



# ■ CAUDIT-ISAC: FROM CONCEPT TO REALITY

AUSCERT, 26<sup>TH</sup> SEPTEMBER 2018

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM



# IN THE BEGINNING.....

## › WHY CAUDIT-ISAC

### › CAUDIT IDENTIFIED CYBERSECURITY IN ITS TOP 10 PRIORITY LIST (2016)

### › THREAT INTELLIGENCE

- › NEED TO PREVENT THREATS BEING REALISED
- › NEED TO DETECT A SUCCESSFULLY EXECUTED THREAT

### › AN ISAC

- › AUSCERT PROPOSED AN ISAC
- › A CENTRALISED, PERSISTENT SOURCE OF TRUSTED THREAT INFORMATION
- › CONSIDERED COLLABORATION WITH REN-ISAC
- › NEEDED A LOCALISED ENTITY FUNCTIONING TAPPING INTO LOCAL AND EXTERNAL THREAT INFORMATION SOURCES
- › THIS WAS THE SAME REASON AUSCERT WAS FORMED IN THE FIRST PLACE BACK IN 1993



# REINVENTING THE WHEEL (NOT!): RESEARCH

---

- › STRUCTURE - STUDY TOUR TO REN-ISAC 2016\
- › MEMBERSHIP MODEL
- › GOVERNANCE STRUCTURE
- › OPERATIONS HOSTING ARRANGEMENT

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM



# REINVENTING THE WHEEL (NOT!): RESEARCH

## › RESEARCH

### › POTENTIAL PLATFORMS (SEVERAL SOLUTIONS AVAILABLE)

- › HP THREAT CENTRAL
- › SOLTRA EDGE
- › LOGRHYTHM THREAT LIFECYCLE MANAGEMENT (TLM) PLATFORM
- › FIREEYE ISIGHT THREAT INTELLIGENCE
- › ALIENVault UNIFIED SECURITY MANAGEMENT (USM)
- › MALWARE INFORMATION SHARING PLATFORM

### › DIFFERENTIATED BY:

- › PRICE (COMMERCIAL VS. FREE)
- › SYSTEM REQUIREMENTS (PROPRIETARY VS. OPEN SOURCE)
- › ALERTING AND REPORTING CAPABILITIES
- › SUPPORT
- › THREAT INTELLIGENCE (OPEN-IOC, STIX) DATA FORMATS SUPPORTED
- › AVAILABLE FEEDS AND DATA SOURCES (OPEN VS. CLOSED)
- › THIRD PARTY INTEGRATION



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM



## > WHAT IS AN ISAC

- > CENTRAL LOCATION FOR SUBMITTING INDICATORS OF COMPROMISE FROM SIGHTED CAMPAIGNS
- > PLATFORM FOR SHARING THREAT INFORMATION FOR HUMAN AND MACHINE CONSUMPTION
- > CURATE SHARED INFORMATION FOR:
  - > ACCURACY (IDENTIFY POSSIBLE FALSE POSITIVES)
  - > RELIABILITY (ESTABLISHING TRUSTWORTHINESS OF SOURCE, HANDLING FALSE INFORMATION)
- > CONFIDENTIALITY (E.G. DELEGATED PUBLICATION OF INDICATORS FOR SERIOUS INCIDENT)
- > THREAT INTELLIGENCE SHARING FORMAT SUPPORT (E.G. MACHINE INGESTIBLE FORMAT)
- > SUPPORT FOR FEEDS



# CAUDIT-ISAC TRIAL

- › **STARTED PLANNING LATE 2016**
- › **STARTED IN FEBRUARY 2017**
  - › **SET UP MISP INSTANCE**
  - › **DEVELOPED PRACTISES**
  - › **ONBOARDING PROCESS**
  - › **ACCESS RESTRICTIONS**
- › **CONTRIBUTIONS FROM MEMBERS IN THE AREAS OF:**
  - › **MALWARE SAMPLES**
  - › **REMOTE MISP SYNC TESTING**
  - › **CONTRIBUTING EVENTS**
  - › **ADOPTING MINDSETS TOWARDS THE THREAT INTEL PLATFORM.. HOW WE SHARE THREAT INTEL**

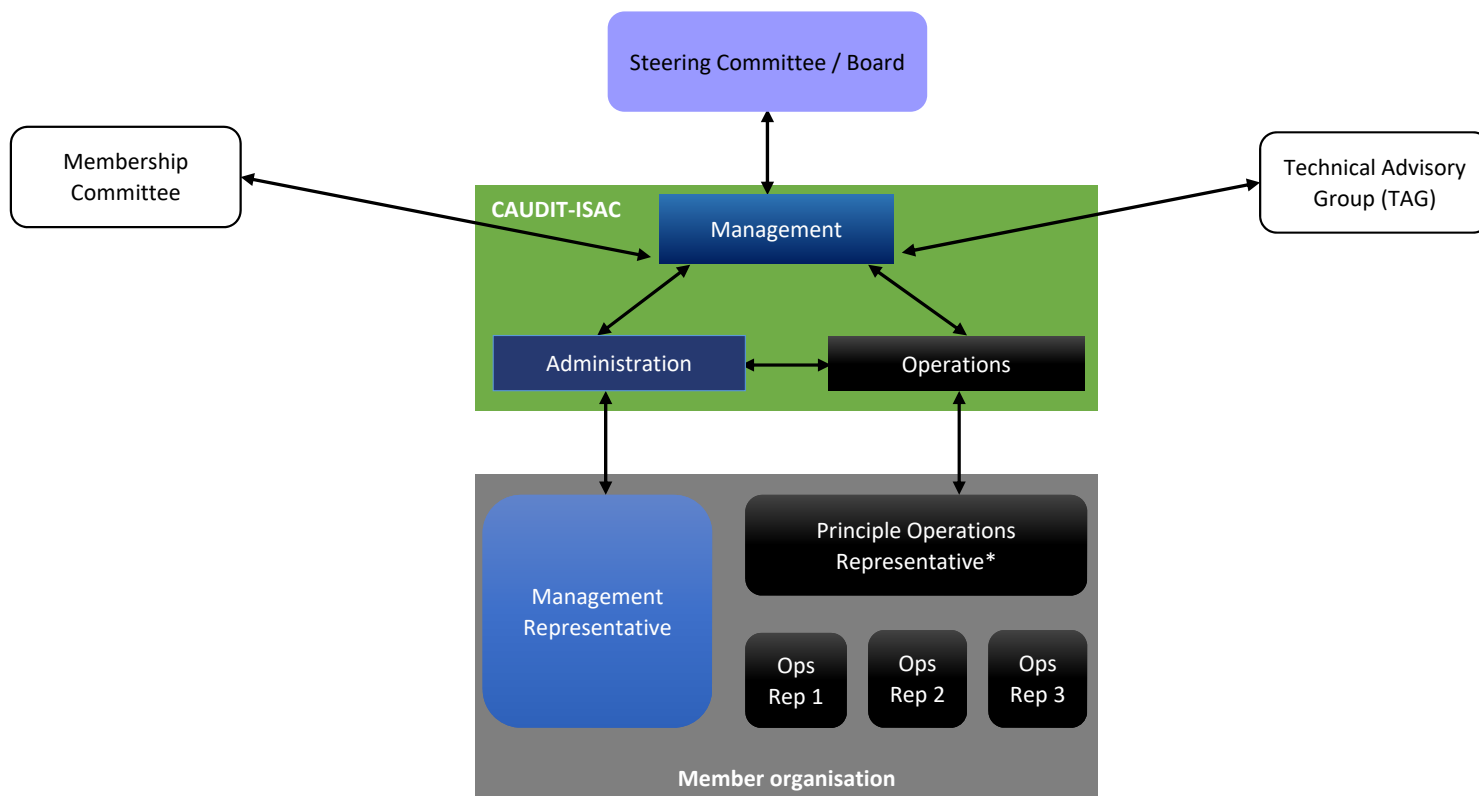


# CAUDIT-ISAC PRINCIPLES

- › LOW VOLUME, HIGH CONFIDENCE
- › ASAP
- › MINIMISE FALSE POSITIVES
- › LOCAL CONTEXT (AND REGION) RELEVANT INFORMATION
- › SHARE, SHARE, SHARE (PRODUCE AS WELL CONSUME)
- › MAXIMISE APPLICABILITY (OF INDICATORS IN MEMBER ENVIRONMENTS) – FORMAT COMPATIBILITY
- › MAXIMISE VISIBILITY (INTO THREATS TARGETING AUSTRALIA AND NZ) – FEED SOURCES



# CAUDIT-ISAC GOVERNANCE AND OPERATION MODEL







# CAUDIT-ISAC STEERING COMMITTEE

- › PROVIDE DIRECTION ON RETAINING MEMBERSHIP, INCREASING MEMBERSHIP
- › MEMBERSHIP FEE AND BENEFIT ADJUSTMENTS
- › ACCEPT/REJECT PROPOSALS FOR CHANGE FROM MEMBERSHIP COMMITTEE & TAG
- › CONSTITUTION:
  - › CAUDIT-ISAC MANAGEMENT (3)
  - › REPS ELECTED FROM MANAGEMENT REPS MEMBER ORGS (5-6)
  - › NOMINATED AND SECONDED EXTERNAL EXPERTS (1-2)
  - › QUORUM TO BE DETERMINED



# CAUDIT-ISAC TECHNICAL ADVISORY GROUP (TAG)

- › PROVIDE INPUT TO CAUDIT-ISAC MANAGEMENT, ON:
  - › FEASIBILITY OF PROPOSED AMENDMENTS TO SHARING POLICY
  - › COMPLAINTS OF VIOLATION OF SHARING POLICY BY A MEMBER
  - › PROPOSALS TO EXPAND THE SCOPE AND DEPTH OF SHARED INFORMATION (E.G. NEW INDICATOR TYPES).
- › CONSTITUTION:
  - › OPERATIONAL REPRESENTATIVES NOMINATED BY MANAGEMENT REPRESENTATIVES, DELIBERATED AND APPROVED BY THE STEERING COMMITTEE
  - › TECHNICAL LIAISONS



# CAUDIT-ISAC MEMBERSHIP COMMITTEE

## › MEMBERSHIP COMMITTEE FUNCTIONS

- › PROVIDE DIRECTION ON RETAINING MEMBERSHIP, INCREASING MEMBERSHIP
- › MEMBERSHIP FEE AND BENEFIT ADJUSTMENTS
- › ACCEPT/REJECT PROPOSALS FOR CHANGE FROM MEMBERSHIP COMMITTEE & TAG

## › CONSTITUTION:

- › CAUDIT-ISAC MANAGEMENT (3)
- › REPS ELECTED FROM MEMBER ORGANIZATION MANAGEMENT REPS



# CAUDIT-ISAC OPERATIONS

## › OPERATIONS

- › **PROVIDE TECHNICAL GUIDANCE AND IMPART KNOWLEDGE** ON THE USE OF TECHNOLOGY PLATFORMS AND TECHNICAL SHARING PRACTICES, BY WAY OF REGULAR TRAINING SESSIONS TO CAUDIT-ISAC OPERATIONAL REPRESENTATIVES
- › **VET INFORMATION** SHARED BY CAUDIT-ISAC MEMBERS, AND WHERE REQUIRED, ISSUE PROPOSALS FOR CHANGE, IN A TIMELY MANNER TO MINIMISE VIOLATIONS OF THE INFORMATION SHARING POLICY, MINIMISE FALSE POSITIVES AND PRESERVE, TO THE FULLEST EXTENT POSSIBLE, THE ACCURACY OF SHARED INFORMATION.
- › **DELEGATION.** RECEIVE RAW INCIDENT DATA AND THREAT INFORMATION FROM MEMBERS AND/OR TRUSTED THIRD PARTIES, CURATE AND SHARE INFORMATION RELEVANT TO THE BUSINESS ACTIVITIES OF THE MEMBERSHIP, WHILE PRESERVING THE ANONYMITY OF THE REPORTER.
- › **ENGAGE WITH TRUSTED AND RELEVANT THIRD PARTY THREAT INTELLIGENCE SOURCES** TO GAIN ADDED VISIBILITY OVER THE THREAT LANDSCAPE
- › **MONITOR** SHARED THREAT INFORMATION FOR **NON-COMPLIANCE** WITH THE CAUDIT-ISAC INFORMATION SHARING POLICY AND TAKE CORRECTIVE ACTION
- › **RECEIVE MALICIOUS ARTEFACTS** FROM THE MEMBERSHIP, TRUSTED THIRD PARTIES AND INTERNAL SOURCES, PERFORM ANALYSIS, EXTRACT ACTIONABLE INDICATORS AND SHARE WITH THE MEMBERSHIP.
- › **MAINTAIN AND SECURE CAUDIT-ISAC INFRASTRUCTURE** TO ENSURE PRESERVATION OF THE CONFIDENTIALITY AND INTEGRITY OF SHARED INFORMATION, AND THE AVAILABILITY OF SERVICES.

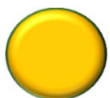


AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## CAUDIT-ISAC INFORMATION SHARING POLICY (1): CONFIDENTIALITY



INFORMATION STRICTLY PASSED IN CONFIDENCE. NO PERSISTENT RECORD OF THIS INFORMATION SHOULD BE CREATED.  
(WE DON'T DO TLP:RED IN MISP)



INFORMATION SHOULD ONLY BE SHARED AMONG ORGANISATIONS WITH A NEED-TO-KNOW (SHARED WITHIN A SUBSET OF USERS IN THE GENERAL MISP INSTANCE, I.E. SHARING GROUP)



CAN BE SHARED WITHIN A MISP COMMUNITY (MISP USERS WITHIN A SINGLE MISP INSTANCE)



INFORMATION CAN BE SHARED IN THE PUBLIC DOMAIN (ALL USERS WITHIN A MISP INSTANCE AND ITS CONNECTED COMMUNITIES)



CHATHAM HOUSE RULES (CHR): THE ORIGINAL SOURCE OF THIS INFORMATION DOES NOT WANT TO BE ATTRIBUTED.

EXAMPLE:

IF THE BANK OF ANTARCTICA WERE COMPROMISED AND WANTED TO SHARE THREAT INDICATORS WITH OTHER BANKS, WITHOUT IDENTIFYING ITSELF, IT COULD DELEGATED PUBLISHING THE INFORMATION TO ANTARCTICA-CERT.



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## CAUDIT-ISAC INFORMATION SHARING POLICY (2): DISTRIBUTION

Distribution	Use condition(s)	Audience
Not allowed	TLP Red	Not applicable
Sharing group (organisation) - special	TLP Amber	Organisational administrators for organisations identified as legitimate recipients of the shared information.
Organisation	TLP Amber	Distribution of information to all users belonging to the sharing member organisation.
Community	TLP Green	All users on the primary channel, including standalone MISP platforms synchronising to CAUDIT-ISAC.
Sharing Group – standard	TLP Green	Sector specific audience for receiving specialised threat information (e.g. finance, government)
All communities	TLP White	All users on the primary channel, including standalone MISP platforms synchronising to CAUDIT-ISAC and all servers synchronised to those servers. This is the largest audience.





AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## CAUDIT-ISAC INFORMATION SHARING POLICY (3): ACCURACY AND TRUST

Rating	Description	Tag
Information Credibility		
1	Confirmed by other sources	admiralty-scale:information-credibility="1"
2	Probably true	admiralty-scale:information-credibility="2"
3	Possibly true	admiralty-scale:information-credibility="3"
4	Doubtful	admiralty-scale:information-credibility="4"
5	Improbable	admiralty-scale:information-credibility="5"
6	Truth cannot be judged	admiralty-scale:information-credibility="6"
Source Reliability		
a	Completely reliable	admiralty-scale:source-reliability="a"
b	Usually reliable	admiralty-scale:source-reliability="b"
c	Fairly reliable	admiralty-scale:source-reliability="c"
d	Not usually reliable	admiralty-scale:source-reliability="d"
e	Unreliable	admiralty-scale:source-reliability="e"
f	Reliability cannot be judged	admiralty-scale:source-reliability="f"





## CAUDIT-ISAC MISP ACCESS: RESTRICTING ACCESS

- › Using an SSL Client Certificate
- › PKCS#12 certificate to be imported to certificate store
- › PEM Format to be used for API access
- › Client certificate is bound to an organisation



**AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM**

## CAUDIT-ISAC MISP ACCESS: WEB PORTAL

Home

Event Actions >

Galaxies >

Input Filters >

Global Actions >

Sync Actions >

Administration >

Audit >

MSPAdminLog out

List Events  
Add Event  
Import From MSP Export  
  
List Attributes  
Search Attributes  
  
View Proposals  
Events with proposals  
  
Export  
Automation

Events

< previous123456789101112next>

QMy EventsOrg Events

Published	Org	Owner Org	ID	Clusters	Tags	#Attr.	#Corr.	#Sightings	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
<input checked="" type="checkbox"/>			1856	Tool: Emotet Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Spyware" brand:go_via</div>	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	
<input checked="" type="checkbox"/>			1858	Tool: Emotet Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Spyware" brand:telstra</div>	21	3		admin@admin.test	2017-09-25	High	Completed	2017-09-25 Malspam - Malware - Spyware (Emotet) - "Telstra Bill - Arrival Notification"	All	
<input checked="" type="checkbox"/>			1857		<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Trojan"</div>	6			peter@auscert.org.au	2017-09-25	Medium	Completed	2017-09-25 Malspam - Malware - Trojan	All	
<input checked="" type="checkbox"/>			1855		<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Trojan"</div>	8			peter@auscert.org.au	2017-09-25	Medium	Completed	2017-09-25 Malspam - Malware - Trojan - RE: 17AP0267-Q269 DOC	All	
<input checked="" type="checkbox"/>			1854	Ransomware: Locky Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Ransomware"</div>	29			admin@admin.test	2017-09-25	High	Completed	2017-09-25 Malspam - Malware - Ransomware (Locky) - "Your Invoice # 115266"	All	
<input checked="" type="checkbox"/>			1846		<div>Hip:green circl:incident. classification:"malware" brand:austpost</div>	22	10		admin@admin.test	2017-09-21	Medium	Completed	2017-09-21 Malspam - Malware - AusPost - "Australia Post Delivery Notification"	All	
<input checked="" type="checkbox"/>			1842	Ransomware: Locky Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Ransomware"</div>	35	4		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "msg0020_Asterisk-11461468201-234142299-114614682011-3097.7z"	All	
<input checked="" type="checkbox"/>			1843	Ransomware: Locky Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Ransomware"</div>	50	5		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "Your Payment # 7831"	All	
<input checked="" type="checkbox"/>			1845	Ransomware: Locky Q	<div>Hip:green circl:incident. classification:"malware" malware_classification:maware-category:"Ransomware"</div>	42	4		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "Status of invoice A2173311-08"	All	
<input checked="" type="checkbox"/>			1844	Ransomware: Locky Q	<div>Hip:green</div>	90	6		admin@admin.test	2017-09-21	High	Completed	2017-09-21 Malspam - Malware - Ransomware (Locky) - "New voice message 1181262574 in mailbox 1181262574-44_Rom_1181262574_P_1181262574-44"	All	

DownloadPGPIGkey

Powered byMISP 2.4.79

RELEVANT TAGS. USEFUL FOR FILTERING EVENTS (E.G. BRAND TAG, TLP TAG)

SEVERITY LEVEL. ALSO USEFUL FOR FILTERING (E.G. HIGH SEVERITY THREATS).

SCOPE OF DISTRIBUTION (GOVERNED BY TLP)

INVESTIGATION STATUS



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

# WARNINGS, CORRELATIONS AND EXTERNAL INFO

Home

Event Actions

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Audit

MISP

Admin

Log out

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from...

Merge attributes from...

Delegate Publishing

Publish event to ZMQ

Contact Reporter

Download as...

List Events

Add Event

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

Event ID

1856

Uuid

59cd5800-c588-44aa-958f-03ca82680909

Org

AusCERT

Owner org

AusCERT

Contributors

Email

admin@admin.test

Tags

tip-green x circ: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

Pivots

Galaxy

Attributes

Discussion

< 1856: 2017-0...

Galaxies

Tool Q

+ Emotet Q

Add new cluster

EXTERNAL ANALYSIS REPORTS

tool: Emotet

Cluster ID

11032

Name

Emotet

Parent Galaxy

Tool

Description

Source

MISP Project

Authors

Alexandre Dulaioy, Florian Roth, Timo Steffens, Christophe Vandeplas

Events

10 event(s)

Analysis article for Emotet banking TROJAN

Key Value

refs

https://occertid.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis

synonyms

Geoids

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

Warning: Potential false positives

2017-09-25 (1856) 2017-09-13 (1801)

Top 1000 website from Alexa

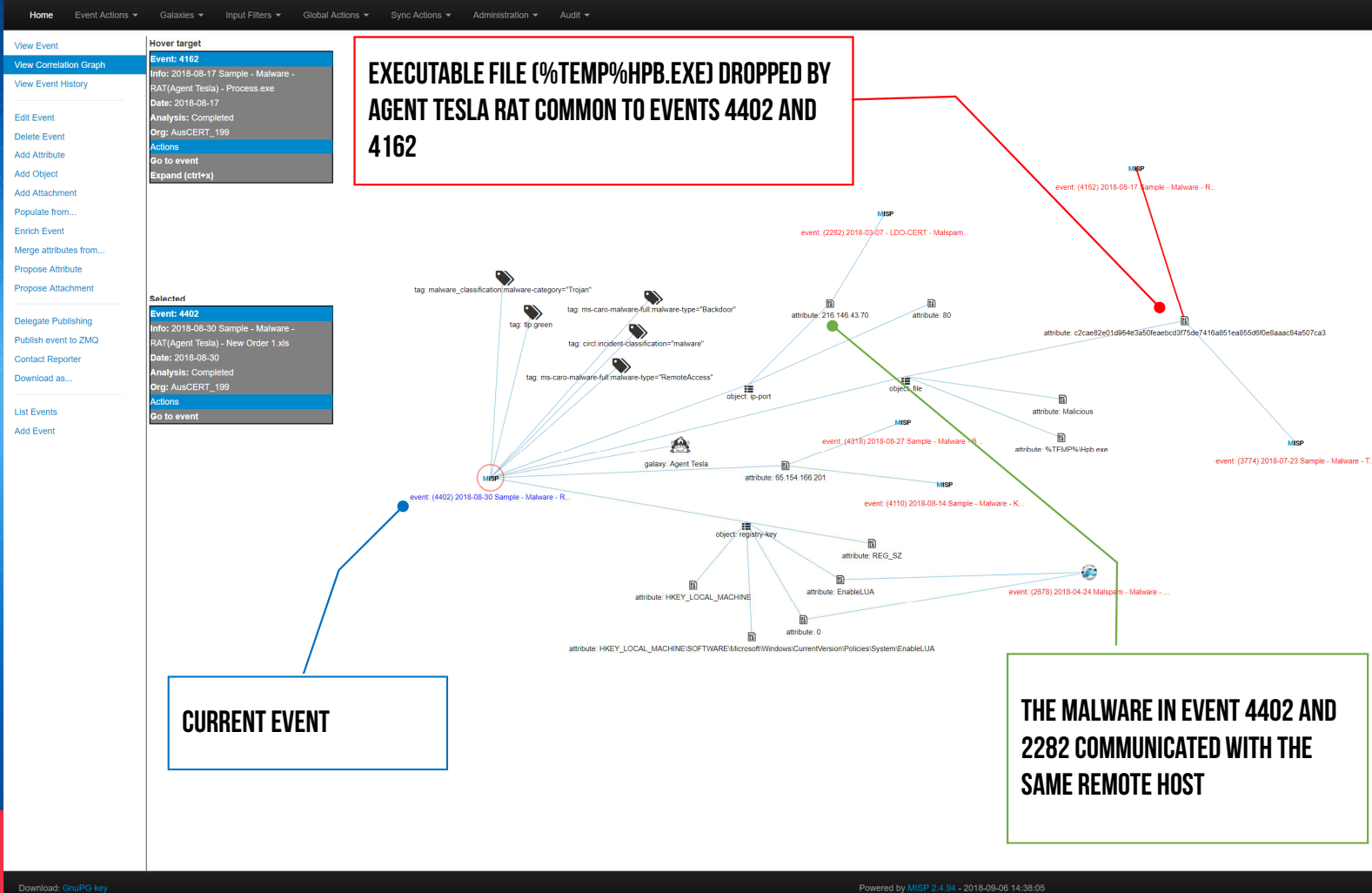
Correlating Event ID

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/5489548246054535f3e3b6b0b067d67a3057785130572f6ea779410d230932ab0detection		Virustotal report for Doc25092017.dm		1858		Yes	Inherit	0 (0/1)		
2017-09-25		Artifacts dropped	sha256	651a344dce6b7d3cd506481947a21ef54b14411cd8fae85b929e78a100b0		Ref: Monthly invoice.js				Yes	Inherit	0 (0/1)		
2017-09-25		Artifacts dropped	filename	Monthly invoice.js		JS extracted from ZIP primary payload				Yes	Inherit	0 (0/1)		
2017-09-25		External analysis	link	https://www.hybrid-analysis.com/sample/5489548246054535f3e3b6b0b067d67a3057785130572f6ea779410d230932ab?environmentId=100		Hybrid analysis report for Doc25092017.dm		1858		Yes	Inherit	0 (0/1)		
2017-09-25		Network activity	ip-dst	185.112.82.64		Remote server contacted by Doc25092017.dm		1858		Yes	Inherit	0 (0/1)		
2017-09-25		Payload delivery	email-subject	Download your go via tax invoice statement now				1801		Yes	Inherit	0 (0/1)		
2017-09-25		Payload delivery	url	http://94.23.204.09/pdfgovia_invoice.pdf		second-stage payload delivery url, extracted from Monthly invoice.js		1858		Yes	Inherit	0 (0/1)		
2017-09-25		Payload delivery	ip-src	94.23.249.207		second-stage payload delivery IP		1858		Yes	Inherit	0 (0/1)		

Download: PGP/GPG key

Powered by MISP 2.4.79

# CORRELATION GRAPH – AGENT TESLA RAT





AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

# COMMENTS AND FALSE POSITIVE WARNINGS

Home

Event Actions

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Audit

MISP

Admin

Log out

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from...

Merge attributes from...

Delegate Publishing

Publish event to ZIMQ

Contact Reporter

Download as...

List Events

Add Event

2017-09-25	Payload delivery	sha256	546954624d654538f3da8b0d67d67a385785130572f6ea7794100230932ab	+	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://m0riarjia/vi/5f-m5/sharepoint.com/personal/kamal_alam_m0riarjia/co.uk/_layouts/15/q/uestaccess.aspx?docid=9d82c3d0d43d84c3bea87b0a958authkey=ARzLqoYb_IMKCHLSAewR ⚠️	+	second-stage payload delivery url, extracted from Monthly invoice.js	✓	1858	Yes	Inherit	(0/0/0)	🔍📄🔗🔒🔑
2017-09-25	Payload delivery	url	https://scrubsetlimited-my.sharepoint.com/personal/sabina_rovamedicalsolutions_com/_layouts/15/q/uestaccess.aspx?docid=0205f9bbe4414baa/8157824ef95633authkey=AVF3P0fc-cFTenE69_8/llq/vM ⚠️	+	second-stage payload delivery url, extracted from Monthly invoice.js	✓	1858	Yes	Inherit	(0/0/0)	🔍📄🔗🔒🔑
2017-09-25	Payload delivery	url	kill-chain:Delivery x co-my.sharepoint.com/personal/sharon_holmesfarmproduce_co_uk/_layouts/15/q/uestaccess.aspx?docid=9d87d9d992a247dca674890a8c0042c38authkey=ATa3cGVUcUWMt-p4q8Fb-Blik ⚠️	+	primary payload delivery URL in email body	✓		Yes	Inherit	(0/0/0)	🔍📄🔗🔒🔑
2017-09-25	Payload delivery	sha256	e53c08d8b978d7b612961d687c36af80d04d3bb3347be9a47451558062630	+	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

COMMENTS AND ATTRIBUTE LEVEL TAGS TO BUILD CONTEXT FOR INDICATORS OF A SIMILAR TYPE (E.G. URLS). AIDS HUMAN INTERPRETATION.

Download

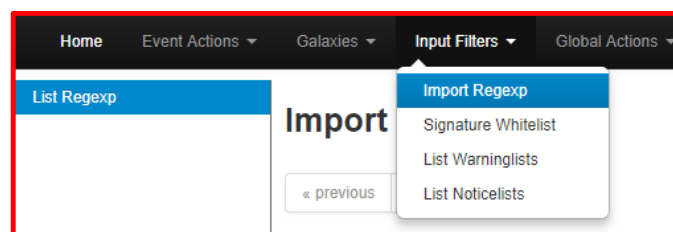
PGP/GPG key

Powered by MISP 2.4.79



REGISTRY KEY ENTRIES THAT MAY EXPOSE A USER'S SID ARE REWRITTEN TO A GENERIC VALUE

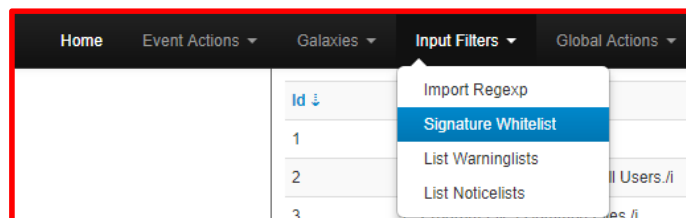
# MINIMISING FALSE POSITIVES: INPUT REGEX FILTERS



FILE DIRECTORY PATHS THAT MAY EXPOSE USER DETAILS REWRITTEN WITH A GENERIC VALUE

Id ↓	Regex	Replacement	Type
1	/.\ProgramData./i	%ALLUSERSPROFILE%\	ALL
2	/.\Documents and Settings\All Users./i	%ALLUSERSPROFILE%\	ALL
3	/.\Program Files\Common Files./i	%COMMONPROGRAMFILES%\	ALL
4	/.\Program Files (x86)\Common Files./i	%COMMONPROGRAMFILES(x86)%\	ALL
5	/.\Users\(.*)\AppData\Local\Temp./i	%TEMP%\	ALL
6	/.\ProgramData./i	%PROGRAMDATA%\	ALL
7	/.\Program Files./i	%PROGRAMFILES%\	ALL
8	/.\Program Files (x86)/i	%PROGRAMFILES(x86)%\	ALL
9	/.\Users\Public./i	%PUBLIC%\	ALL
10	/.\Documents and Settings\(.*)\Local Settings\Temp./i	%TEMP%\	ALL
11	/.\Users\(.*)\AppData\Local\Temp./i	%TEMP%\	ALL
12	/.\Users\(.*)\AppData\Local./i	%LOCALAPPDATA%\	ALL
13	/.\Users\(.*)\AppData\Roaming./i	%APPDATA%\	ALL
14	/.\Users\(.*)\Application Data./i	%APPDATA%\	ALL
15	/.\Windows\(.*)\Application Data./i	%APPDATA%\	ALL
16	/.\Users\(.*)\i	%USERPROFILE%\	ALL
17	/.\DOCUME~1\(.*)\i	%USERPROFILE%\	ALL
18	/.\Documents and Settings\(.*)\i	%USERPROFILE%\	ALL
19	/.\Windows./i	%WINDIR%\	ALL
20	/.\Windows./i	%WINDIR%\	ALL
21	/REGISTRY\USER.S(-[0-9]{1})(2)-[0-9]{2}(-[0-9]{9})(1)(-[0-9]{10})(1)-[0-9]{9}(-[0-9]{4})/i	HKCU	ALL
22	/REGISTRY\USER.S(-[0-9]{1})(2)-[0-9]{2}(-[0-9]{10})(2)-[0-9]{9}(-[0-9]{4})/i	HKCU	ALL
23	/REGISTRY\USER.S(-[0-9]{1})(2)-[0-9]{2}(-[0-9]{10})(3)-[0-9]{4}/i	HKCU	ALL
24	/REGISTRY\MACHINE./i	HKLM\	ALL
25	/Registry.Machine./i	HKLM\	ALL

# MINIMISING FALSE POSITIVES: SIGNATURE WHITELIST



IP RESOLVING TO A SHARED HOSTING SERVER  
THAT MAY BLOCK ACCESS TO LEGITIMATE SITES,  
IF BLACKLISTED

PREVENT ANY ATTRIBUTES MATCHING  
AUSCERT.ORG.AU FROM BEING EXPORTED  
AS A THREAT INDICATOR

## Signature Whitelist

Regex entries (in the standard php regex `/[regex]/[modifier]` format) entered below will restrict matchi

« previous next »

Id	Name
4	/203.5.76.236/
3	/203.5.76.238/
2	/auscert.org.au/
7	/bit.ly/
8	/comodoca4.com/
5	/dropbox.com/
10	/www.msftconnecttest.com/

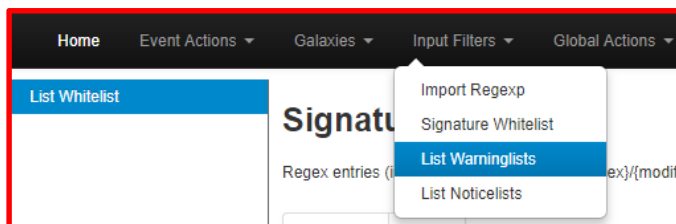
Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7





ATTRIBUTE TYPES AFFECTED BY  
WARNING LIST

# MINIMISING FALSE POSITIVES: INPUT REGEX FILTERS



38	List of known public DNS resolvers expressed as hostname	20171224	Event contains one or more public DNS resolvers (expressed as hostname) as attribute with an IDS flag set	hostname	hostname, domain, url
37	List of known OvH Cluster IP	20180222	OvH Cluster IP address (https://docs.ovh.com/fr/hosting/liste-des-adresses-ip-des-clusters-et-hebergements-web/)	string	ip-src, ip-dst, domain
36	List of RFC 5771 multicast CIDR blocks	3	Event contains one or more entries part of the RFC 5771 multicast CIDR blocks	cidr	ip-src, ip-dst, domain
35	List of known Office 365 IP address ranges in China	20171229	Office 365 IP address ranges in China	cidr	ip-src, ip-dst, domain
34	List of known Office 365 URLs and IP address ranges	20171229	Office 365 URLs and IP address ranges	substring	ip-src, ip-dst, domain
33	List of known Microsoft Azure Datacenter IP Ranges	20171229	Microsoft Azure Datacenter IP Ranges	cidr	ip-src, ip-dst, domain
32	List of known microsoft domains	2	Event contains one or more entries of known microsoft domains	hostname	domain, hostname, domain
31	List of IPv6 link local blocks	2	Event contains one or more entries part of the IPv6 link local prefix (RFC 4291)	cidr	ip-src, ip-dst, domain
30	List of known google domains	4	Event contains one or more entries of known google domains	hostname	domain, hostname, domain
29	List of known hashes for empty files	2	Event contains one or more entries of empty files based on known hashes	string	md5, sha1, sha224, sha256
28	List of hashes for EICAR test virus	2	Event contains one or more entries based on hashes for EICAR test virus	string	md5, sha1, sha256, sha384
27	List of known domains used by automated malware analysis services & security vendors	3	Domains used by automated malware analysis services & security vendors	substring	domain, hostname, domain
26	List of known Amazon AWS IP address ranges	20180222	Amazon AWS IP address ranges (https://ip-ranges.amazonaws.com/ip-ranges.json)	cidr	ip-src, ip-dst, domain
25	Top 1000 website from Alexa	20171222	Event contains one or more entries from the top 1000 of the most used website (Alexa)	hostname	hostname, domain, url

WARNING LIST ENABLED

## TOP 1000 WEBSITE FROM ALEXA

Id	25	25339
Name	Top 1000 website from Alexa	
Description	Event contains one or more entries from the top 1000 of the most used website (Alexa)	
Version	20171222	431
Type	hostname	
Accepted attribute types	hostname, domain	
Enabled	Yes	16
Values	04dn8g4f.space 104.com.tw 123movies.is 123rf.com 1337x.to 163.com 1688.com 17ok.com 2ch.net 360.cn 39.net 3sk.tv 4chan.org 4dsply.com 4pda.ru 4shared.com 51sole.com 52pk.com	1491 1948 152 1 665 5 15 17 889 1000

CLICK ICON TO VIEW DETAILS

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM



In the Event page of interest, Click on "Download as.."

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## ACCESSING ATTRIBUTES FROM A MISP EVENT: VIA THE WEB USER INTERFACE (2)

Choose the format that you wish to download the event in

MISP XML (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
MISP JSON (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
OpenIOC (all indicators marked to IDS)	
CSV	Include non-IDS marked attributes <input type="checkbox"/>
CSV with additional context	Include non-IDS marked attributes <input type="checkbox"/>
STIX XML (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
Export as STIX XML (metadata + all attributes)	
STIX2 (requires the STIX 2 library)	
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 <input type="checkbox"/>

Cancel



## DNS FIREWALL VENDORS

1. CLOUDFLARE (US)
2. BLUECAT (CANADA)
3. INFOBLOX (US)
4. EFFICIENTIP (FRANCE)
5. EONSCOPE (US)
6. NOMINUM (US)
7. CISCO (US)
8. F5 NETWORKS (US)
9. VERISIGN (US)
10. SWITCH (SWITZERLAND)
11. ESENTIRE (CANADA)
12. THREATSTOP (US)
13. CONSTELLIX (US)
14. VERIGIO COMMUNICATIONS (US)

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## DOWNLOADED EVENT AND RULE OUTPUT FOR EVENT 4494: RESPONSE POLICY ZONE (RPZ) FILE FOR DNS FIREWALL

TIMEOUT DNS QUERIES FOR  
199.115.115.68/32

DNS QUERIES FOR THIS  
DOMAIN AND IT'S  
SUBDOMAINS WILL  
TIMEOUT

```
$TTL 1w;  
@      SOA localhost. root.localhost (2018090700 2h 30m  
30d 1h)  
      NS localhost.
```

; The following list of IP addresses will timeout.  
32.68.115.115.199.rpz-ip CNAME rpz-drop.

; The following domain names and all of their sub-domains will  
timeout.  
gunther.com CNAME rpz-drop.  
\*.gunther.com CNAME rpz-drop.

Choose the format that you wish to download the event in

MISP XML (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
MISP JSON (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
OpenIOC (all indicators marked to IDS)	
CSV	Include non-IDS marked attributes <input type="checkbox"/>
CSV with additional context	Include non-IDS marked attributes <input type="checkbox"/>
STIX XML (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
STIX2 (requires the STIX 2 library)	
RPZ Zone file	

Export as STIX XML (metadata + all attributes)

Cancel



ALERT ON MALICIOUS  
EMAIL SUBJECT

ALERT ON OUTGOING  
TRAFFIC TO MALICIOUS IP

ALERT ON OUTGOING DNS  
REQUEST FOR MALICIOUS  
DOMAIN

ALERT ON OUTGOING HTTP  
REQUEST FOR SECONDARY  
PAYLOAD DELIVERY URL

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM


## DOWNLOADED EVENT AND RULE OUTPUT FOR EVENT 4494: SNORT RULES

alert tcp \$EXTERNAL\_NET any -> \$SMTP\_SERVERS 25 (msg: "**MISP e4494 [] Bad Email Subject**"; flow:established,to\_server;  
content:"Subject|3a|"; nocase; content:"**\*\*\*Quotation Request\*\*\***"; fast\_pattern; nocase; content:"|0D 0A 0D 0A|";  
within:8192; tag:session,600,seconds; classtype:trojan-activity; sid:6755061; rev:1; priority:2;  
reference:url,https://misp.auscert.org.au/events/view/4494;)

alert ip \$HOME\_NET any -> **199.115.115.68** any (msg: "**MISP e4494 [] Outgoing To IP: 199.115.115.68**"; classtype:trojan-  
activity; sid:6755181; rev:1; priority:2; reference:url,https://misp.auscert.org.au/events/view/4494;)

alert udp any any -> any **53** (msg: "**MISP e4494 [] Domain: gunther.com**"; content:"|01 00 00 01 00 00 00 00 00 00|";  
depth:10; offset:2; content:"|07|gunther|03|com|00|"; fast\_pattern; nocase; classtype:trojan-activity; sid:6755221; rev:1;  
priority:2; reference:url,https://misp.auscert.org.au/events/view/4494;)

alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET \$HTTP\_PORTS (msg: "**MISP e4494 [] Outgoing HTTP URL:**  
**http|3a|//194.5.99.87|3a|4560/codes/press1.exe**"; flow:to\_server,established;  
content:"http|3a|//194.5.99.87|3a|4560/codes/press1.exe"; nocase; http\_uri; tag:session,600,seconds; classtype:trojan-  
activity; sid:6755261; rev:1; priority:2; reference:url,https://misp.auscert.org.au/events/view/4494;)  
#

STIX2 (requires the STIX 2 library)
RPZ Zone file
Download Suricata rules
Download Snort rules 
Download Bro rules
Export all attribute values as a text file <input type="checkbox"/>
Include non-IDS marked attributes <input type="checkbox"/>
Cancel



## ACCESSING ATTRIBUTES FROM A MISP EVENT: NIDS RULES VIA THE REST API

NETWORKS IDS RULE EXPORT API SYNTAX

### FORMAT OPTIONS:

1. SURICATA
2. SNORT

EXPORT RULES FOR A SINGLE EVENT

**HTTPS://MISP.AUSCERT.ORG.AU/EVENTS/NIDS/[FORMAT]/DOWNLOAD/[EVENTID]/[FRAME]/[TAGS]/[FROM]/[TO]/[LAST]/[TYPE]/[ENFORCEWARNINGLIST]/[INCLUDEALLTAGS]**

EXPORT RULES FOR EVENTS FROM LAST  
"N" DAYS, HOURS

FROM/TO TO SPECIFY A DATA RANGE

SUBJECT RULE EXPORT TO EXCLUDE ATTRIBUTES FLAGGED  
BY ACTIVE WARNING LISTS (E.G. DON'T EXPORT A DOMAIN  
FLAGGED AS A FALSE POSITIVE BY THE ALEXA TOP 1000 LIST)

EXPORT ATTRIBUTES ONLY FOR THIS  
ATTRIBUTE TYPE (E.G. URL)





## ACCESSING ATTRIBUTES FROM A MISP EVENT: TEXT ATTRIBUTE EXPORT API SYNTAX

EXPORT ATTRIBUTES ONLY FOR THIS  
ATTRIBUTE TYPE (E.G. URL)

EXPORT ATTRIBUTES FROM EVENTS  
CONTAINING THESE TAGS

**HTTPS://MISP-  
C.AUSCERT.ORG.AU/ATTRIBUTES/TEXT/DOWNLOAD/[TYPE]/[TAGS]/[EVENT\_ID]/[ALLOWNONIDS]/  
[FROM]/[TO]/[LAST]/[ENFORCEWARNINGLIST]/[ALLOWNOTPUBLISHED]**

IF SET TO "TRUE", EXPORTS ATTRIBUTES  
FROM EVENTS THAT ARE NOT PUBLISHED.

NOT RECOMMENDED!

FROM/TO TO SPECIFY A DATA RANGE

IF VALUE="TRUE", EXPORTS ATTRIBUTES NOT MARKED "FOR  
IDS" AS WELL.

NOT RECOMMENDED!!!



# MISP API: CUSTOM SCRIPTS USING THE API (1)

## EXAMPLE 1: RETRIEVE EMAIL SUBJECTS FOR EVENT 2350

```
CURL --INSECURE --CERT-TYPE PEM --CERT $CERT_NAME -H "AUTHORIZATION: $AUTH_KEY" HTTPS://MISP.AUSCERT.ORG.AU/ATTRIBUTES/TEXT/DOWNLOAD/EMAIL-SUBJECT/NULL/2100 -KS
```

```
Your Payment - 0160  
Your Payment - 4129  
Your Payment - 5709  
Your Payment - 5839  
Your Payment - 6570
```

## EXAMPLE 2: RETRIEVE URLS FROM EVENT 2300

```
CURL --INSECURE --CERT-TYPE PEM --CERT $CERT_NAME -H "AUTHORIZATION: $AUTH_KEY" HTTPS://MISP.AUSCERT.ORG.AU/ATTRIBUTES/TEXT/DOWNLOAD/URL/NULL/2321 -KS
```

```
https://austaralia-tax.com/homepage?page=index&token=b1e08029e5fe04129dfdefe64b97c3d33be5fdb5&session=90a3749219bbd1f167b4ec96dca3f73e&cookies=9e0e239f7e11f657c842830ab8c7991622f99526&b=4
```

```
https://austaralia-tax.com/homepage?page=verification&token=82fdf7c4b66fe428c70ad6b7d4fdb004081bbf4f&session=19084c897a11c2ce15f130593a97cb90&cookies=1a86b510597091bfa2d94e22994d6423a0f9562e
```

```
https://austaralia-tax.com/send_results?access_code=477a31aa813beeab7a751fd6562eb102&token=6d17c85eb1de9a7771d5c5b15d5ac3df0ed5bb2c-MHF
```





# MISP API: PYMISP (1)

Installing PyMISP <https://github.com/MISP/PyMISP>

## 1. Using pip:

```
pip3 install pymisp
```

## 2. From repo

```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP  
git submodule update --init  
pip3 install -I .
```

## Prerequisite:

Python "requests" library

Documentation available at:

<https://media.readthedocs.org/pdf/pymisp/latest/pymisp.pdf>





# MISP API: PYMISP USAGE EXAMPLES (2)

## 3. Get all events with references to "Lokibot"

```
/PyMISP/examples$ ./searchall.py -s lokibot
```

```
{
  "Event": {
    "timestamp": "1529567070",
    "Galaxy": [],
    "proposal_email_lock": false,
    "org_id": "1",
    "attribute_count": "9",
    "orgc_id": "382",
    "id": "22242",
    "Object": [],
    "Orgc": {
      "id": "382",
      "uuid": "56700651-031c-46bb-96a0-4dc9950d210f",
      "name": "CSIRT-CV_4307",
      "Attribute": [
        {
          "timestamp": "1529565155",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "email body",
          "id": "2010050",
          "uuid": "5b2b4fe3-cbbc-4e0a-8f34-4dc9950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "Hello,\r\n\r\nGood day...\r\n\r\nPlease find attached swift copy in attachment for invoice Payment made.\r\n\r\n\r\nKindly confirm you receive the amount.\r\n\r\n\r\nRegards,\r\n\r\n\r\nMohammed Saif\r\n\r\n\r\nAccounts Payables/Receivables",
          "type": "text",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565184",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "",
          "id": "2010054",
          "uuid": "5b2b5000-2af0-42e1-86bd-4c06950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "Lmartinez@royalgas.mx",
          "type": "email-src",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565212",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "",
          "id": "2010058",
          "uuid": "5b2b501c-8cd4-446c-b6b0-49d2950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "Payment Advice",
          "type": "email-subject",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565700",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "Payment Advice.doc",
          "id": "2010062",
          "uuid": "5b2b5204-65d4-4e25-834b-490e950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "dfded1873ff3fd8fa652641df1c2281",
          "type": "md5",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565735",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "2Wxni.jpg",
          "id": "2010066",
          "uuid": "5b2b5227-79b4-4ead-973d-4de2950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "ca4502d15e675eff7450def47291669f",
          "type": "md5",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565769",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "Ec5rt.hta",
          "id": "2010070",
          "uuid": "5b2b5249-5dd0-40b5-b2f6-4948950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "8900553f1983ec3bb01c62ee012cefc5",
          "type": "md5",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565796",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Network activity",
          "comment": "",
          "id": "2010074",
          "uuid": "5b2b5264-c94c-4ff5-af8d-40dd950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "u.teknik.io",
          "type": "url",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529565817",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Other",
          "comment": "",
          "id": "2010078",
          "uuid": "5b2b5279-bfed-45d6-8dc9-480e950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "RTF document downloads stage1 Ec5rt.hta (hta) that once executed downloads stage2 2Wxni.jpg (exe).",
          "type": "comment",
          "ShadowAttribute": [],
          "event_id": "22242",
          "timestamp": "1529567070",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Network activity",
          "comment": "C2 communication",
          "id": "2010082",
          "uuid": "5b2b575e-0294-4035-aeb3-4df3950d210f",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "http://www.mrkafy22.tk/948847839367294784599484/93847388388883/fre.php",
          "type": "uri",
          "ShadowAttribute": [],
          "event_id": "22242",
          "extends_uuid": "",
          "publish_timestamp": "1529570417",
          "Tag": [
            {
              "id": "131",
              "user_id": "0",
              "hide_tag": false,
              "exportable": true,
              "colour": "#700cf0",
              "name": "MalSpam",
              "id": "500",
              "user_id": "0",
              "hide_tag": false,
              "exportable": true,
              "colour": "#6ed8f0",
              "name": "Lokibot"
            }
          ],
          "analysis": "0",
          "ShadowAttribute": [],
          "distribution": "3",
          "date": "2018-06-21",
          "published": true,
          "Org": {
            "id": "1",
            "uuid": "595591f6-b518-4844-8158-3db68266bc0e",
            "name": "AuscERT",
            "RelatedEvent": [
              {
                "id": "60",
                "uuid": "56a647a-63dc-4471-bce9-4acc25ed029",
                "name": "CERT-BUND",
                "Attribute": [
                  {
                    "timestamp": "1512393593",
                    "deleted": false,
                    "object_relation": null,
                    "Galaxy": [],
                    "distribution": "5",
                    "object_id": "0",
                    "category": "Network activity",
                    "comment": "",
                    "id": "855600",
                    "uuid": "5a254b79-2070-4686-9325-7ee20a2b115a",
                    "disable_correlation": false,
                    "to_ids": true,
                    "sharing_group_id": "0",
                    "value": "ipvhos.duckdns.org/host/fre.php",
                    "type": "url",
                    "ShadowAttribute": [],
                    "event_id": "8514",
                    "timestamp": "1512393593",
                    "deleted": false,
                    "object_relation": null,
                    "Galaxy": [],
                    "distribution": "5",
                    "object_id": "0",
                    "category": "Network activity",
                    "comment": "",
                    "id": "855601",
                    "uuid": "5a254b79-2098-4551-9249-7ee20a2b115a",
                    "disable_correlation": false,
                    "to_ids": true,
                    "sharing_group_id": "0",
                    "value": "www.gtld-server.com/panel/fre.php",
                    "type": "url",
                    "ShadowAttribute": [],
                    "event_id": "8514",
                    "timestamp": "1512393594",
                    "deleted": false,
                    "object_relation": null,
                    "Galaxy": [],
                    "distribution": "5",
                    "object_id": "0",
                    "category": "Network activity",
                    "comment": "",
                    "id": "855602",
                    "uuid": "5a254b7a-fb6c-40bc-8b26-7ee20a2b115a",
                    "disable_correlation": false,
                    "to_ids": true,
                    "sharing_group_id": "0",
                    "value": "www.gtld-server.com",
                    "type": "domain",
                    "ShadowAttribute": [],
                    "event_id": "8514",
                    "timestamp": "1512393594",
                    "deleted": false,
                    "object_relation": null,
                    "Galaxy": [],
                    "distribution": "5",
                    "object_id": "0",
                    "category": "Network activity",
                    "comment": "",
                    "id": "855603",
                    "uuid": "5a254b7a-1790-4fea-8561-7ee20a2b115a",
                    "disable_correlation": false,
                    "to_ids": true,
                    "sharing_group_id": "0",
                    "value": "ipvhos.duckdns.org",
                    "type": "domain",
                    "ShadowAttribute": [],
                    "event_id": "8514",
                    "extends_uuid": "",
                    "publish_timestamp": "1512446171",
                    "Tag": [
                      {
                        "id": "2",
                        "user_id": "0",
                        "hide_tag": false,
                        "exportable": true,
                        "colour": "#ffffff",
                        "name": "tlp:white",
                        "analysis": "2",
                        "ShadowAttribute": [],
                        "distribution": "3",
                        "date": "2017-12-04",
                        "published": true,
                        "Org": {
                          "id": "1",
                          "uuid": "595591f6-b518-4844-8158-3db68266bc0e",
                          "name": "AuscERT",
                          "RelatedEvent": [
                            {
                              "timestamp": "1511860842",
                              "analysis": "2",
                              "distribution": "3",
                              "org_id": "1",
                              "orgc_id": "60",
                              "published": true,
                              "id": "8483",
                              "Org": {
                                "id": "1",
                                "uuid": "595591f6-b518-4844-8158-3db68266bc0e",
                                "name": "AuscERT",
                                "Orgc": {
                                  "id": "60",
                                  "uuid": "56a647a-63dc-4471-bce9-4acc25ed029",
                                  "name": "CERT-BUND",
                                  "uuid": "5a1d27de-1148-4c97-9d89-70cca02b115a",
                                  "date": "2017-11-28",
                                  "threat_level_id": "3",
                                  "info": "Malicious PDF Spam"
                                }
                              }
                            }
                          ]
                        }
                      }
                    ],
                    "threat_level_id": "3",
                    "info": "Lokibot C2"
                  }
                ]
              }
            ]
          }
        }
      ]
    }
  }
}
```

```
{
  "Event": {
    "timestamp": "1535010639",
    "Galaxy": [],
    "proposal_email_lock": false,
    "org_id": "1",
    "attribute_count": "12",
    "orgc_id": "324",
    "id": "23302",
    "Object": [],
    "Orgc": {
      "id": "324",
      "uuid": "58a4534c-33c8-4a70-b866-c8dc950d210f",
      "name": "CERT PKO BP",
      "Attribute": [
        {
          "timestamp": "1535007605",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "From address",
          "id": "2063854",
          "uuid": "5b7e5b75-7f24-4629-9d06-4035c0a81726",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "imports.falcos@gmail.com",
          "type": "email-src",
          "ShadowAttribute": [],
          "event_id": "23302",
          "timestamp": "1535007605",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "Subject",
          "id": "2063858",
          "uuid": "5b7e5b75-f558-47f5-ba66-4dc8c0a81726",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "ORDER n\u00b0050 5771308",
          "type": "email-subject",
          "ShadowAttribute": [],
          "event_id": "23302",
          "timestamp": "1535007632",
          "deleted": false,
          "object_relation": null,
          "Galaxy": [],
          "distribution": "5",
          "object_id": "0",
          "category": "Payload delivery",
          "comment": "",
          "id": "2063862",
          "uuid": "5b7e5b90-163c-4121-9189-4224c0a81726",
          "disable_correlation": false,
          "to_ids": false,
          "sharing_group_id": "0",
          "value": "Dear Sir,\r\n\r\nPlease find herewith attached our Purchase order.\r\n\r\n\r\nKindly acknowledge the receipt, send order confirmation and proceed for early delivery.\r\n\r\n\r\nRegards,\r\n\r\n\r\nBELLENTANI"
        }
      ]
    }
  }
}
```



## CAUDIT-ISAC MISP ACCESS: OWN INSTANCE

- › STAND UP YOUR OWN LOCAL MISP INSTANCE.
- › AUSCERT'S INFRA TEAM CAN HELP SET UP BY WAY OF AN ANSIBLE SCRIPT FOR DEPLOYING MISP (CONTACT US TO GET ACCESS TO THE PLAYBOOK)
- › SYNCHRONISE TO THE CAUDIT-ISAC MISP INSTANCE
  - › PULL (CONSUME) OR PUSH (PRODUCT) FROM OR TO THE CAUDIT-ISAC MISP
  - › APPLY PULL AND PUSH RULES TO ALLOW OR PREVENT CERTAIN EVENT TYPES BEING EXPORTED OR IMPORTED TO OR FROM THE REMOTE MISP INSTANCE



# CAUDIT-ISAC MISP USE CASES: MALWARE INDICATORS (1)

+ [Icons] Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields [Search]												
Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	
2018-09-21		Artifacts dropped	filename	%LOCALAPPDATA%\Microsoft\Windows\search\sd.exe	+	Add	dropped file indicative of Emotet activity	✓	2118		Yes	
2018-09-21		Payload delivery	url	http://athleticedgeamarillo.com/NSC	+	Add	emotet payload serving url	✓			Yes	
2018-09-21		Payload delivery	url	http://cuentocontigo.net/7ekN0IPi	+	Add	emotet payload serving url	✓			Yes	
2018-09-21		Payload delivery	url	http://stmmg.com.br/MFon	+	Add	emotet payload serving url				Yes	
2018-09-21		Payload delivery	url	http://kerasova-photo.ru/q5Lwh	+	Add	emotet payload serving url				Yes	
2018-09-21		Payload delivery	url	http://198.61.187.137/project/LN	+	Add	emotet payload serving url	✓			Yes	
2018-09-21		Payload delivery	domain	athleticedgeamarillo.com	+	Add	Emotet malware serving domain	✓			Yes	
2018-09-21		Payload delivery	domain	stmmg.com.br	+	Add	Emotet malware serving domain	✓			Yes	
2018-09-21		Payload delivery	domain	kerasova-photo.ru	+	Add	Emotet malware serving domain	✓			Yes	
2018-09-21		Payload delivery	domain	cuentocontigo.net	+	Add	Emotet malware serving domain	✓	1568 2258		Yes	
2018-09-21		Payload delivery	ip-src	198.61.187.137	+	Add	Emotet malware serving IP	✓			Yes	

SINGLE EMOTET MALWARE DOWNLOADING URL





# CAUDIT-ISAC MISP USE CASES: MALWARE INDICATORS (2)

2018-09-21	Name: file References: 0	Analysed malware sample: PAYROLL #257568T.doc			
2018-09-21	Payload delivery	md5:	2fe57e21ac0e190e020fa41bb814f6fc	+	Add
2018-09-21	Payload delivery	sha256:	e4e0dffae1c152ce0f009fde08eb246770cf71db41aabb34f22ff19a7f141f00	+	Add
2018-09-21	Payload delivery	filename:	PAYROLL #257568T.doc		
2018-09-21	Payload delivery	sha1:	387d03d877a4e64222adf147f080e7502503ec1c		
2018-09-21	Other	state:	Malicious		
Emotet malware is dropped as this executable file					
2018-09-21	Artifacts dropped	md5:	b999b3619c1c3dcf0023582e80a005ca	+	Add
2018-09-21	Artifacts dropped	sha256:	bb894a7b03081d81830aca9f36b4a4e59b737dea2be3ee08053ef6851503d9c9	+	Add
2018-09-21	Artifacts dropped	filename:	%PUBLIC%\653.exe	+	Add
2018-09-21	Other	size-in-bytes:	172032	+	Add
2018-09-21	Other	state:	Malicious	+	Add
C&C server					
2018-09-21	Network activity	dst-port:	80	+	Add
2018-09-21	Network activity	ip:	81.215.192.201	+	Add

FILE OBJECT FOR ANALYSED MALWARE SAMPLE

FILE OBJECT DEFINING EXECUTABLE EMOTET MALWARE IS DROPPED AS

IP-PORT OBJECT DEFINING C&C SERVER



# CAUDIT-ISAC MISP USE CASES: PHISHING INDICATORS (1)

## ATO PHISHING PAGE (1)

EMAIL OBJECT DESCRIBING PHISHING MAIL

2018-09-19	Name: http-request	References: 0	POST request with content of type x-www-form-urlencoded	Inherit	
2018-09-19	Network activity	content-type: other	application/x-www-form-urlencoded	No	Inherit (0/0/0)
2018-09-19	Network activity	host: hostname	www.acton.org	Yes	Inherit (0/0/0)
2018-09-19	Network activity	method: http-method	POST	No	Inherit (0/0/0)
2018-09-19	Network activity	uri: uri	/reg/get.php	Yes	Inherit (0/0/0)
2018-09-19	Network activity	uri: uri	http://www.acton.org/reg/get.php	Yes	Inherit (0/0/0)
2018-09-19	Network activity	user-agent: user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0	No	Inherit (0/0/0)
2018-09-19	Name: email	References: 0	ATO phishing mail	Inherit	
2018-09-19	Payload delivery	from-display-name: email-src-display-name	Australian Taxation Office	No	Inherit (0/0/0)
2018-09-19	Payload delivery	from: email-src	atopk506@r7.case927317.review	Yes	Inherit (0/0/0)
2018-09-19	Payload delivery	email-body: email-body	Australian Taxation Office (ATO) 8/09/2018  After the recent calculation of your fiscal activity, we have confirmed that you are eligible to receive a tax refund. To proceed, save the attached form and open it with any web browser.  Amanda Ariett Australian Taxation Office, Message ID: ATO60250 To unsubscribe from future notifications, reply to this email with Unsubscribe in the subject line.	Yes	Inherit (0/0/0)
2018-09-19	Payload delivery	subject: email-subject	ATO Refund Notification (1B1851)	Yes	Inherit (0/0/0)
2018-09-19	Payload delivery	message-id: email-message-id	01010165b4ce1751-d4b55a7d-b409-4a2f-823c-eb5925e5f42e-000000@us-west-2.amazonaws.com	No	Inherit (0/0/0)
2018-09-19	Name: http-request	References: 0	Captured form data is passed to	Inherit	



# CAUDIT-ISAC MISP USE CASES: PHISHING INDICATORS (2)

## ATO PHISHING PAGE (2)



Congratulations, your identity has been confirmed and your tax refund it is being processed.

Processing may take up to 28 days. In the meantime, if your financial details are changed, please resubmit this form.

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

Australian Government  
Australian Taxation Office

Australian Taxation Office - Tax Refund Form Secure

We ask you for some personal and financial information, so that we can identify you and process your tax refund application.  
The Taxation Administration Act 1953 authorises us to request your personal and financial information.

Country  
Australia

Email address  
john.doe@gmail.com

Personal password [?]

Full Name (Enter your full legal name)  
John Doe

Date of Birth  
04 April 1984

Place of Birth (e.g. Els, UK)  
red, AU

Street Address 1 (avoid PO Box)  
13 raid street

Street Address 2 (optional)

Suburb  
Jomma

State  
NT

Postcode

Phone number Type  
1424732742874 Mobile

Phone number Type  
Home

Card Type [?] Currency Available Funds [?]  
Debit Card AUD 3000 - 4000

Card Number [?]  
4151625694776090

Card Expiry Date CSC [?]  
06 2020

Name on Card (e.g. MR IAN J GAIL) [?]  
John Doe

Verified by Visa password [?]

Card Bank Name [?]  
Delphi Bank

Customer ID [?] Cardholder's Date of Birth [?]  
Month

Security Questions Answers  
Mother's Maiden Name [?] fggf  
Name of first pet [?] gfgf

By clicking the button below, I confirm that my information is correct.

Submit



# CAUDIT-ISAC MISP USE CASES: PHISHING INDICATORS (3)

## MYGOV PHISHING PAGE

Event Actions ▾ Galaxies ▾ Input Filters ▾ Global Actions ▾ Sync Actions ▾ Administration ▾ Audit ▾

MISP Nsoysa Log out

< previous next > view all

<



# CAUDIT-ISAC MISP USE CASES: INCIDENT INFORMATION STORAGE

- › USE MISP'S CAPABILITY TO STORE THREAT INDICATORS TO STORE INTERNAL INFORMATION
- › SEVERAL RISKS
  - › PARTITIONING FAILURE LEADING TO DISCLOSURE OF INFORMATION AND RELATE IMPACT TO TRUST, REPUTATION, ETC
  - › HANDLING ERROR LEADING ACCIDENTAL DISCLOSURE OF INTERNAL INCIDENT INFORMATION (E.G. INCORRECT DISTRIBUTION SETTINGS)
- › RECOMMENDED PRACTICE
  - › USE YOUR OWN LOCAL MISP INSTANCE TO STORE INCIDENT INFORMATION
  - › SET DISTRIBUTION AS "ORGANISATION ONLY"
  - › USE TAGS TO IDENTIFY EVENTS THAT SHOULD NOT BE PUSHED TO AN EXTERNAL MISP INSTANCE (E.G. TLP:AMBER OR CUSTOM TAG INCIDENT\_INFO) AND MARK THE INTERNAL INCIDENT EVENTS WITH THAT TAG.
  - › SYNCHRONISE "PULL" FROM CAUDIT-ISAC MISP TO YOUR MISP INSTANCE TO REPLICATE CAUDIT-ISAC EVENTS IN YOUR MISP INSTANCE



# CAUDIT-ISAC MISP USE CASES: DISCUSSION FORUM (1)

CAUDIT ISAC

Event Actions ▾

Galaxies ▾

Input Filters ▾

Global Actions ▾

Sync Actions ▾

Administration ▾

Audit ▾

## View Event

[View Correlation Graph](#)

[View Event History](#)

[Edit Event](#)

[Delete Event](#)

[Add Attribute](#)

[Add Object](#)

[Add Attachment](#)

[Populate from...](#)

[Enrich Event](#)

[Merge attributes from...](#)

[Delegate Publishing](#)

[Publish event to ZMQ](#)

[Contact Reporter](#)

[Download as...](#)

[List Events](#)

## 2018-07-24 Potential Security Issue - TimeWeave - Acqui...

Event ID	1234
Uuid	5b568dc8-73e0-4347-90e6-5fb98266bc08
Org	<a href="#">AusCERT</a>
Owner org	<a href="#">AusCERT</a>
Contributors	
Email	nsoysa@auscert.org.au
Tags	<a href="#">x</a> <a href="#">cicrl:incident-classification="information-leak"</a> <a href="#">x</a> <a href="#">+</a>
Date	2018-07-24
Threat Level	Undefined
Analysis	Initial
Distribution	This community only ⓘ
Info	2018-07-24 Potential Security Issue - TimeWeave - Acquisition and storage of student credentials and reconnaissance of university websites
Published	Yes
#Attributes	19
Last change	2018/07/27 02:34:03
Extends	
Extended by	
Sightings	0 (0) ↗
Activity	

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM





# CAUDIT-ISAC MISP USE CASES: DISCUSSION FORUM (2)

Discussion centre for issues (TimeWeave).

POTENTIALLY MALICIOUS IP FOR BLOCKING

<input type="checkbox"/>	2018-07-27	External analysis	link	<a href="https://www.hybrid-analysis.com/sample/eeaeab70f7c13bf09c00e02a0ed388c8216a33d24753980cc6bf907485052a89">https://www.hybrid-analysis.com/sample/eeaeab70f7c13bf09c00e02a0ed388c8216a33d24753980cc6bf907485052a89</a>	<input type="checkbox"/>	+	Add	Ref: Timeweave_au.com.timeweave.app.apk	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-07-24	Network activity	ip-src	40.126.225.234	<input type="checkbox"/>	+	Add	Scraping traffic sighted originating from this IP (www.timeweave.io)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-07-27	Network activity	url	https://timeweave-989.firebaseio.com	<input type="checkbox"/>	+	Add	URL referenced within the Timeweave APK. Google's Firebase app development platform for web, Android and iOS	<input checked="" type="checkbox"/>





AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

# CAUDIT-ISAC MISP USE CASES: DISCUSSION FORUM (3)

Discussion centre for issues (TimeWeave).

TEXT ATTRIBUTE DETAILING COURSE OF  
ACTION

2018-07-24

Other

comment

CAUDIT-ISAC is aware of a potential security weakness introduced by a sharing application, TimeWeave (<https://www.timeweave.io/>), that's available on both iOS and Android platforms.

+

Add

The application has the following features (based on site):

1. import  
Automatically import your class schedule.
2. connect  
Add your friends and get automatically placed in group chats with all the people in your classes.
3. compare  
Weave your schedule with friends so you can find a time to hang out.

Potential Security concerns:

1. Social engineering vector (in the form of cash incentives) to entice students to share their SSO credentials (Confidentiality impact)
2. Use of those credentials to map out a University's website (Confidentiality impact)
3. Potential unsafe storage of acquired student credentials in a central storage location, possibly a cloud-based resource (Confidentiality impact)
4. Disclosure of timetables leading physical safety issues (stalking) and other privacy violations

Action to be taken

-----



# CAUDIT-ISAC MISP USE CASES: DISCUSSION FORUM (4)

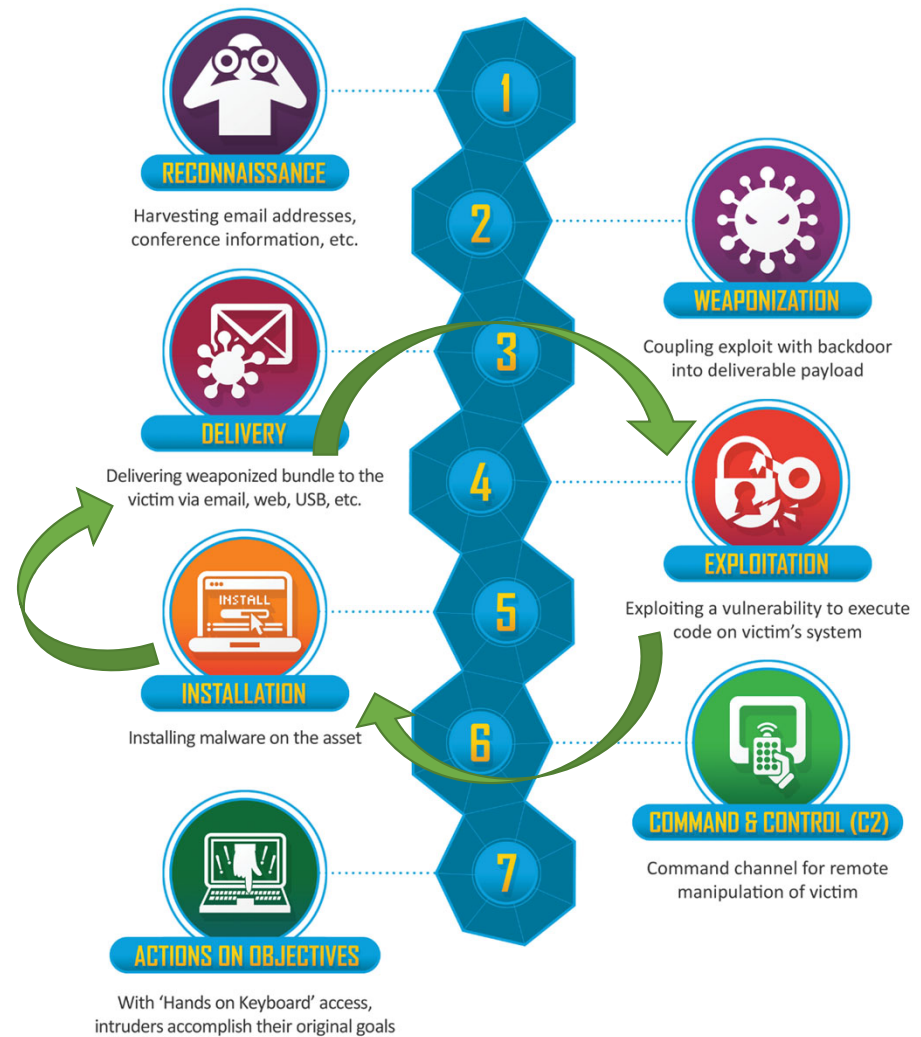
Discussion centre for issues (TimeWeave).

<input type="checkbox"/>	2018-07-25	External analysis	link	<a href="https://www.appbrain.com/dev/Galah+Enterprises/">https://www.appbrain.com/dev/Galah+Enterprises/</a>	<input type="checkbox"/>	+	Add	APPBrain page on Galah Enterprises	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-07-25	External analysis	link	<a href="https://play.google.com/store/apps/details?id=au.com.timeweave.app">https://play.google.com/store/apps/details?id=au.com.timeweave.app</a>	<input type="checkbox"/>	+	Add	TimeWeave installation page on Google Play	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-07-27	External analysis	comment	File Permissions	<input type="checkbox"/>	+	Add	File permissions for Timeweave APK	<input checked="" type="checkbox"/>

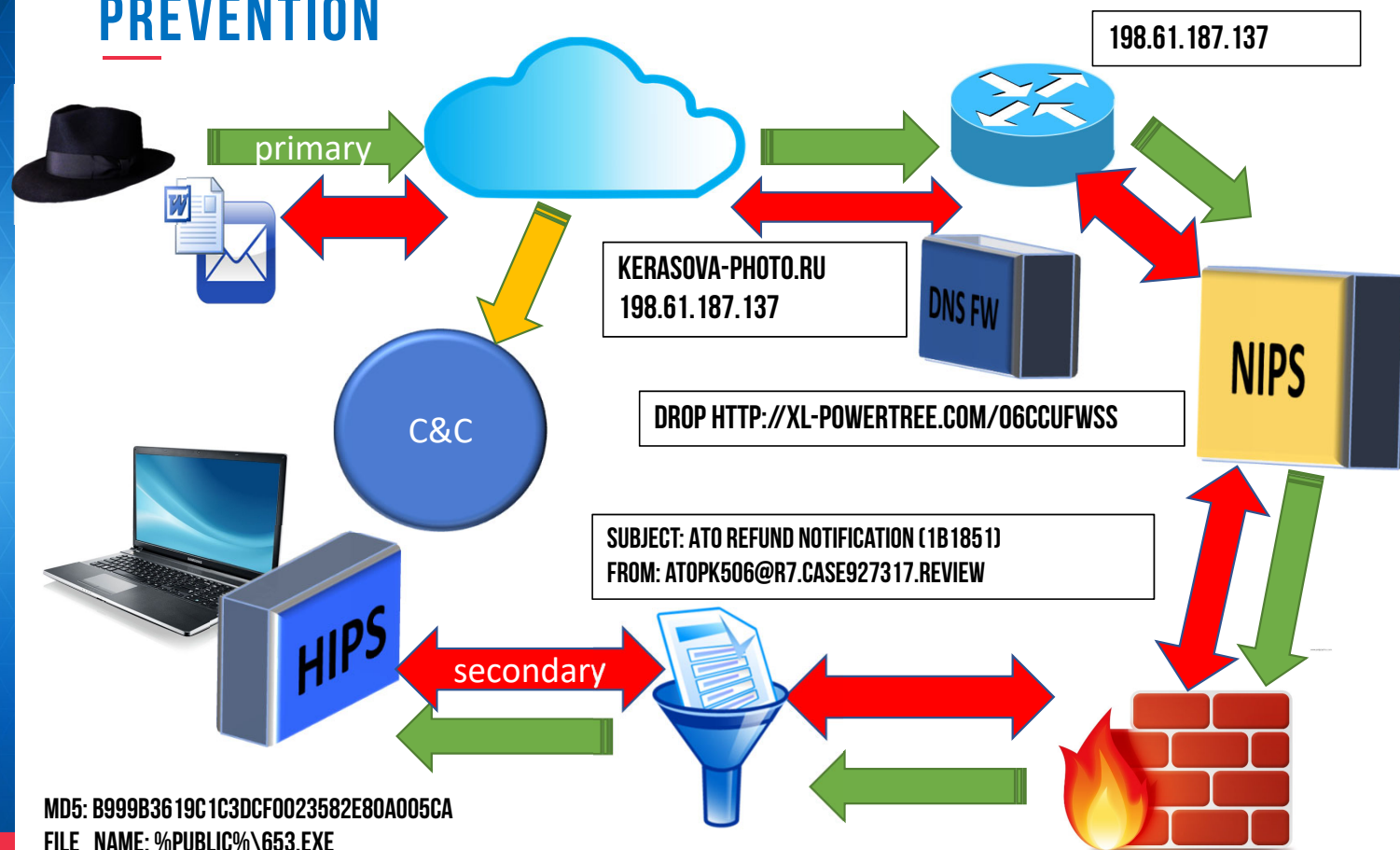
**APP BRAIN REPORT ON GALAH  
ENTERPRISES**

# CYBER KILL CHAIN

- MODEL DEVELOPED BY LOCKHEED MARTIN
- DEFINES THE VARIOUS STAGES INVOLVED IN THE CREATION, DISTRIBUTION AND USE OF MALWARE
- APPLICABLE TO MOST “MALICIOUS” ACTIVITIES INCLUDING PHISHING, SCAMS AS WELL



# CAUDIT-ISAC MISP USE CASES: PREVENTION



MD5: B999B3619C1C3DCF0023582E80A005CA

FILE\_NAME: %PUBLIC%\653.EXE

REGKEY | VALUE: HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\WRITE,

RUNDLL32.EXE ZIPFLDR.DLL,ROUTETHECALL %TEMP%\QWERTY2.EXE



# CAUDIT-ISAC MISP USE CASES: DETECTION – COMPUTRACE LOJACK AGENT DETECTION

2018-05-02

Payload installation

yara

+

Add

YARA signature to detect executable Lojack Agent (rpcnetp.exe)

```
rule ComputraceAgent
{
  meta:
    description = "Absolute Computrace Agent Executable"
    thread_level = 3
    in_the_wild = true
  strings:
    $a = {D1 E0 F5 8B 4D 0C 83 D1 00 8B EC FF 33 83 C3 04}
    $mz = {4d 5a}
    $b1 = {72 70 63 6E 65 74 70 2E 65 78 65 00 72 70 63 6E 65 74 70 00}
    $b2 = {54 61 67 49 64 00}
  condition:
    ($mz at 0 ) and ($a or ($b1 and $b2))
}
```

RULE MATCH CONDITION

MAGIC BYTE MATCH





**ALERT MODE RULE TO DETECT OUTBOUND  
DNS REQUEST FOR MALICIOUS DOMAIN  
PIZZA24.FR**

# CAUDIT-ISAC MISP USE CASES: DETECTION – TRICKBOT DETECTION RULE

2017-10-31	Payload installation	comment	<p>YARA signature "Office_OLE_DDEAUTO" classified file "--WRD0000.tmp" as "dde,exploit" based on indicators:</p> <p>"13204444454155544f20433a5c5c77696e646f77735c5c73797374656d33325c5c636d642e65786520222f6b206563686f20506f7765725368656c6c20284e65772d4f626a6563742053797374656d2e4e65742e576562436c69656e74292e446f776e6c6f616446696c652827687474703a2f2f70697a7a6132342e66722f6c6f757362616e642e706e67272c2725544d50255c5c696f79752e65786527293b53746172742d50726f63657373202725544d50255c5c696f79752e657865273e2025544d50255c5c6378762e62617420262025544d50255c5c6378762e6261742220"</p> <p>YARA signature "Office_OLE_DDEAUTO" classified file "--WRD0003.tmp" as "dde,exploit" based on indicators:</p> <p>"13204444454155544f20433a5c5c77696e646f77735c5c73797374656d33325c5c636d642e65786520222f6b206563686f20506f7765725368656c6c20284e65772d4f626a6563742053797374656d2e4e65742e576562436c69656e74292e446f776e6c6f616446696c652827687474703a2f2f70697a7a6132342e66722f6c6f757362616e642e706e67272c2725544d50255c5c696f79752e65786527293b53746172742d50726f63657373202725544d50255c5c696f79752e657865273e2025544d50255c5c6378762e62617420262025544d50255c5c6378762e6261742220"</p> <p>YARA signature "Office_OLE_DDEAUTO" classified file</p>	<p>+</p>	<p>Add</p>	<p>yara signature match for DDE exploit used by efax19482842345523_32531.doc</p>
------------	----------------------	---------	--	----------	------------	--

**DDE EXPLOIT DETECTION RULE, INDICATE  
ATTEMPT TO FETCH AND INSTALL  
TRICKBOT PAYLOAD**

```
alert tcp any any -> any 53 (msg: "MISP e1978 [] Domain: pizza24.fr"; content:"|01  
00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|07|pizza24|02|fr|00|";  
fast_pattern; nocase; flow:established; classtype:trojan-activity; sid:5694512;  
rev:1; priority:2; reference:url,https://misp.auscert.org.au/events/view/1978;)
```

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

2017-10-31	Payload installation	yara	<p>rule Office_OLE_DDEAUTO { strings: \$a = /x13's"DDEAUTO\b["\x14]+/ nocase condition: uint32be(0) == 0xD0CF11E0 and \$a }</p>	<p>+</p>	<p>Add</p>	<p>Office_OLE_DDEAUTO YARA Rule</p>
------------	----------------------	------	---	----------	------------	-------------------------------------





SIGHTED WEBLOGIC RCE EXPLOIT  
DELIVERING HOST IP.

EXPORTED AND GREPPED AGAINST  
TRAFFIC LOGS

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

## CAUDIT-ISAC MISP USE CASES: FORENSICS (1): CRYPTOJACKING CASE

<input type="checkbox"/>	2018-01-16	Network activity	url	http://165.227.215.25/xmrig-y	+	Add	IP address 165.227.215.25 was both the source of the attacks and the repository of cryptocurrencies miner's binaries.	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-16	Network activity	url	http://165.227.215.25/5555	+	Add	IP address 165.227.215.25 was both the source of the attacks and the repository of cryptocurrencies miner's binaries.	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-05	Network activity	url	http://pastebin.com/raw/yDnzKz72 ⚠	+	Add	Known C&C for python-based crypto miner	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-11	Network activity	ip-dst port	67.21.81.179:8220	+	Add	On port 8220	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-16	Network activity	ip-dst	165.227.215.25	+	Add	IP address 165.227.215.25 was both the source of the attacks and the repository of cryptocurrencies miner's binaries.	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-16	Network activity	url	http://165.227.215.25/	+	Add	IP address 165.227.215.25 was both the source of the attacks and the repository of cryptocurrencies miner's binaries.	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-05	Network activity	ip-dst	148.251.133.246	+	Add	Mining pool (HQ) IP	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-16	Network activity	url	http://165.227.215.25/xmrig-y%20\$	+	Add	IP address 165.227.215.25 was both the source of the attacks and the repository of cryptocurrencies miner's binaries.	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-11	Network activity	ip-dst	35.194.156.203	+	Add	Seen delivering exploit and post-exploit	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-11	Network activity	ip-dst port	58.218.198.162:45987	+	Add	Inbound SSH to compromised host	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-05	Network activity	url	http://pastebin.com/raw/rWjyEGDq ⚠	+	Add	Known C&C for python-based crypto miner	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-05	Network activity	domain	letoscribe.ru	+	Add	Known Monero Miner HQ domain	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-05	Network activity	hostname	pool.supportbtxmr.com	+	Add	Known mining pool host	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018-01-11	Network activity	pattern-in-traffic	199.188.104.74	+	Add	Unclassified IP	<input checked="" type="checkbox"/>



INBOUND HTTP TRAFFIC LOG MATCH ON  
MALICIOUS ATTRIBUTE

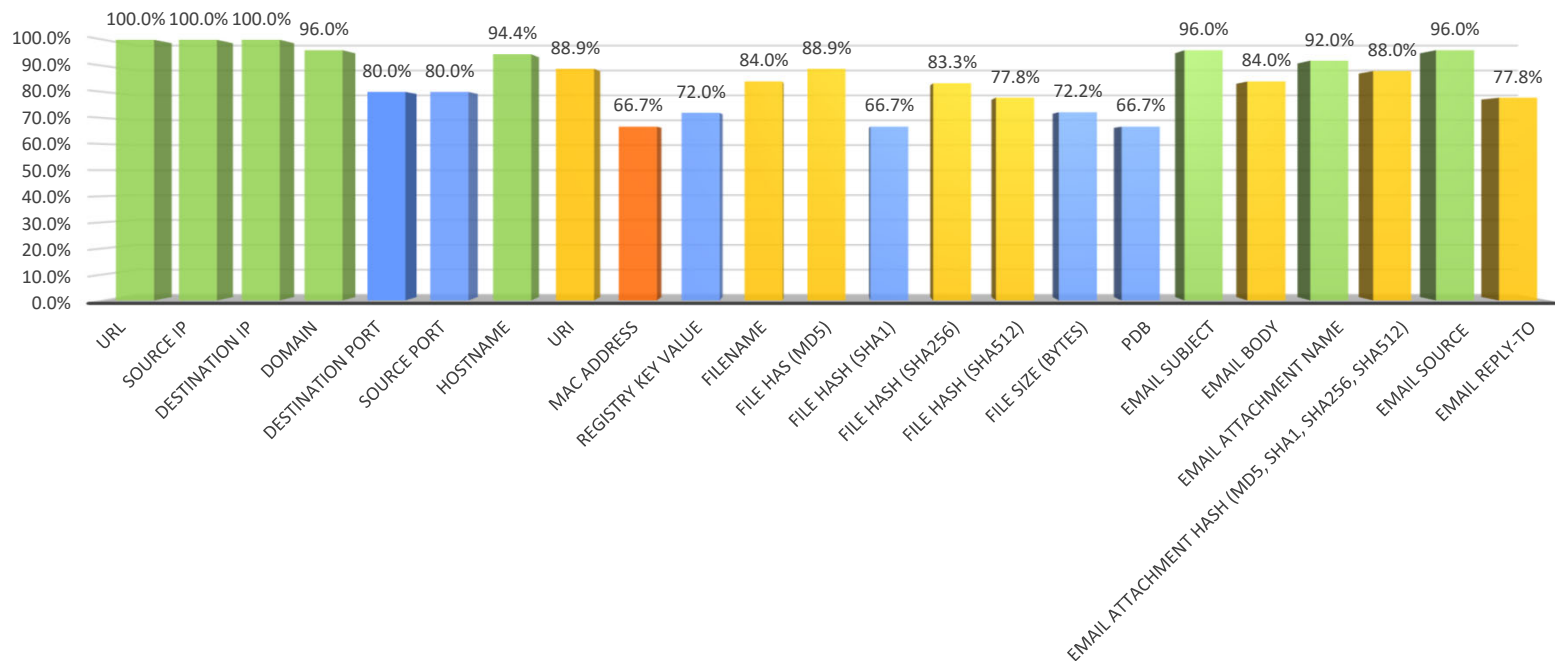
## CAUDIT-ISAC MISP USE CASES: FORENSICS (2)

```
2017-12-31_00.00-ingress.log.gz:2017-12-30 05:30:08 [REDACTED] - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1429 607 0 HTTP/1.1  
Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 - http://www.baidu.com  
2017-12-31_00.00-ingress.log.gz:2017-12-30 12:37:36 72.11.140.178 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1366 607 0 HTTP/1.1  
Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 - http://www.baidu.com  
2017-12-31_00.00-ingress.log.gz:2017-12-30 12:38:28 35.194.156.203 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1055 607 0 HTTP/1.1 python-requests/2.18.4 --  
2017-12-31_00.00-ingress.log.gz:2017-12-30 12:47:02 72.11.140.178 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1429 607 0 HTTP/1.1  
Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 - http://www.baidu.com  
2017-12-31_00.00-ingress.log.gz:2017-12-30 12:53:15 35.194.156.203 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1055 607 0 HTTP/1.1 python-requests/2.18.4 --  
2017-12-31_00.00-ingress.log.gz:2017-12-30 18:37:06 72.11.140.178 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1366 607 0 HTTP/1.1  
Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 - http://www.baidu.com  
2017-12-31_00.00-ingress.log.gz:2017-12-30 18:46:37 72.11.140.178 - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1429 607 0 HTTP/1.1  
Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 - http://www.baidu.com  
2017-12-31_00.00-ingress.log.gz:2017-12-30 23:42:44 [REDACTED] - HTTP [REDACTED] 443 POST /wls-  
wsat/CoordinatorPortType - 500 1366 607 0 HTTP/1.1
```



# SOME STATS:

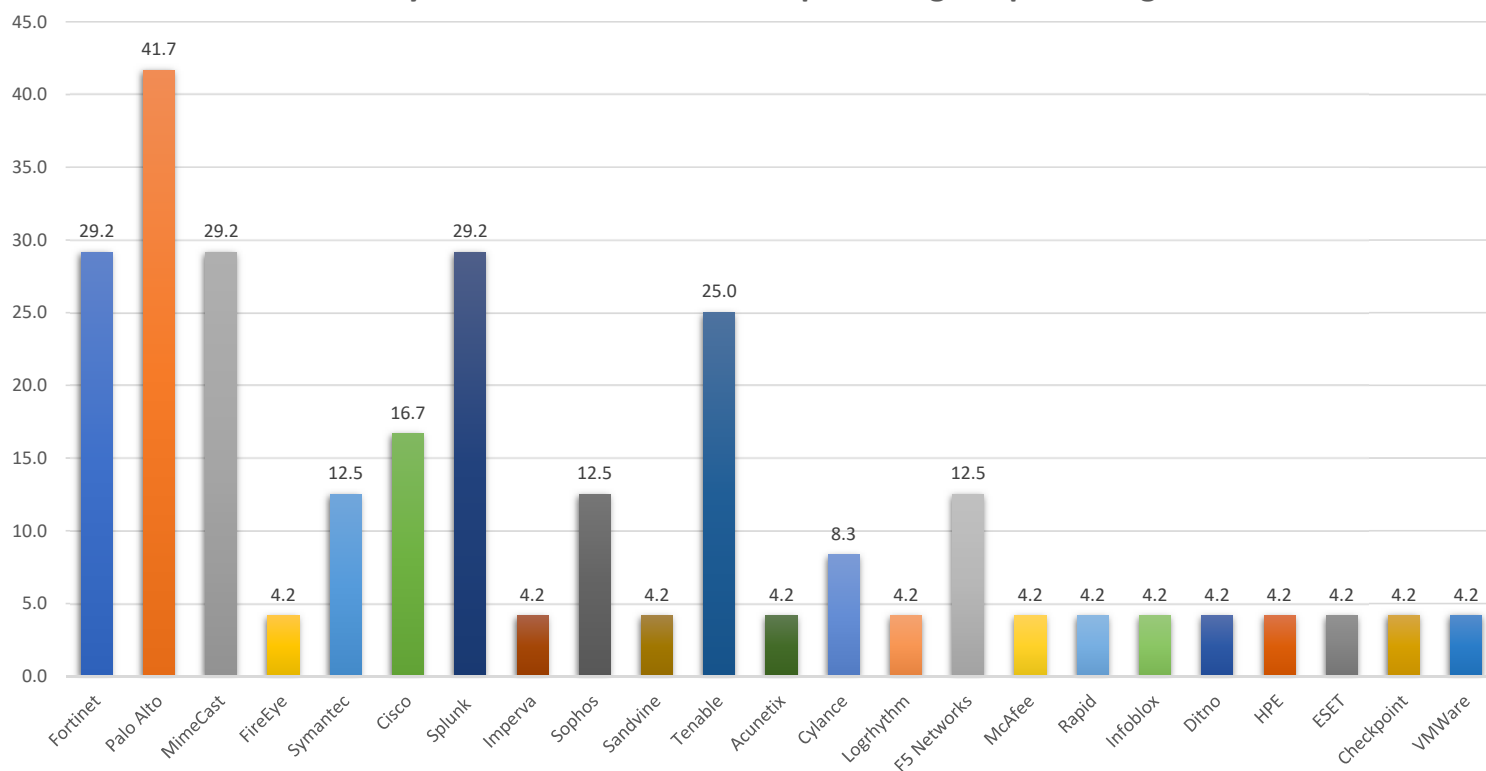
## THREAT INDICATOR USAGE BY UNIVERSITIES





## SOME STATS: SECURITY TOOLS USED

Security vendor brands used as a percentage of polled organisations



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM





# ROADMAP



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM



■ **THANK YOU!**

AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM





# INDICATOR-CONTROL MATRIX

LOCATION	SECURITY CONTROL	MISP CATEGORY	MISP INDICATOR TYPE				
NETWORK	NIDS / NIPS	Network activity	ip-dst	port	hostname	url	ip-src
		Payload delivery	ip-src	ip-dst	url		
	DSN FIREWALL	Network activity	domain				
		Payload delivery					
	EMAIL SECURITY GATEWAY	Payload delivery	email-src	email-subject	email-attachment		
HOST	HIDS	Artefacts dropped	sha256	md5	sha512	filename	
		Payload installation	sha256	md5	sha512	filename	
	YARA	Artefacts dropped	yara				
		Payload installation	yara				
	Registry Monitors	Persistence mechanism	regkey value				
		Artefacts dropped	regkey value				



AUSTRALIA'S PIONEER  
CYBER EMERGENCY RESPONSE TEAM

RECONNAISSANCE

WEAPONIZATION

DELIVERY

Exploitation

Installation

Command  
and Control

Actions on  
Objectives

## RED TEAM

Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).

Transmission of the weapon to the targeted environment.

After the weapon is delivered to victim host, exploitation triggers the intruders' code.

Installation of a remote access tool or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. Once the C2 channel establishes, intruders have "hands on the keyboard" access.

Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives [i.e., data exfiltration].

## BLUE TEAM

### PREVENTATIVE

- User education, News
- Organisational security policy
- System hardening (close unnecessary services)
- Network security controls (Firewall, ACLs)

- AusCERT Security bulletins with alerts indicating active exploits
- Exploit publication sites (exploits-db)
- Exploit kit sales sites

- NIPS/HIPS
- DNS Firewalls (RPZ)
- Firewalls (Network and host)
- Router ACLs
- Mail filters
- URL blacklists (web proxy)

- User Account management
- Penetration testing
- System hardening (e.g. CIS Benchmarks)

- User Account Management
- System hardening

- NIPS
- Firewall
- DNS Firewall (RPZ)
- Web proxy (URL blacklists)

- NIPS (Destination IP, Hostname, domain for dropzone)
- Firewall
- DNS Firewall (RPZ)
- Web proxy (URL blacklists)
- Dark web (data sales)

### DETECTIVE

- Inbound scan traffic
- Public dumps of harvested credentials and other PII
- External Vulnerability Assessment (Nmap, Web vulnerability scans)

- MSINs indicating exploitable vulnerabilities in assets

- NIDS (Snort, Suricata, Bro)
- HIDS (OSSEC)
- SIEM

- HIDS (OSSEC)
- YARA Signatures

- Registry monitors (Registry key additions/modifications)
- File system integrity checks (Dropped files)

- NIDS (Destination IP, Hostname, Domain for remote servers)
- SIEMs

- NIDS (Destination IP, Hostname, Domain for remote servers)
- SIEMs
- BTC Wallets (track payments)

### CORRECTIVE

- Feedback mechanism to provide input on publicly exposed sensitive information  
(e.g. banners on web servers revealing server version, organisational structure and contact details)

- Patching/Upgrading software

- Antivirus (Quarantine)
- Mail filters

- Antivirus
- Network/host isolation
- Patching
- Apply workarounds (mitigations)

- Workarounds
- Remote backups

- Remote backups

- Decryptors (ransomware)
- Remote backups