



RNEP-GW

MÓDULO MISP



MISP - HISTÓRIA

Projeto desenvolvido e mantido pela equipa CIRCL (Computer Incident Response Center Luxembourg)

Open Source Software:
<https://github.com/MISP/MISP>



O QUE É O MISP?

Plataforma que permite a partilha, armazenamento e corelacionamento de informação sobre indicadores de diversos tipos:

- Inteligência contra ameaças
- Informações sobre fraudes financeiras
- Informações sobre vulnerabilidades
- Informações sobre contra terrorismo
- Informações sobre malware



PARA QUEM É INDICADO? PARA QUE FINS?



ESTRUTURA E TIPO DE DADOS NO MISP

Eventos e classificação (Malware, Phishing, Denial of Service, XSS, etc)

Atributos diversos (Network, Payload Delivery, External Analysis, etc)

Published	Org	Id	Clusters	Tags	#Attr.	#Corr.	Date ↑	Info	Distribution	Actions
✓	camichel.com	11238		tlp:green automatic-collection MalSpam Formbook	32	58	2019-03-28	Formbook MalSpam Run (2019-03-28) "Invoice due for payment."	All	
✓	camichel.com	11239		tlp:green automatic-collection MalSpam Log Password Stealer (PWS)	23	57	2019-03-28	LogBot MalSpam Run (2019-03-28) "RFQ: THI - PO 4854 EBOP"	All	
✓	camichel.com	11240		tlp:green automatic-collection MalSpam Nanocore RAT	37	57	2019-03-28	Nanocore RAT MalSpam Run (2019-03-28) "PRODUCT LIST"	All	
✓	GTO-CERT	11241		MalSpam Phishing tlp:white	3		2019-03-28	Phishing Citibank - AVISO DE PAGO - CITIBANK N.A.	All	
✓	GTO-CERT	11242		MalSpam Phishing tlp:white	5		2019-03-28	Phishing - New Management Message	All	
✓	TRUESEC.be	11244		tlp:white phishing	6		2019-03-28	NatWest Bank Phishing Attempt	All	
✓		11245		LockerGoga tlp:white	78	3	2019-03-28	CERTFR-2019-ACT-005 (LockerGoga)	All	

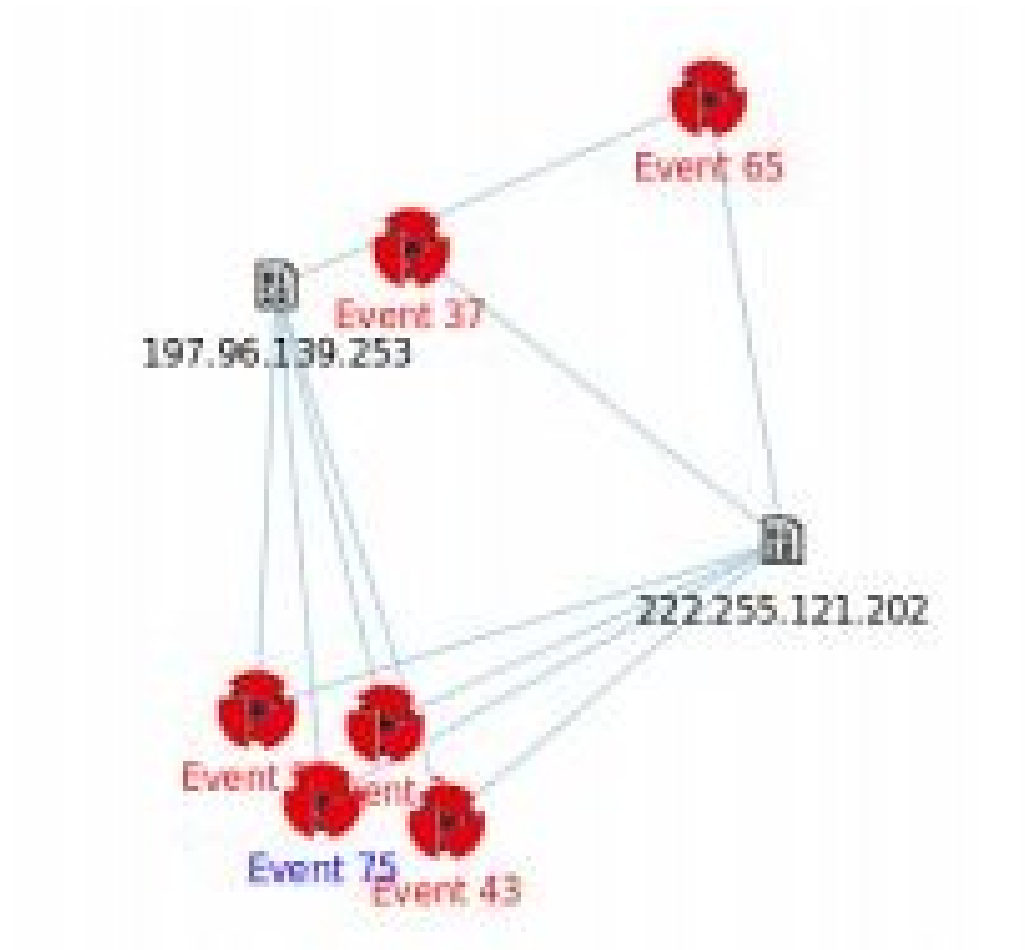
Phishing campaign bank institution Montepio net24

Event ID	11129
Uuid	5c87c909-b9a8-48e2-a5d3-0250d5d09a03
Org	RCTS CERT
Contributors	
Email	viktor.sousa@fccn.pt
Tags	Phishing x tlp:white x +
Date	2019-03-12
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	Phishing campaign bank institution Montepio net24
Published	Yes (2019-03-25 23:28:32)
#Attributes	4
Last change	2019-03-25 23:28:23
Extends	
Extended by	
Sightings	0 (0)
Activity	

[Pivots](#)
[Galaxy](#)
[+ Event graph](#)
[+ Correlation graph](#)
[+ ATT&CK matrix](#)
[- Attributes](#)
[- Discussion](#)

11129: Phishi...

CORELACIONAMENTO DE EVENTOS



COMO PODE SER ACEDIDA A INFORMAÇÃO?

Acesso direto por uma interface web

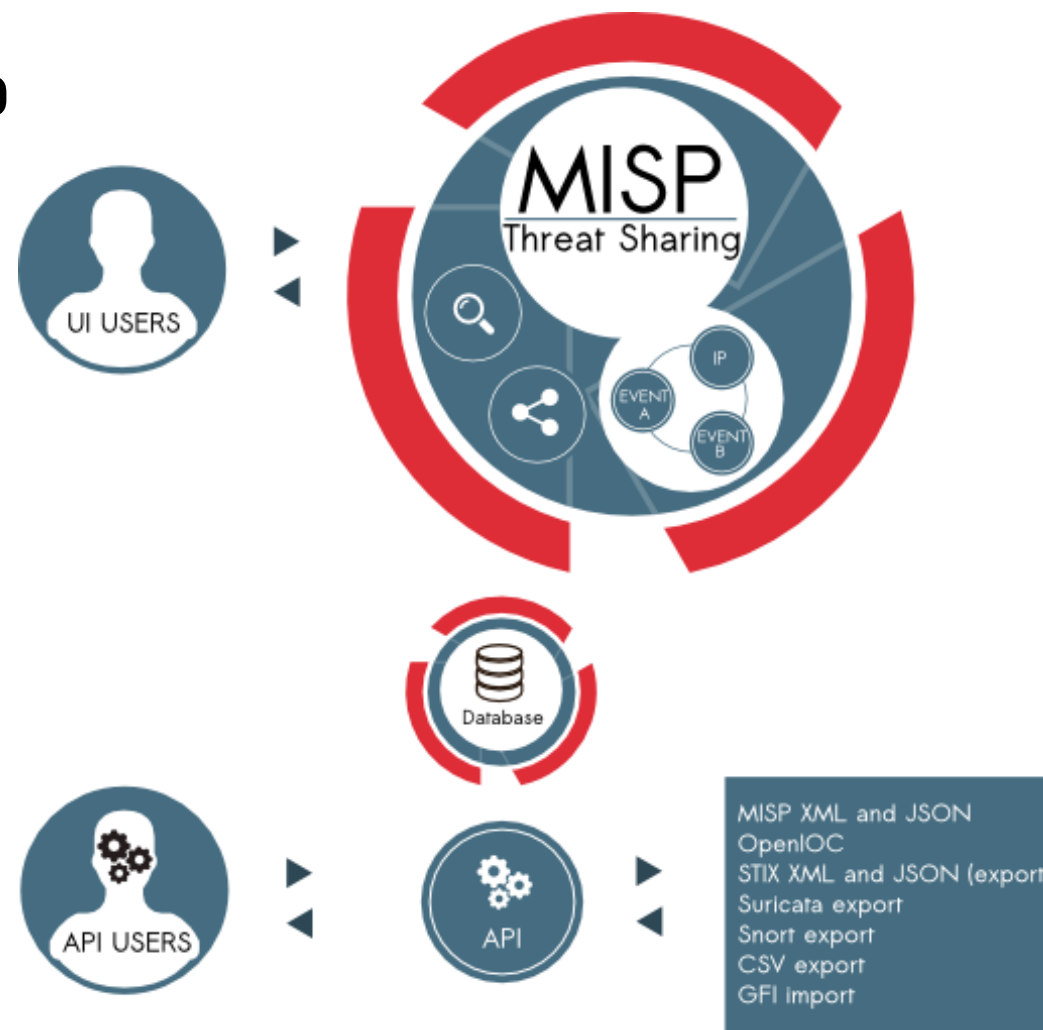
Acesso através de API



Login

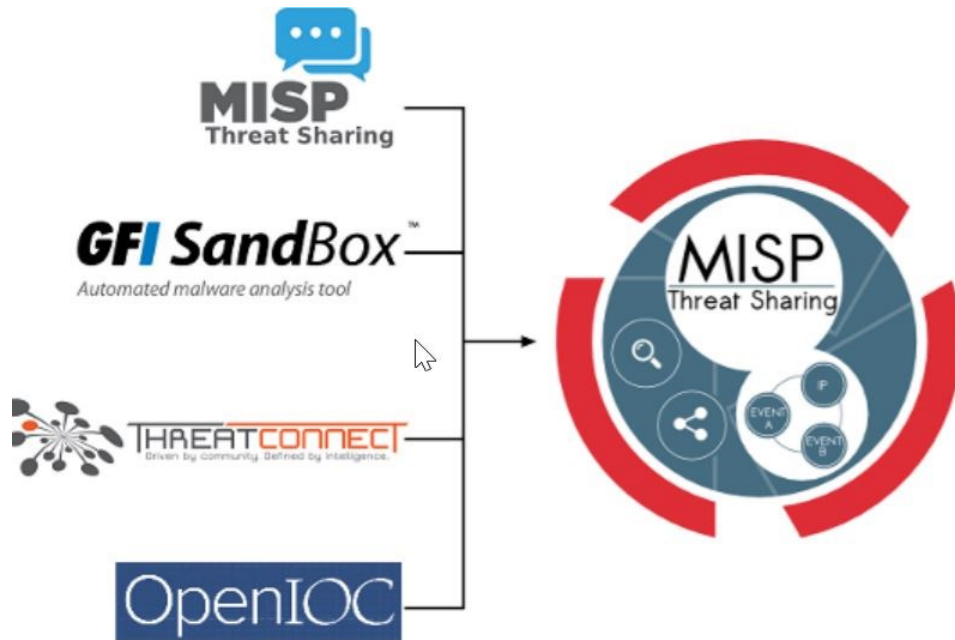
Email

Password

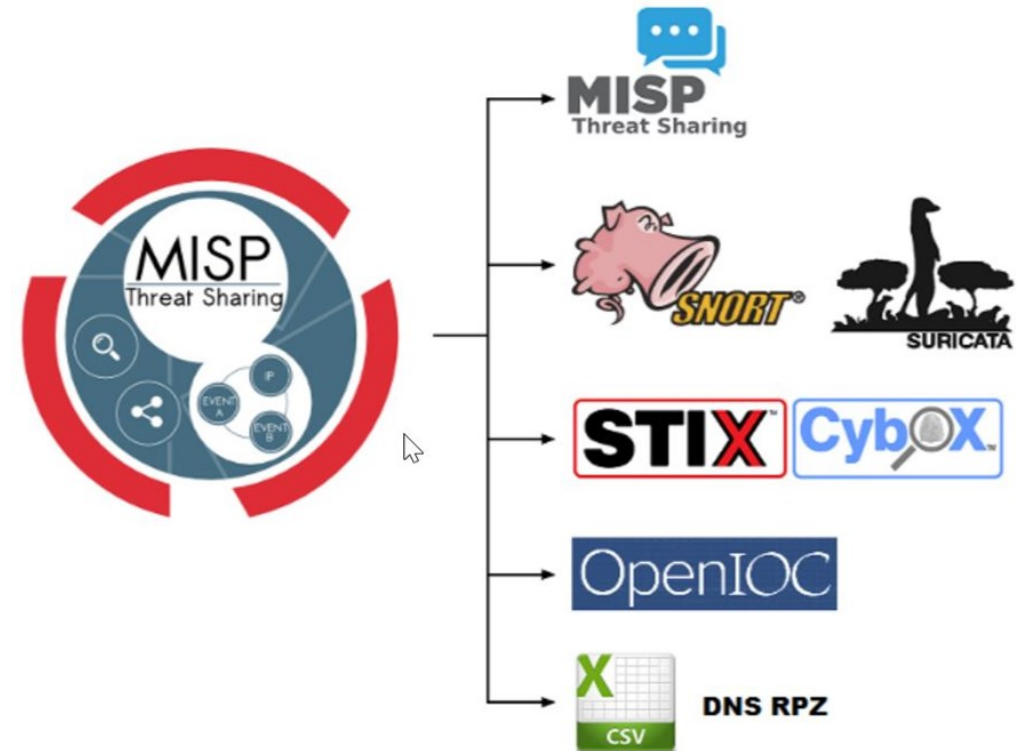


IMPORTAÇÃO E EXPORTAÇÃO DE DADOS

Importação de dados para o MISP



Exportação de dados



SEGURANÇA DA INFORMAÇÃO

Partilha é feita apenas entre membros confiáveis

Exige certificado válido

Uso de PGP (Pretty Good Privacy)

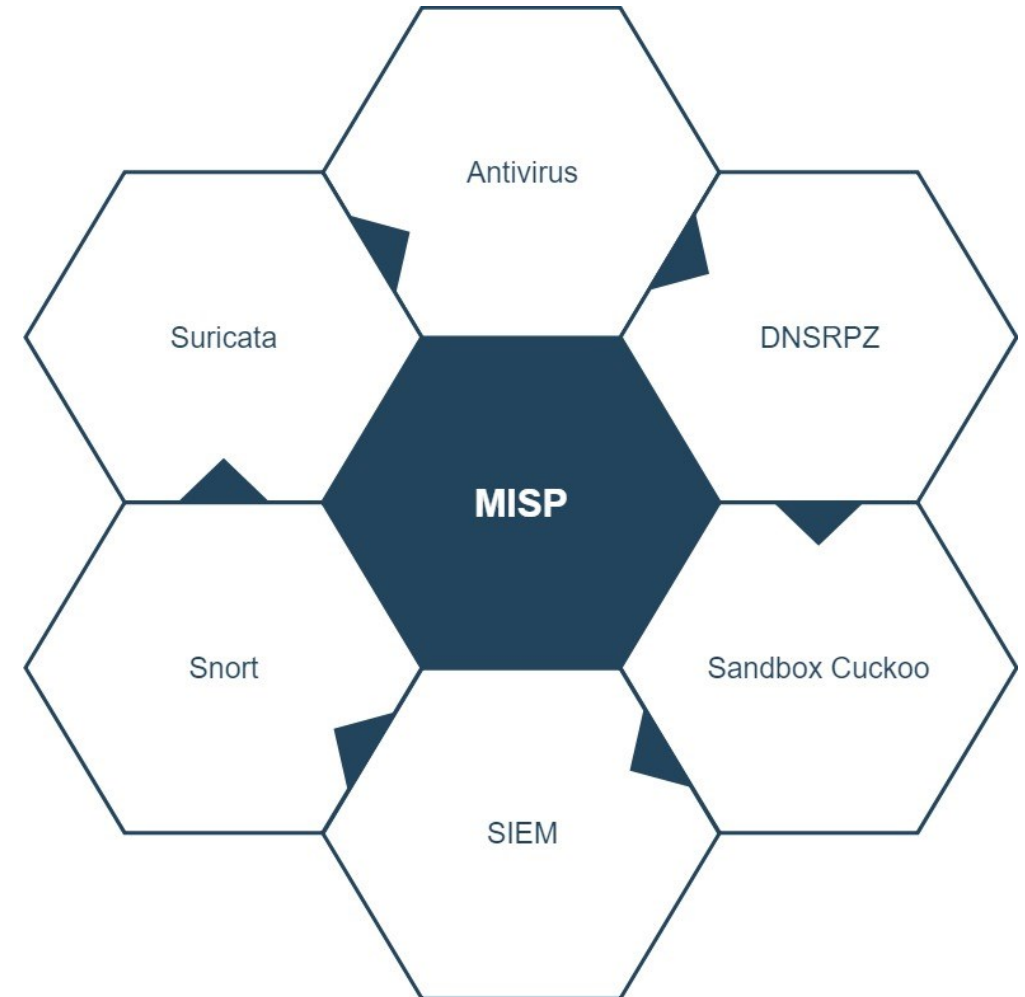


PRINCIPAIS OBJECTIVOS DO MISP

Armazenar IOC's de forma estruturada

Ajudar na investigação de casos concretos

Aumentar a eficiência dos sistemas de segurança



INSTÂNCIAS MISP EXISTENTES



PROJECTO MISP

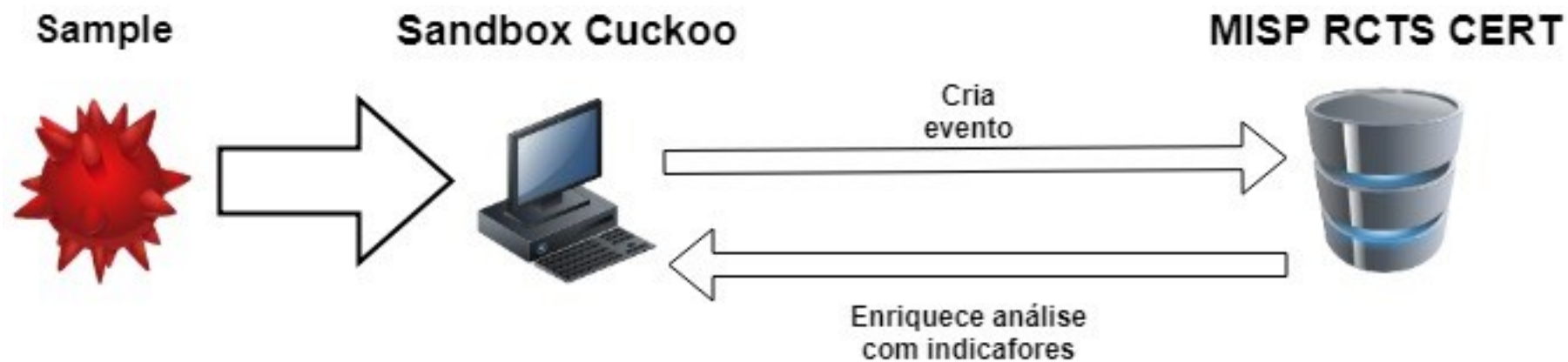
Instalação e configuração da instância MISP

Sincronização com outras instâncias MISP

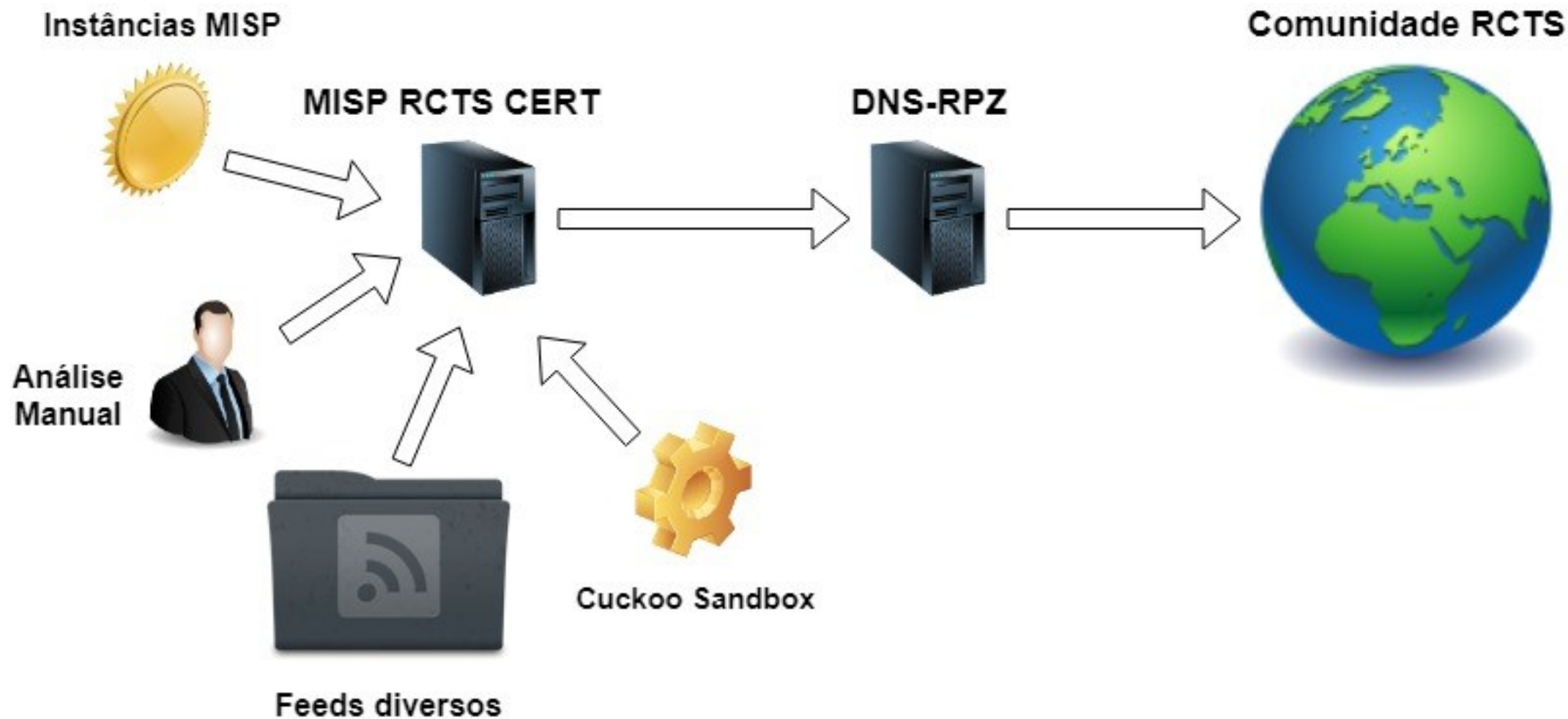
- GALP
- CMVM

Interligação com sistemas existentes

SANDBOX CUCKOO



MISP E DNS-RPZ



EVENTOS

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

Published	Org	Id	Clusters	Tags	#Attr.	#Corr.	Date ↑	Info	Distribution	Actions
✓	camichel.com	11238		tip:green automatic-collection Malspam Formbook	32	58	2019-03-28	Formbook Malspam Run (2019-03-28) "Invoice due for payment "	All	
✓	camichel.com	11239		tip:green automatic-collection Malspam Loki Password Stealer (PWS)	23	57	2019-03-28	LokiBot Malspam Run (2019-03-28) "RFQ: THI - PO 4854 EBOP"	All	
✓	camichel.com	11240		tip:green automatic-collection Malspam Nanocore RAT	37	57	2019-03-28	Nanocore RAT Malspam Run (2019-03-28) "PRODUCT LIST"	All	
✓	GTO-CERT	11241		MalSpam Phishing tip:white	3		2019-03-28	Phishing Citibank - AVISO DE PAGO - CITIBANK N.A.,	All	
✓	GTO-CERT	11242		MalSpam Phishing tip:white	5		2019-03-28	Phishing - New Management Message	All	
✓	TRUESEC.be	11244		tip:white phishing	6		2019-03-28	NatWest Bank Phishing Attempt	All	
✓		11245		LockerGoga tfn:white	78	3	2019-03-28	CERTFR-2019-ACT-005 (LockerGoga)	All	



EVENTO E CLASSIFICAÇÃO

Event ID	11129
Uuid	5c87c909-b9a8-48e2-a5d3-0250d5d09a03
Org	RCTS CERT
Contributors	
Email	vitor.sousa@fccn.pt
Tags	Phishing x tlp:white x +
Date	2019-03-12
Threat Level	Undefined
Analysis	Completed
Distribution	All communities ⓘ

Published	Yes (2019-03-25 23:28:32)
#Attributes	4
Last change	2019-03-25 23:28:23
Extends	
Extended by	
Sightings	0 (0) 🔧
Activity	

- Pivots - Galaxy + Event graph + Correlation graph + ATT&CK matrix - Attributes - Discussion

✕ 11129: Phishi...



ATRIBUTOS ASSOCIADOS AO EVENTO

+		📄 ⓘ 🔁		Filters: All File Network Financial Proposal Correlation Warnings Deleted Context Related Tags 🔍												
☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐	2019-03-12		Network activity	domain		+	Add	Domain contacted after the redirection from first Domain	☒			☐	Inherit	👍👎🔑 (0/0/0)		🔗🗑
☐	2019-03-12		Network activity	domain		+	Add	First Domain contacted	☒			☐	Inherit	👍👎🔑 (0/0/0)		🔗🗑
☐	2019-03-12		Targeting data	target-user	Clients from the bank "Montepio24"	+	Add		☒	11052		☐	Inherit	👍👎🔑 (0/0/0)		🔗🗑
☐	2019-03-12		Payload delivery	email-body	Estimado(a) Sr.(a) , Informamos que seu Utilizador foi bloqueado temporariamente porque seu Cartão Matriz ainda não foi activado. Para continuar utilizando os servicos Net24 Particulares/Empresas, por favor efectue sua activação agora. Aceda em seu utilizador normalmente em "Activar Cartão Matriz". ⊗ Activar Cartão Matriz Caso não efectue o processo de activação, teu Cartão Matriz sera cancelado permanentemente, e será cobrado uma taxa de 635,50 EUR para nova emissão.	+	Add		☒			☐	Inherit	👍👎🔑 (0/0/0)		🔗🗑



IDEIAS CHAVE



MISP é uma ferramenta que permite a gestão de indicadores (IoC)



A ferramenta é interoperável com outras ferramentas



É possível interligar MISPs para partilhar informação



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc