

MISP: Rapportera in nätfiske-domän(er) eller stulna konton

En instruktion för hur du enklare ska rapportera nätfiske eller stulna konton via MISPs sätt (mha templates)

1) Skapa ett nytt MISP Event

Välj "Add Event" i menyn till vänster, och fyll i de åtminstone den nödvändigaste information gällande informationdelning och rubriken för din rapport.

HomeEvent ActionsGalaxiesInput FiltersGlobal ActionsSync ActionsAdministrationAudit

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

List EventsAdd EventImport from REST clientList AttributesSearch AttributesView ProposalsEvents with proposalsExportAutomation

Add Event

Date2019-04-25Distribution ⓘAll communities

Threat Level ⓘUndefinedAnalysis ⓘInitial

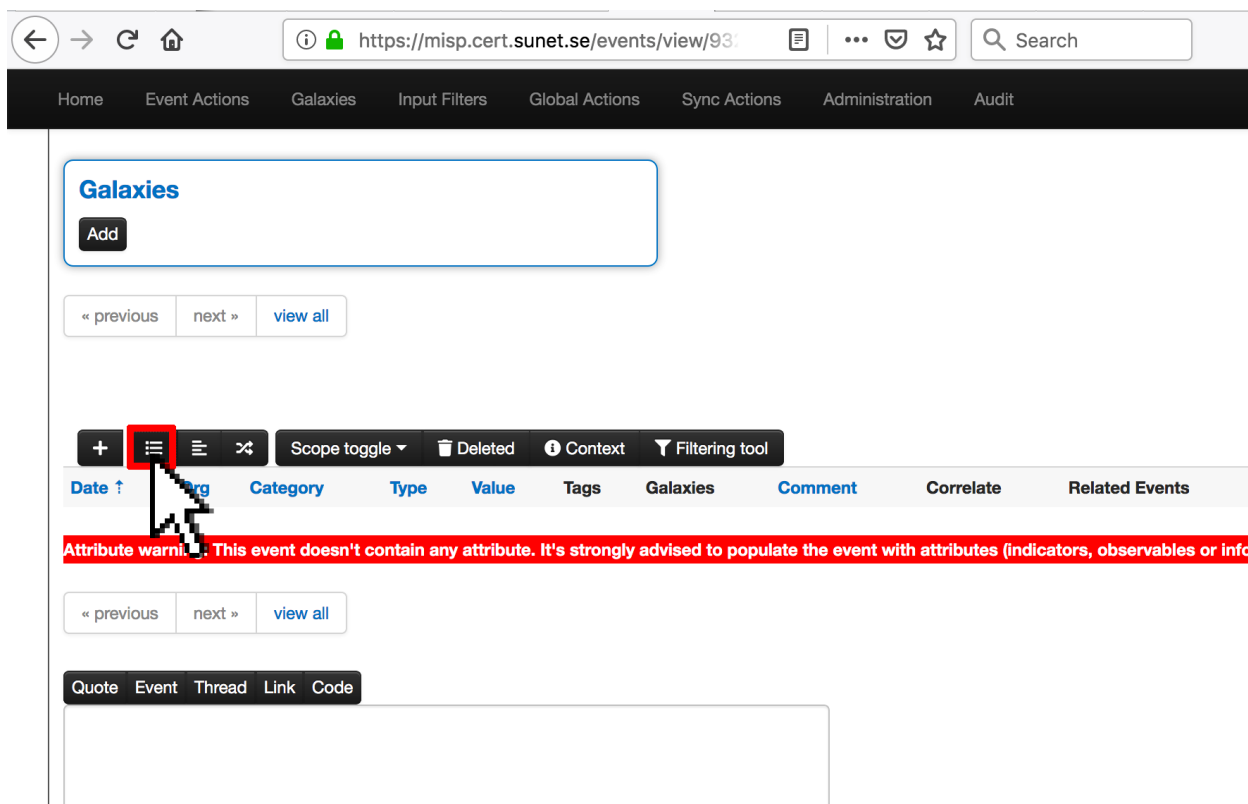
Event InfoRapportera Phishing/Malware domäner...

Extends eventEvent UUID or ID. Leave blank if not applicable.

Add

2) Välj att lägga till attribut via template

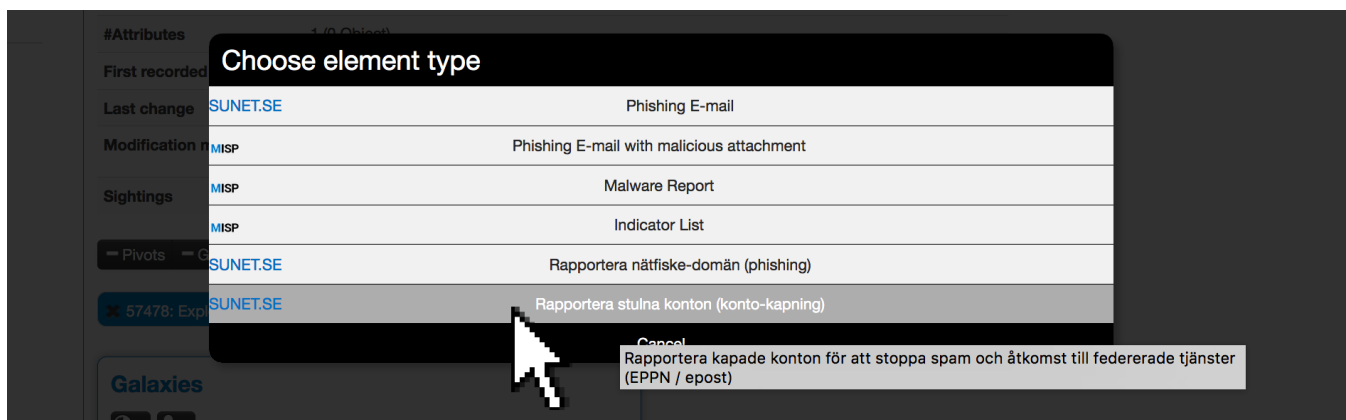
"Scrolla" ner i det nya MISP Event:et som du skapat för att hitta knappen på bilden nedan.



3) Välj template:n från menyn

För nätfiske, välj "Rapportera nätfiske-domän (phishing)"

För kapade konton, välj "Rapportera stulna konton (konto-kapning)"



4a) Fyll i de attribut som finns färdigt angivna i template:n

För nätfiske, fyll i alla domäner (om det är fler) samt en intern referens. Det går även bra att lägga in länk till ärende-system, IP-adressen domänen pekade på samt en fritext kommentar (som skulle kunna vara information från ärendet angående den här domänen etc.)

Home

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...

Populate From Template

Enrich Event

Merge attributes from...

Propose Attribute

Propose Attachment

Contact Reporter

Download as...

List Events

Add Event

Template Description

Template ID:5

Template Name:Rapportera phishingdomän

Created by:SUNET.SE

Description:Rapportera en eller flera domäner som används för phishing (eller har skadligt innehåll, tex. virus). Dessa går vidare in i RPZ-zon genereringen.

Tags automatically assigned:

tip:white

OSINT

rsit:fraud="phishing"

Field:Domännamn (*)

Description:Domännamnet "FQDN" är den eller de skadliga domänerna som ska in i RPZ. OBS! Det är viktigt att hela FQDN skrivs in, annars finns det risk att

Type:

domain

phishing.domän.ett.
phishing.domän.två.
(osv...)

Field:Referens (*)

Description:Din interna referens, typiskt ticketnr i ärendesystem

Type:

text

[# ÄRENDENR] samt ev. rubrik för ärendet

Field:Länk

Description:Länk direkt till ärendet i ärendesystemet

Type:

link

https://mitt.ändesystem.se/ärende=<ÄRENDENR>...

Field:IP-adress

Description:IP adressen domänen pekar på

Type:

domain|ip

[IP_ADRESS_VID_TILFÄLLET]

Field:Kommentar

Description:Ev. kommentar

4b) Fyll i de attribut som finns färdigt angivna i template

För kontokapning, fyll i eppn samt en intern referens. Det går även bra att lägga in länk till ärende-system, epost-adressen kontot är förknippat med, IP-adressen som användes av förövaren samt en fritext kommentar (som skulle kunna vara information från ärendet angående den hur/när kontot blev kapat mm.)

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Populate From Template

Enrich Event

Merge attributes from...

Propose Attribute

Propose Attachment

Download as...

List Events

Add Event

Template Description

Template ID: 6

Template Name: Rapportera stulna konton (konto-kapning)

Created by: SUNET.SE

Description: Rapportera kapade konton för att stoppa spam och åtkomst till federerade tjänster (EPPN / epost)

Tags automatically assigned:

tip:amber

rsit:intrusions="unprivileged-account-compromise"

Field: EPPN (*)

Description: EPPN (EduPersonPrincipalName) för det kapade kontot

Type: eppn

[EPPN här]

Field: Referens (*)

Description: Internt referens (typiskt ticketnummer i det interna ticketsystemet)

Type: text

[# Ärendenr] samt rubrik i ärendet

Field: Länk

Description: Länk till det interna ärendet i ticketsystemet

Type: link

https://mitt.arendesystem.se/?ärende=<ärende>

Field: Epost

Description: Epost-adressen för det kapade kontot (om det finns risk för att kontot börjar spamma)

Type: email-src

[ev_epost_adress_för_det_kapade_kontot]