MISP RCTS CERT

Malware Information Sharing Platform

Vitor Sousa

Patrocinadores **Platina**

Patrocinadores **Ouro**

Patrocinadores **Prata**

Apoios

Organização

Agenda

- Projeto MISP
- Projeto instância MISP RCTS CERT

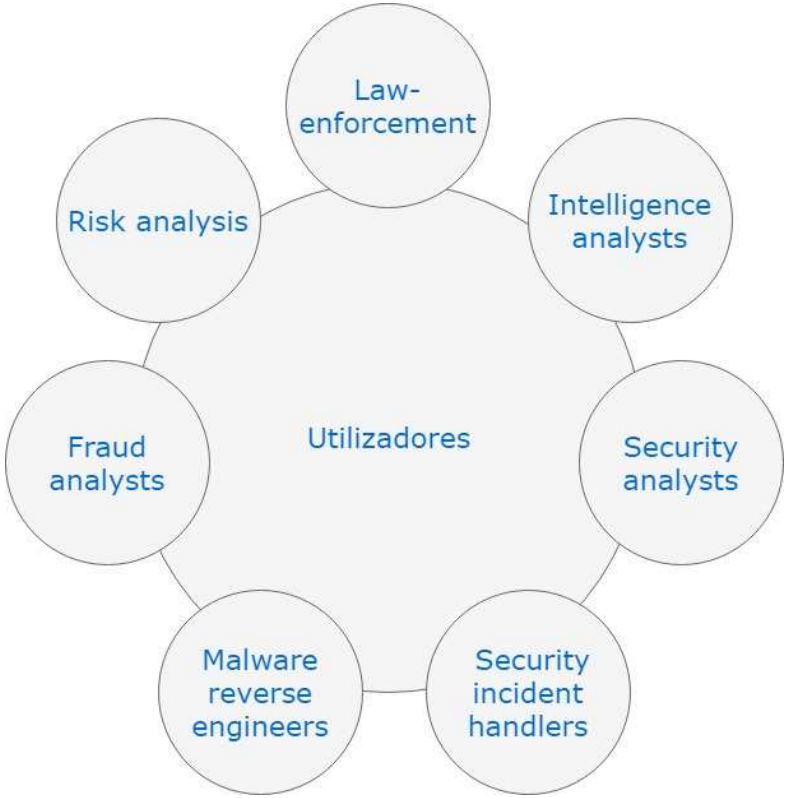
MISP - História

- 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?

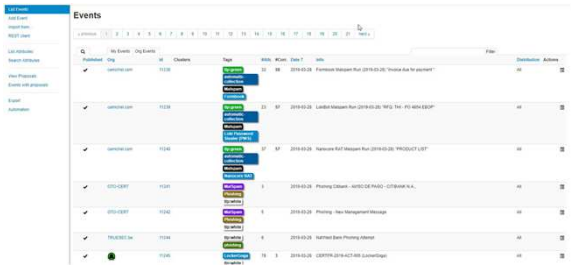
- Plataforma que permite a partilha, armazenamento e correlacionamento de informação sobre indicadores de diversos tipos:
  - Inteligência contra ameaças
  - Informações sobre fraudes financeiras
  - Informações sobre vulnerabilidades
  - Informações sobre contra terrorismo
  - Informações sobre malware

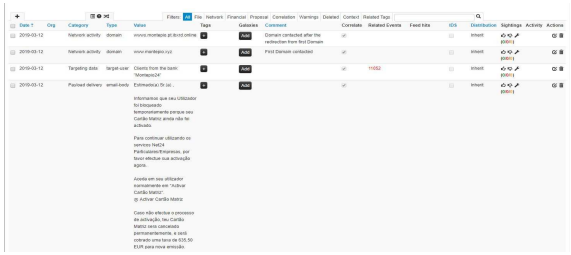
Para quem é indicado?Para que fins?



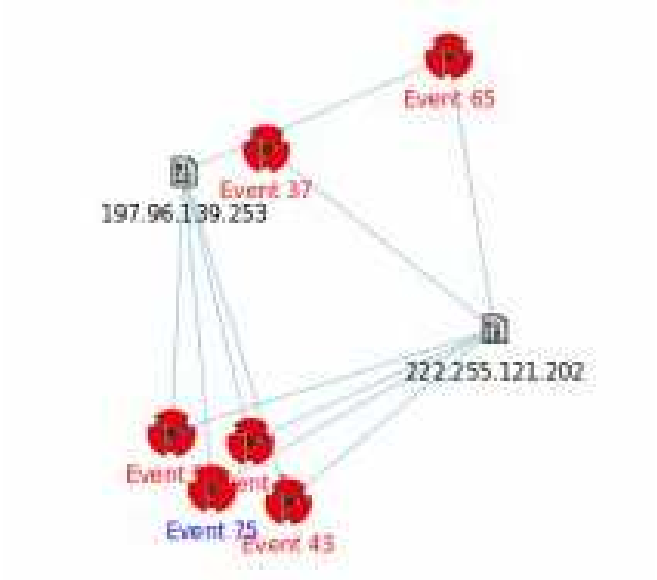
Estrutura e tipo de dados no MISP

- Eventos e classificação (Malware, Phishing, Denial of Service, XSS, etc)
- Atributos diversos (Network, Payload Delivery, External Analysis, etc)



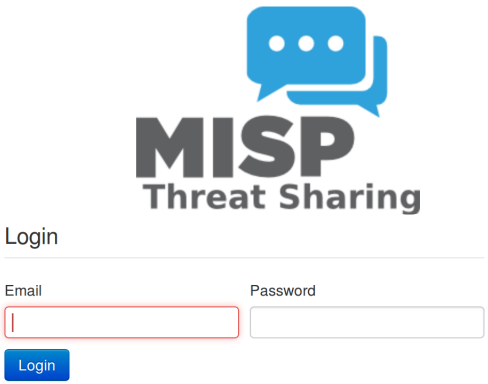


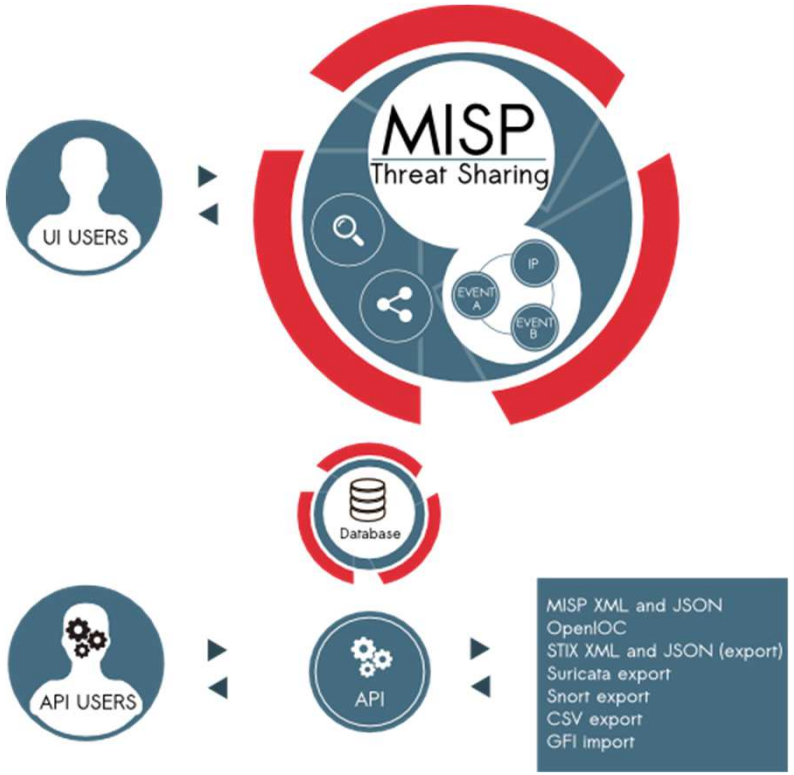
Corelacionamento de eventos



Como pode ser acedida a informação?

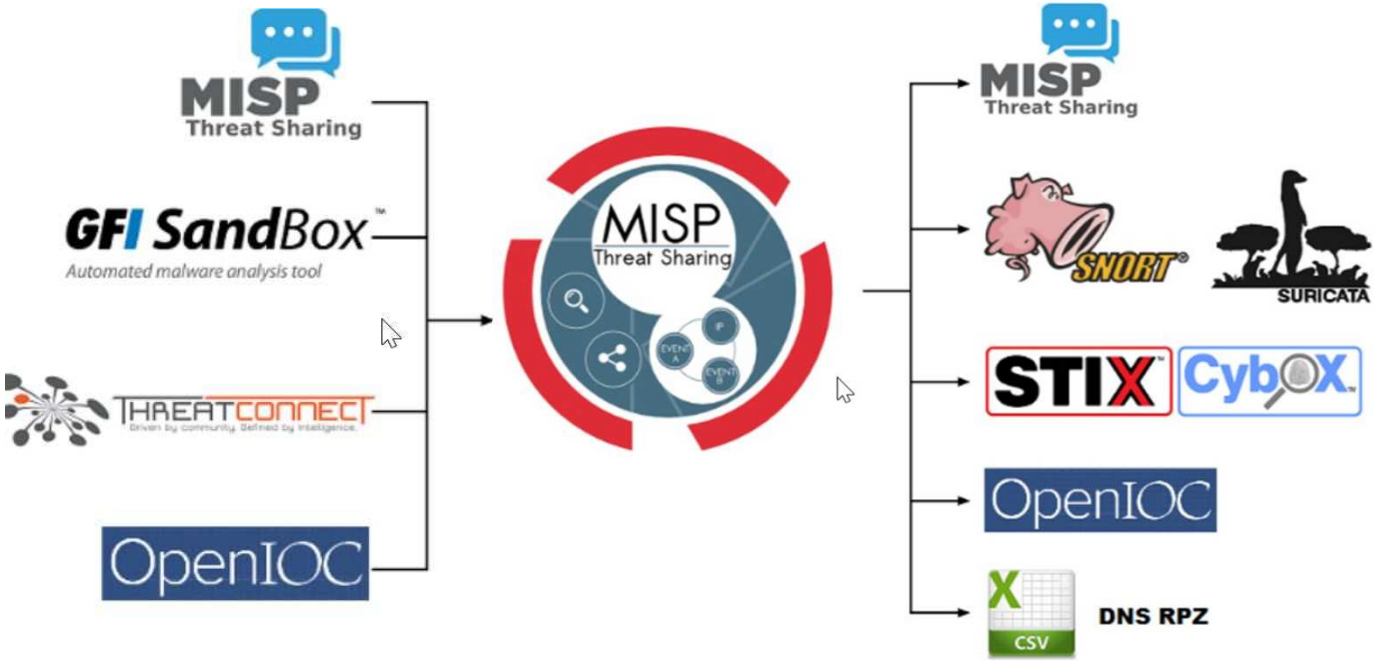
- Acesso direto por uma interface web
- Acesso através de API





Importação e Exportação de dados

- Importação de dados para o MISP
- Exportação de dados

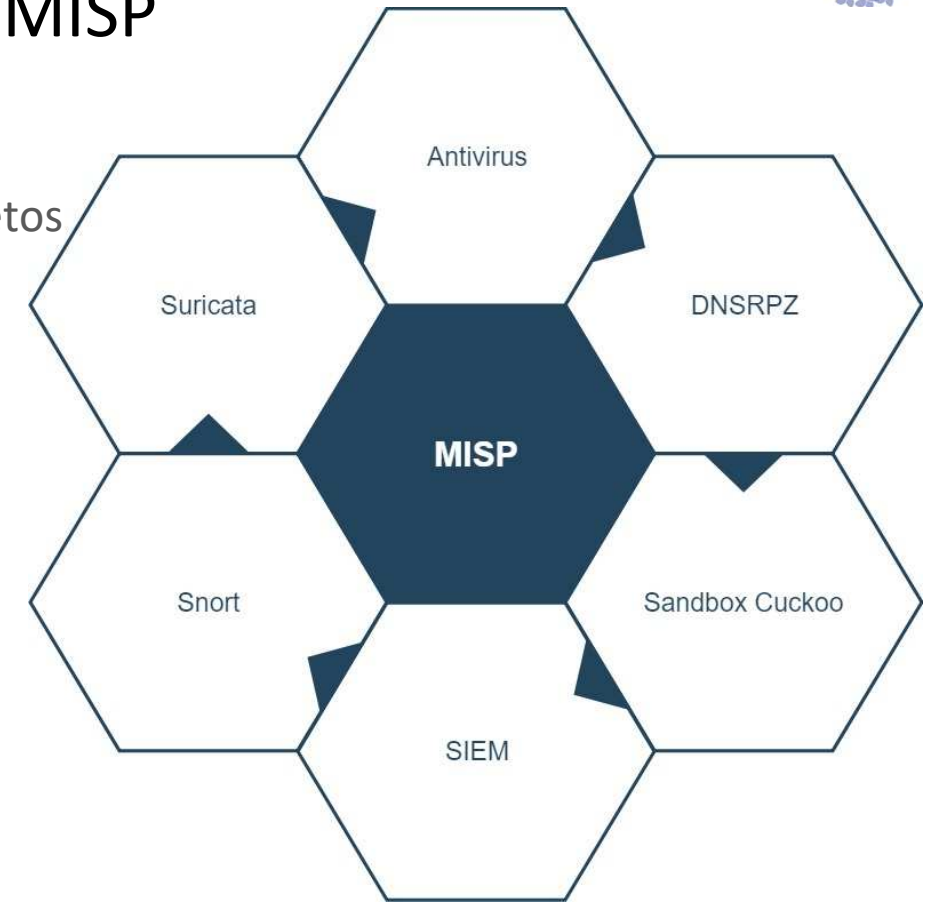


Segurança da informação

- Partilha é feita apenas entre membros confiáveis
- Exige certificado válido emitido pela instância e chave de utilizador para acesso à API
- Possibilita o uso de PGP (Pretty Good Privacy) para garantir uma partilha segura em trânsito

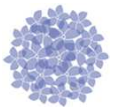
PRINCIPAIS OBJECTIVOS DO MISP

- Armazenar IOC´s de forma estruturada
- Ajudar na investigação de casos concretos
- Aumentar a eficiência dos sistemas de segurança



Instâncias MISP existentes

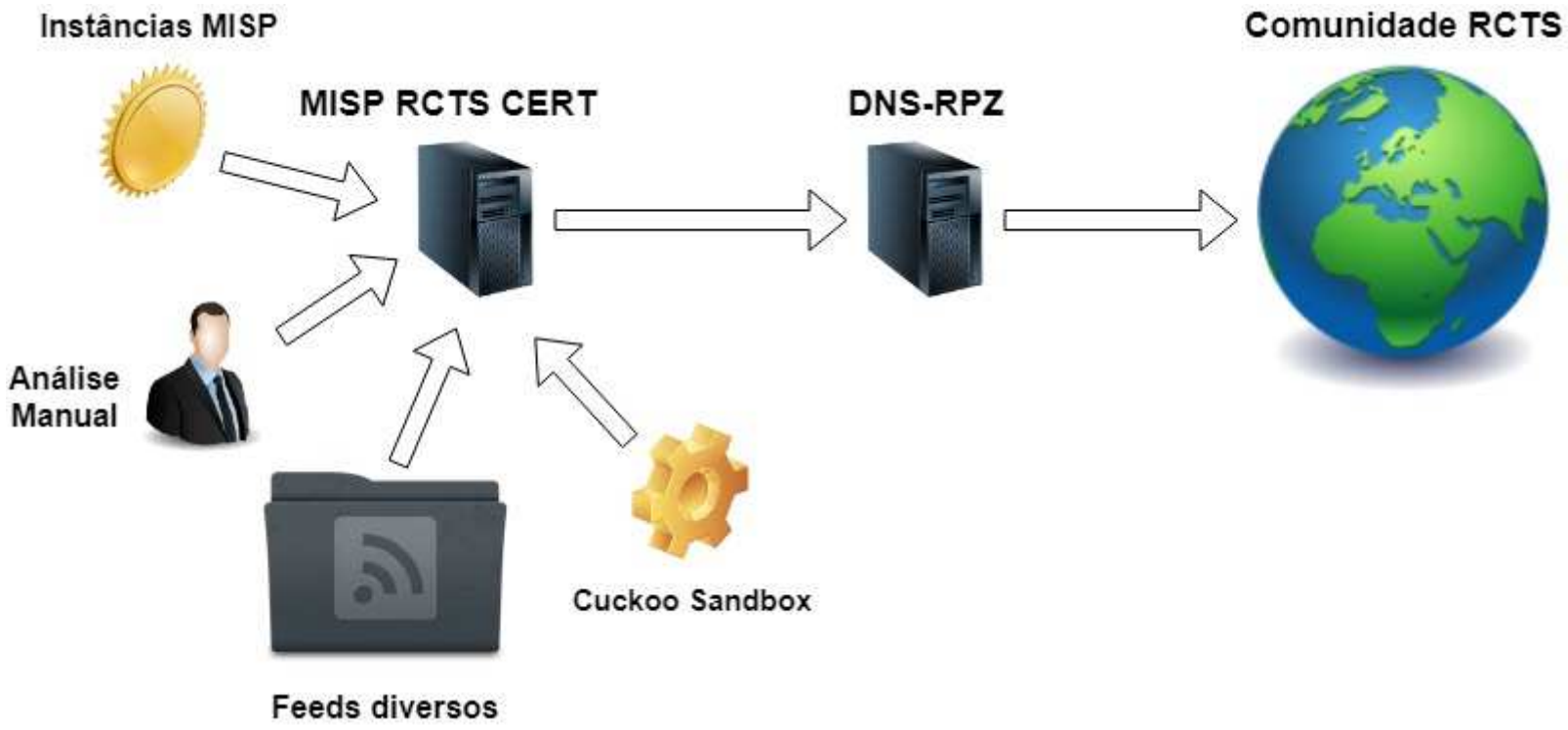
PROJECTO MISP RCTS CERT



- Instalação e configuração da instância MISP RCTS CERT
- Sincronização com outras instâncias MISP
- Interligação com sistemas existentes

Sandbox cuckoo e MISP RCTS CERT

MISP RCTS CERT e DNS-RPZ



O que se espera das organizações?

- Solicitem o acesso ao serviço através do email info@cert.rcts.pt
- Contribuam para a adição de novos eventos na instância

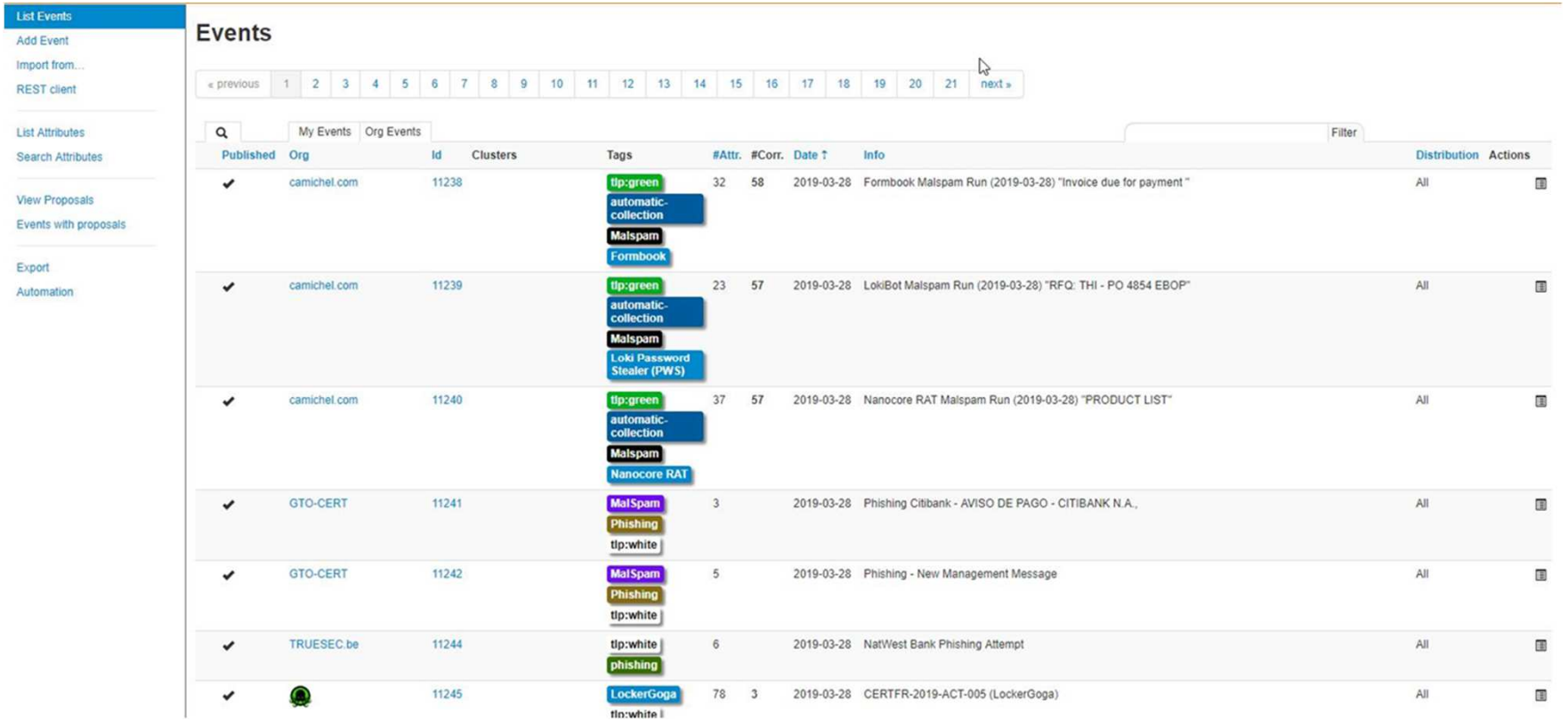
Obrigado!

Questões?

Vitor Sousa

08 de maio de 2019

Eventos


List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
Events
« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »
My Events Org Events
Filter
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 Loki Password Stealer (PWS) 23 57 2019-03-28 LokiBot 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 78 3 2019-03-28 CERTFR-2019-ACT-005 (LockerGoga) All

Evento e classificação

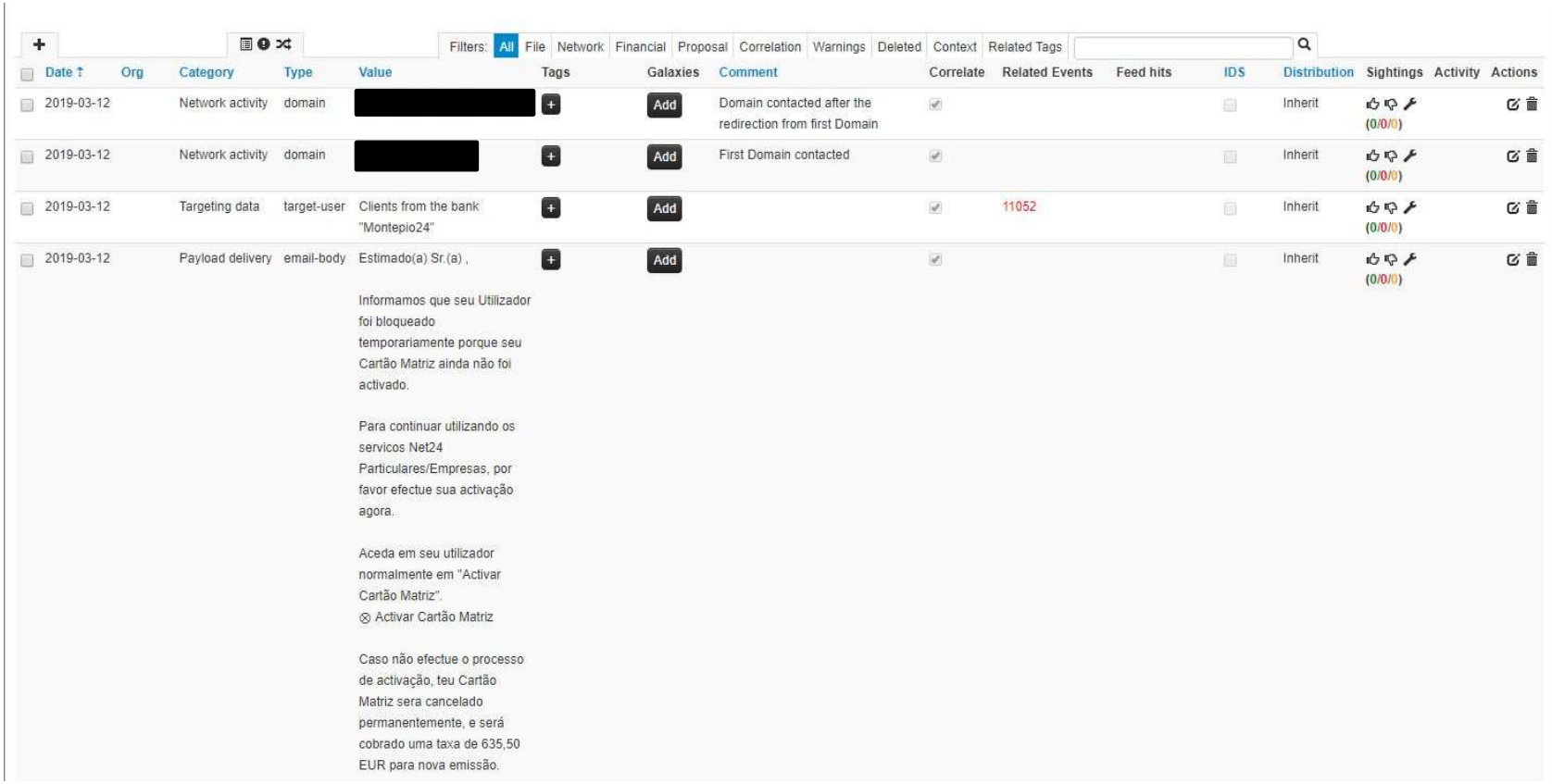
[redacted]

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
[redacted]	
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	[redacted]	+	Add	Domain contacted after the redirection from first Domain	✓				Inherit	(0/0/0)		
2019-03-12		Network activity	domain	[redacted]	+	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)		