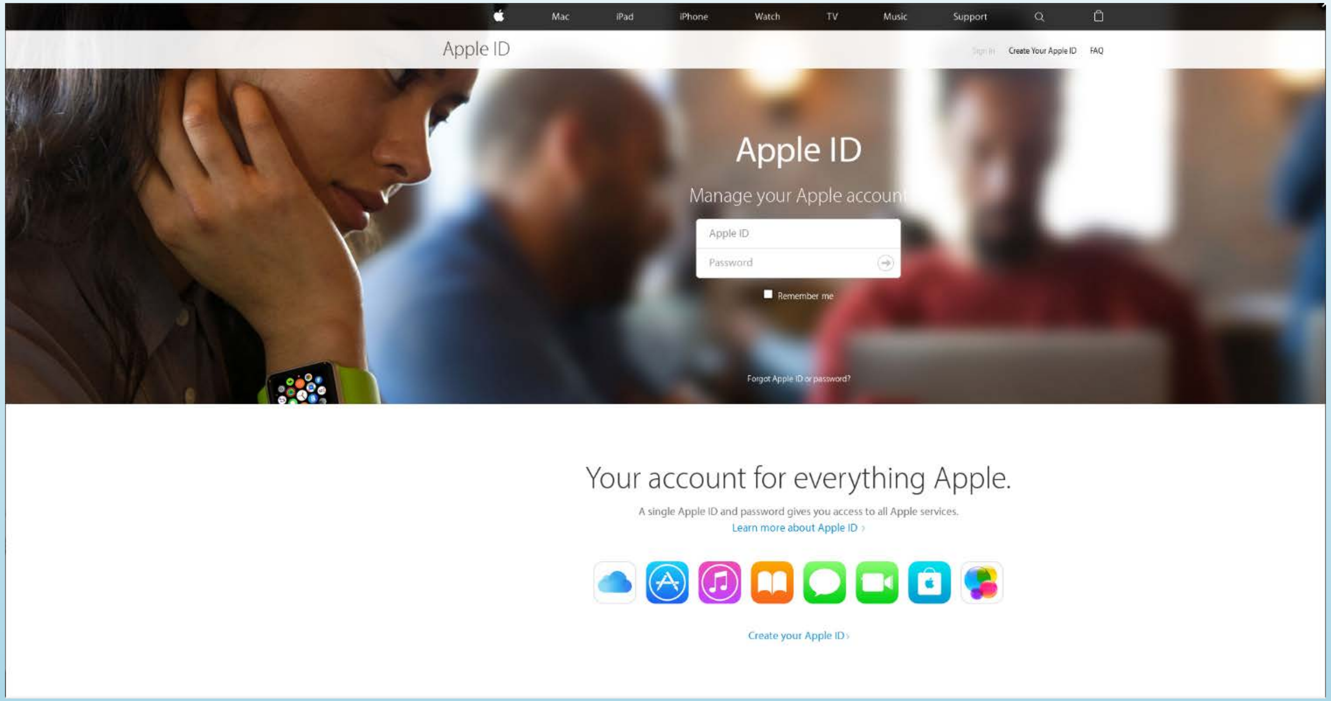
For answers to frequently asked questions, visit Apple Support

If you did not autorize this purchase, pleas visit iTunes Pament Cancellation

Clcik here ! to Cancellation Payment

Apple ID Summary | Terms of Sale | Privacy Policy

Copyright © 2017 Apple Inc.
All rights reserved



Apple ID

Manage your Apple account

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID ›

Create your Apple ID ›

Phishing Link in PDF document attached with phishing mail.
https://cancellation.payment.apple.com.att.securinformation.me/%23!&page=signin/secured/costumer-app/restore/apple-stroe/MN5SQJ9YD/Login.php

Questions?

AusCERT: membership@auscert.org.au

Phone: 1800 648 458

James Culverhouse | AusCERT General Manager

Mike Holm | Operations Manager

Web: https://www.auscert.org.au | Twitter: https://twitter.com/AusCERT