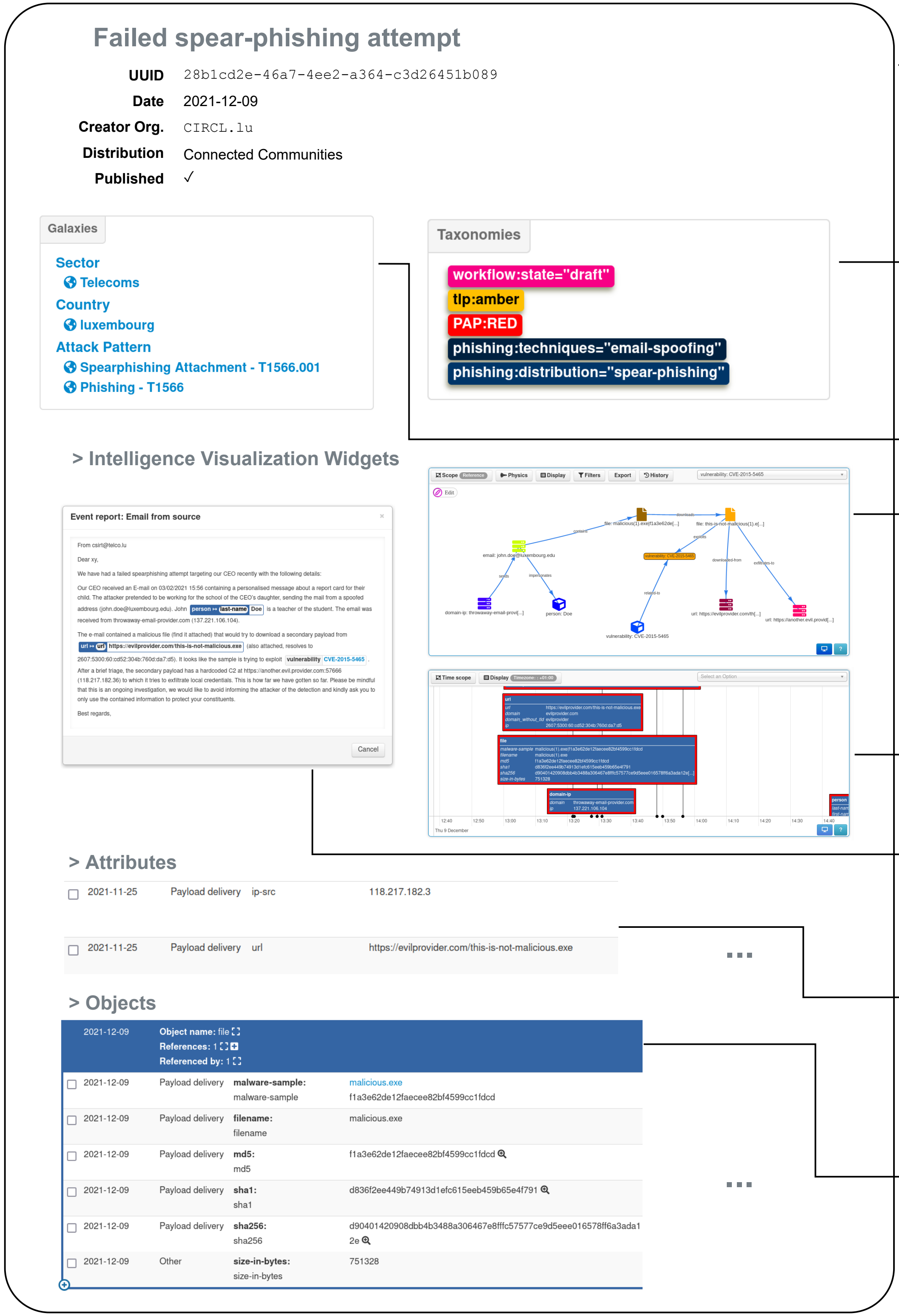
Representation of an incident in MISP



Failed spear-phishing attempt

UUID	28b1cd2e-46a7-4ee2-a364-c3d26451b089
Date	2021-12-09
Creator Org.	CIRCL.lu
Distribution	Connected Communities
Published	✓

Galaxies

- Sector
  - Telecoms
- Country
  - luxembourg
- Attack Pattern
  - Spearphishing Attachment - T1566.001
  - Phishing - T1566

Taxonomies

- workflow:state="draft"
- tlp:amber
- PAP:RED
- phishing:techniques="email-spoofing"
- phishing:distribution="spear-phishing"

> Intelligence Visualization Widgets

Event report: Email from source

From csirt@telco.lu

Dear xy,

We have had a failed spearphishing attempt targeting our CEO recently with the following details:

Our CEO received an E-mail on 03/02/2021 15:56 containing a personalised message about a report card for their child. The attacker pretended to be working for the school of the CEO's daughter, sending the mail from a spoofed address (john.doe@luxembourg.edu). John person ↦ last-name Doe is a teacher of the student. The email was received from throwaway-email-provider.com (137.221.106.104).

The e-mail contained a malicious file (find it attached) that would try to download a secondary payload from url ↦ url https://evilprovider.com/this-is-not-malicious.exe (also attached, resolves to 2607:5300:60:cd52:304b:760d:da7:d5). It looks like the sample is trying to exploit vulnerability CVE-2015-5465. After a brief triage, the secondary payload has a hardcoded C2 at https://another.evil.provider.com:57666 (118.217.182.36) to which it tries to exfiltrate local credentials. This is how far we have gotten so far. Please be mindful that this is an ongoing investigation, we would like to avoid informing the attacker of the detection and kindly ask you to only use the contained information to protect your constituents.

Best regards,

×
Cancel
Scope Reference
Physics
Display
Filters
Export
History
vulnerability: CVE-2015-5465
Edit
file: malicious(1).exe|f1a3e62de[...]
downloads
file: this-is-not-malicious(1).e[...]
contains
exploits
email: john.doe@luxembourg.edu
vulnerability: CVE-2015-5465
downloaded-from
exfiltrates-to
sends
impersonates
related-to
domain-ip: throwaway-email-provi[...]
person: Doe
url: https://evilprovider.com/th[...]
url: https://another.evil.provid[...]
vulnerability: CVE-2015-5465
?
Time scope
Display Timezone: : +01:00
Select an Option
12:40
12:50
13:00
13:10
13:20
13:30
13:40
13:50
14:00
14:10
14:20
14:30
14:40
Thu 9 December
?

url

url	https://evilprovider.com/this-is-not-malicious.exe
domain	evilprovider.com
domain_without_tld	evilprovider
ip	2607:5300:60:cd52:304b:760d:da7:d5

file

malware-sample	malicious(1).exe|f1a3e62de12faecee82bf4599cc1fdcd
filename	malicious(1).exe
md5	f1a3e62de12faecee82bf4599cc1fdcd
sha1	d836f2ee449b74913d1efc615eeb459b65e4f791
sha256	d90401420908dbb4b3488a306467e8fffc57577ce9d5eee016578ff6a3ada12e[...]
size-in-bytes	751328

domain-ip

domain	throwaway-email-provider.com
ip	137.221.106.104

person

last-nam
first-nam

> Attributes

□	2021-11-25	Payload delivery	ip-src	118.217.182.3
□	2021-11-25	Payload delivery	url	https://evilprovider.com/this-is-not-malicious.exe

...

> Objects

2021-12-09 **Object name:** file
References: 1
Referenced by: 1

□	2021-12-09	Payload delivery	**malware-sample:** malware-sample	malicious.exe f1a3e62de12faecee82bf4599cc1fdcd
□	2021-12-09	Payload delivery	**filename:** filename	malicious.exe
□	2021-12-09	Payload delivery	**md5:** md5	f1a3e62de12faecee82bf4599cc1fdcd
□	2021-12-09	Payload delivery	**sha1:** sha1	d836f2ee449b74913d1efc615eeb459b65e4f791
□	2021-12-09	Payload delivery	**sha256:** sha256	d90401420908dbb4b3488a306467e8fffc57577ce9d5eee016578ff6a3ada1 2e
□	2021-12-09	Other	**size-in-bytes:** size-in-bytes	751328

...

Event: Encapsulates contextually linked information.
Events also have basic information including ownership and access-control
Here: Contains all the information related to the spear-phishing incident.

Taxonomies: Simple label standardised on common set of vocabularies.
Here: Usage of labels to classify the current completeness of the Event, what recipient can do with the information and the category of the incident.

Galaxies & Galaxy-Clusters: Advanced label containing meta-data
Here: The sector affected by the incident as well as the country. The kill-chain of the attack can be described using the MITRE ATT&CK framework

Event Graph: Visualization of the relationships between entities contained in the Event.
Here: The whole story of the attack can be described with relationships defined between Attributes and Objects

Event Timeline: Visualization of the temporality of the data contained in the event.
Here: A timeline of the steps performed during the attack. The time data is taken directly from the Attributes and Objects belonging to the Event.

Event Report: Markdown-aware supporting text document to describe events or incidents
Here: The report describe the steps taken by the attacker and provide additional contextual information. It also contains references to Attributes and Object encoded in the Event

Attributes: Basic building block to represent information.
They can have context such as taxonomy and express if they are supportive data or meant for automation. An Event can have multiple Attributes
Here: Two Attributes representing payload delivery. One is an IP address, the other is an URL.

Objects: Advanced building block allowing Attribute composition via predefined templates.
As an Object is an instantiation of its template, it is composed of Attributes that make sense Together. They can also have relationship to other entity contained in the Event
Here: A file object composed of Attributes such as the filename, size and hashes. It also have a relationship