MISP

10th

Name : MoonGyu Lee

Contents

Account Information

Web address: https://3.87.57.59/

[Figure 1 Login Form]

ID	readevent@gmail.com
Password	Readevent*10025800

[Figure 2 Account information]

1. A description of the deployment

I used these kinds of tags for identifying what case is. My custom tags are APT, Lazarus, email, hwp, maldoc, malware, postscript, network_icmp. These Things make it easier to identify cases. And then, Galaxy, internal of MISP, is very useful to handle the cases sush as APT group attack pattern. The postscript tag is a method used in hwp malicious documents.

Id	Exportable	Hidden	Name	Restricted to org	Restricted to user	Taxonomy	Tagged events	Tagged attributes	Activity	Favourite	Actions
18	✔	✖	APT				5	0		☐	
1	✔	✖	Lazarus				7	0		☐	
5	✔	✖	email				1	0		☐	
3	✔	✖	hwp				4	0		☐	
27	✔	✖	maldoc				2	0		☐	
2	✔	✖	malware				4	0		☐	
24	✔	✖	misp-galaxy:malpedia="Lazarus (Windows)"				5	0		☐	
29	✔	✖	misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103"				1	0		☐	
28	✔	✖	misp-galaxy:mitre-attack-pattern="Execution through API - T1106"				1	0		☐	
25	✔	✖	misp-galaxy:mitre-attack-pattern="Process Injection - T1055"				1	0		☐	
23	✔	✖	misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193"				1	0		☐	
19	✔	✖	misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28"				1	0		☐	
21	✔	✖	misp-galaxy:threat-actor="APT 29"				1	0		☐	
17	✔	✖	misp-galaxy:threat-actor="APT 30"				1	0		☐	
10	✔	✖	misp-galaxy:threat-actor="Axiom"				1	0		☐	

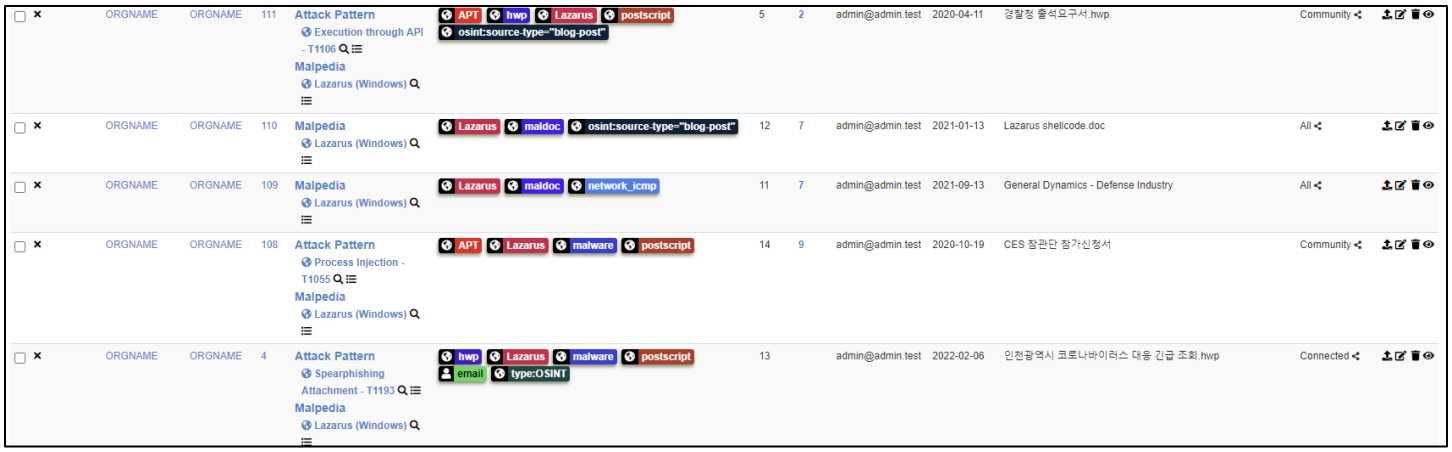
[Figure 3 Tag list that I used]

16	✔	✖	misp-galaxy:threat-actor="Equation Group"				1	0		☐	
11	✔	✖	misp-galaxy:threat-actor="Sofacy"				4	0		☐	
12	✔	✖	misp-galaxy:threat-actor="Turla Group"				2	0		☐	
20	✔	✖	misp-galaxy:threat-actor="WildNeutron"				1	0		☐	
15	✔	✖	misp-galaxy:tool="EquationDrug"				1	0		☐	
14	✔	✖	misp-galaxy:tool="Regin"				2	0		☐	
22	✔	✖	misp-galaxy:tool="Trojan.Seaduke"				1	0		☐	
13	✔	✖	misp-galaxy:tool="Turla"				1	0		☐	
26	✔	✖	network_icmp				1	0		☐	
9	✔	✖	osint:source-type="blog-post"				3	0		☐	
4	✔	✖	postscript				3	0		☐	
7	✔	✖	tlp:green				18	0		☐	
8	✔	✖	tlp:white				42	0		☐	
6	✔	✖	type:OSINT				56	0		☐	

[Figure 4 Tag list that I used]

2. Use case of sharing based on the chosen campaign

I designed a case for the Lazarus apt group. This group distributes document-type malicious codes such as hwp and docm. Samples were obtained directly from hybrid analysis and cases were created based on information from Virustotal. Among them, I directly analyzed 인천광역시 코로나바이러스 대응 긴급 조회. hwp file in 2020.



ORGNAME	ORGNAME	111	Attack Pattern Execution through API - T1106 Malpedia Lazarus (Windows)	APT, hwp, Lazarus, postscript, osint:source-type="blog-post"	5	2	admin@admin.test	2020-04-11	경찰청 출석요구서.hwp	Community		
ORGNAME	ORGNAME	110	Malpedia Lazarus (Windows)	Lazarus, maldoc, osint:source-type="blog-post"	12	7	admin@admin.test	2021-01-13	Lazarus shellcode.doc	All		
ORGNAME	ORGNAME	109	Malpedia Lazarus (Windows)	Lazarus, maldoc, network_icmp	11	7	admin@admin.test	2021-09-13	General Dynamics - Defense Industry	All		
ORGNAME	ORGNAME	108	Attack Pattern Process Injection - T1055 Malpedia Lazarus (Windows)	APT, Lazarus, malware, postscript	14	9	admin@admin.test	2020-10-19	CES 참관단 참가신청서	Community		
ORGNAME	ORGNAME	4	Attack Pattern Spearphishing Attachment - T1193 Malpedia Lazarus (Windows)	hwp, Lazarus, malware, postscript, email, type:OSINT	13		admin@admin.test	2022-02-06	인천광역시 코로나바이러스 대응 긴급 조회.hwp	Connected		

[Figure 5 List event]

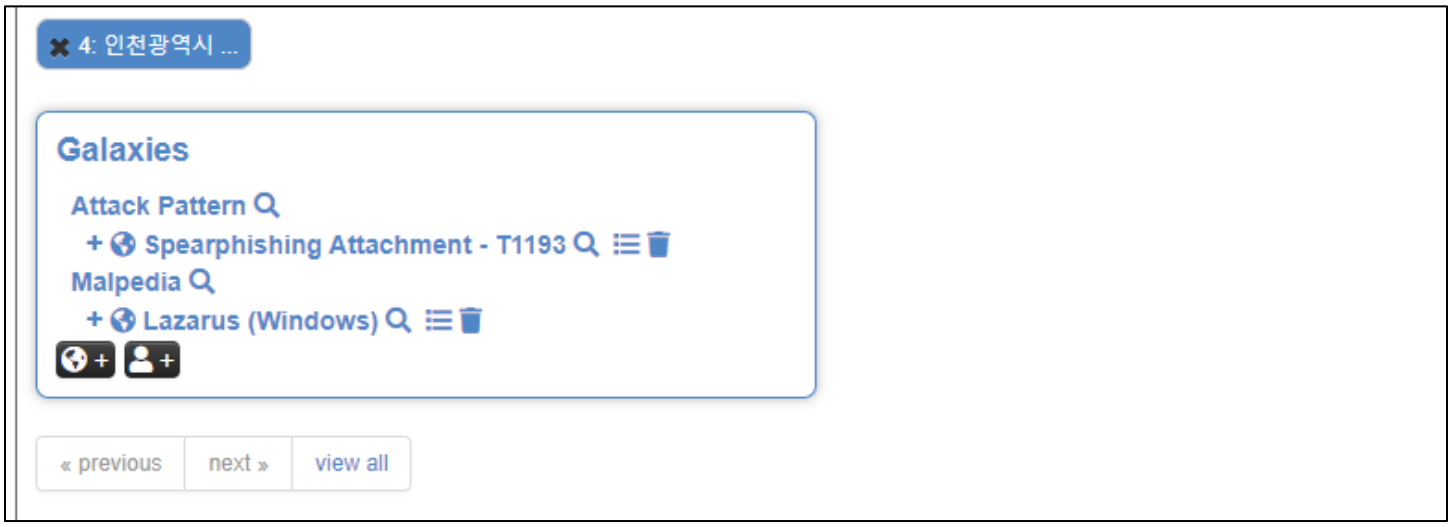
The document file below was used in a spear phishing attack targeting public institutions. In the hwp file, a malicious postscript was inserted under bindata, and if we analyze this postscript, there is a built-in PowerShell code that downloads and executes the dropper from the C&C server.

인천광역시 코로나바이러스 대응 긴급 조회.hwp

Event ID	4
UUID	5160476e-fc91-4b24-87d3-0ac4a5157d83
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Tags	hwp x, Lazarus x, malware x, postscript x, email x, type:OSINT x

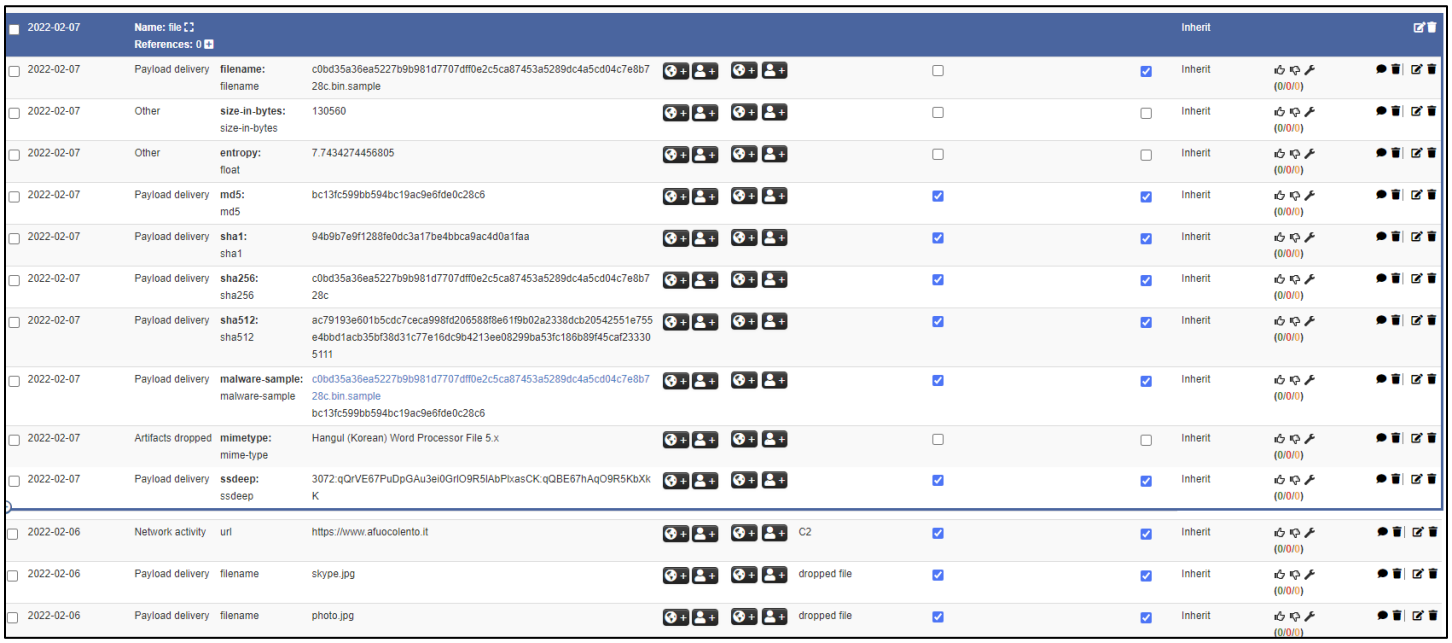
[Figure 6 인천광역시 코로나바이러스 대응 긴급 조회.hwp]

Galaxies show detail attack patterns and apt groups. Through this, this case is a spear phishing attack and information about the Lazarus apt group can be confirmed.



[Figure 7 Galaxies of MISP]

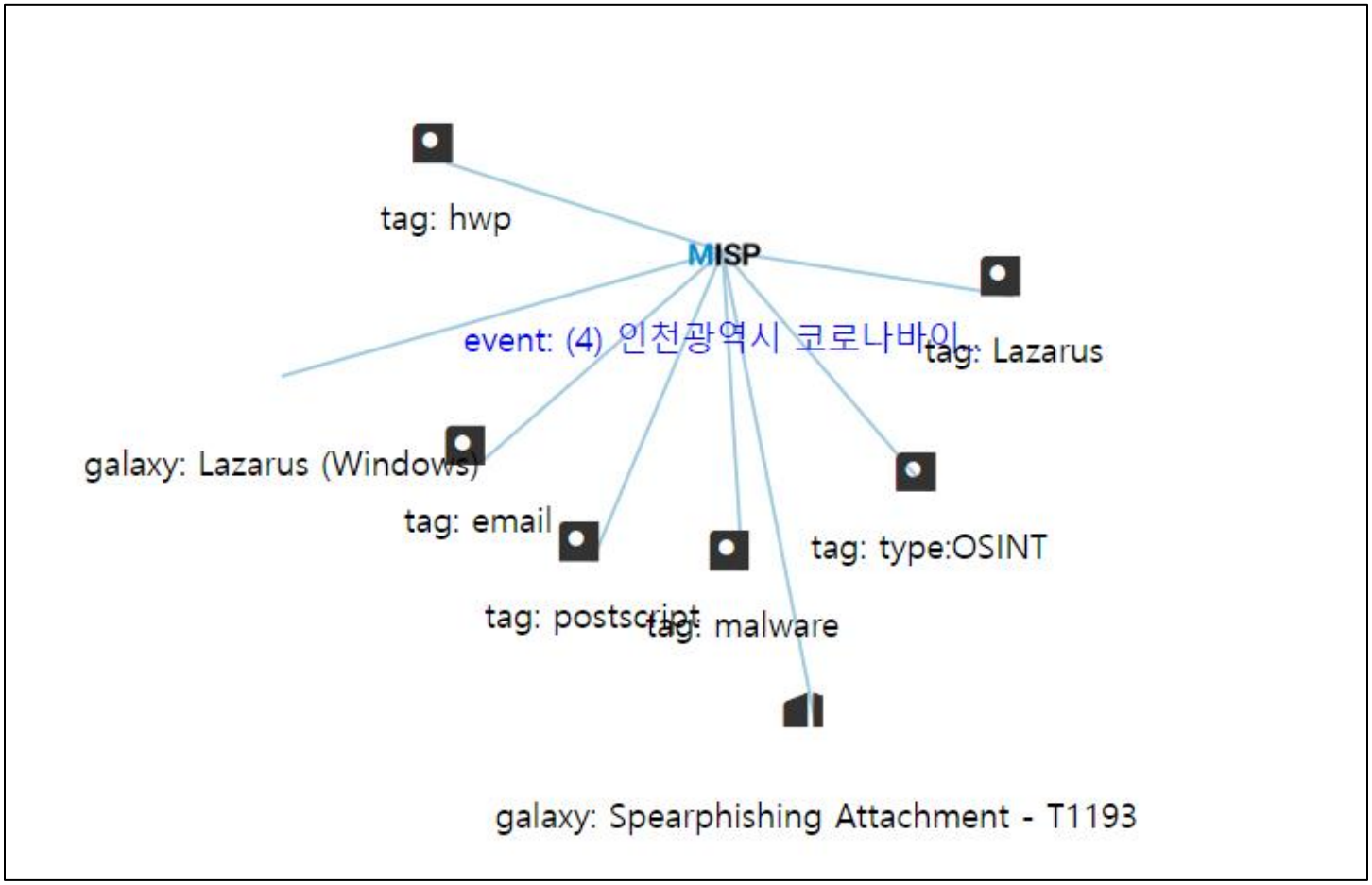
IOCs have each payload hash value (md5, sha1, sha256), C&C server, and dropper file name. If you look at the dropper file name, you can see that it is a jpg extension, but it is actually an executable PE file.



2022-02-07	Name: file References: 0						Inherit	
2022-02-07	Payload delivery	filename: filename	c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b728c.bin.sample			☑	Inherit	(0/0/0)
2022-02-07	Other	size-in-bytes: size-in-bytes	130560			☐	Inherit	(0/0/0)
2022-02-07	Other	entropy: float	7.7434274456805			☐	Inherit	(0/0/0)
2022-02-07	Payload delivery	md5: md5	bc13fc599bb594bc19ac9e6fde0c28c6		☑	☑	Inherit	(0/0/0)
2022-02-07	Payload delivery	sha1: sha1	94b9b7e9f1288fe0dc3a17be4bbca9ac4d0a1faa		☑	☑	Inherit	(0/0/0)
2022-02-07	Payload delivery	sha256: sha256	c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b728c		☑	☑	Inherit	(0/0/0)
2022-02-07	Payload delivery	sha512: sha512	ac79193e601b5cdc7ceca998fd206588f8e61f9b02a2338dcb20542551e755e4bbd1acb35bf38d31c77e16dc9b4213ee08299ba53fc186b89f45caf233305111		☑	☑	Inherit	(0/0/0)
2022-02-07	Payload delivery	malware-sample: malware-sample	c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b728c.bin.sample bc13fc599bb594bc19ac9e6fde0c28c6		☑	☑	Inherit	(0/0/0)
2022-02-07	Artifacts dropped	mimetype: mime-type	Hangul (Korean) Word Processor File 5.x		☐	☐	Inherit	(0/0/0)
2022-02-07	Payload delivery	ssdeep: ssdeep	3072:qQrVE67PuDpGAu3el0GrlO9R5lAbPlxasCK:qQBE67hAqO9R5KbXkK		☑	☑	Inherit	(0/0/0)
2022-02-06	Network activity	url	https://www.afuocolento.it	C2	☑	☑	Inherit	(0/0/0)
2022-02-06	Payload delivery	filename	skype.jpg	dropped file	☑	☑	Inherit	(0/0/0)
2022-02-06	Payload delivery	filename	photo.jpg	dropped file	☑	☑	Inherit	(0/0/0)

[Figure 8 IOCs]

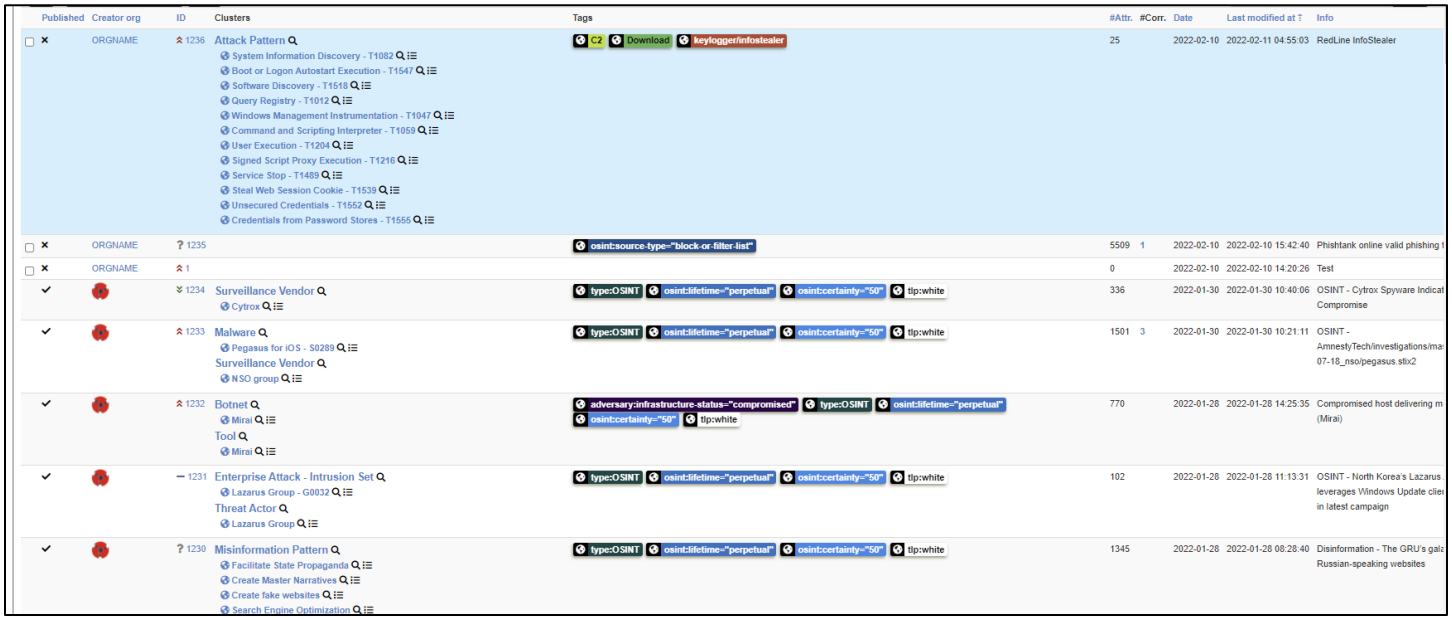
The graph below makes it easy to identify the data associated with the case.



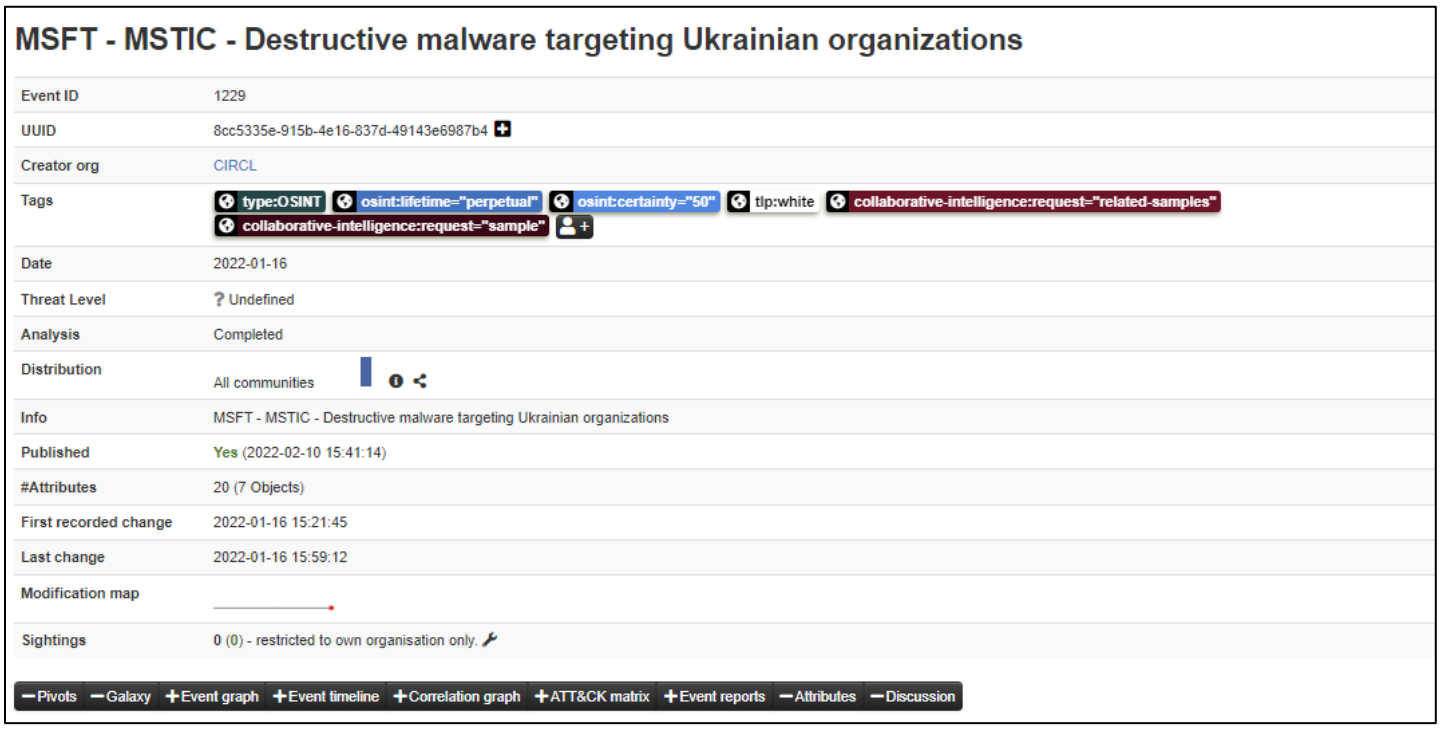
[Figure 9 Correlation Graph]

3. MISP network

I visited the MISP(SungHwan Seo). There are lots of events. Among them, malware targeting Ukrainian government agencies was interesting.



[Figure 10 Event List of MISP(SungHwan Seo)]



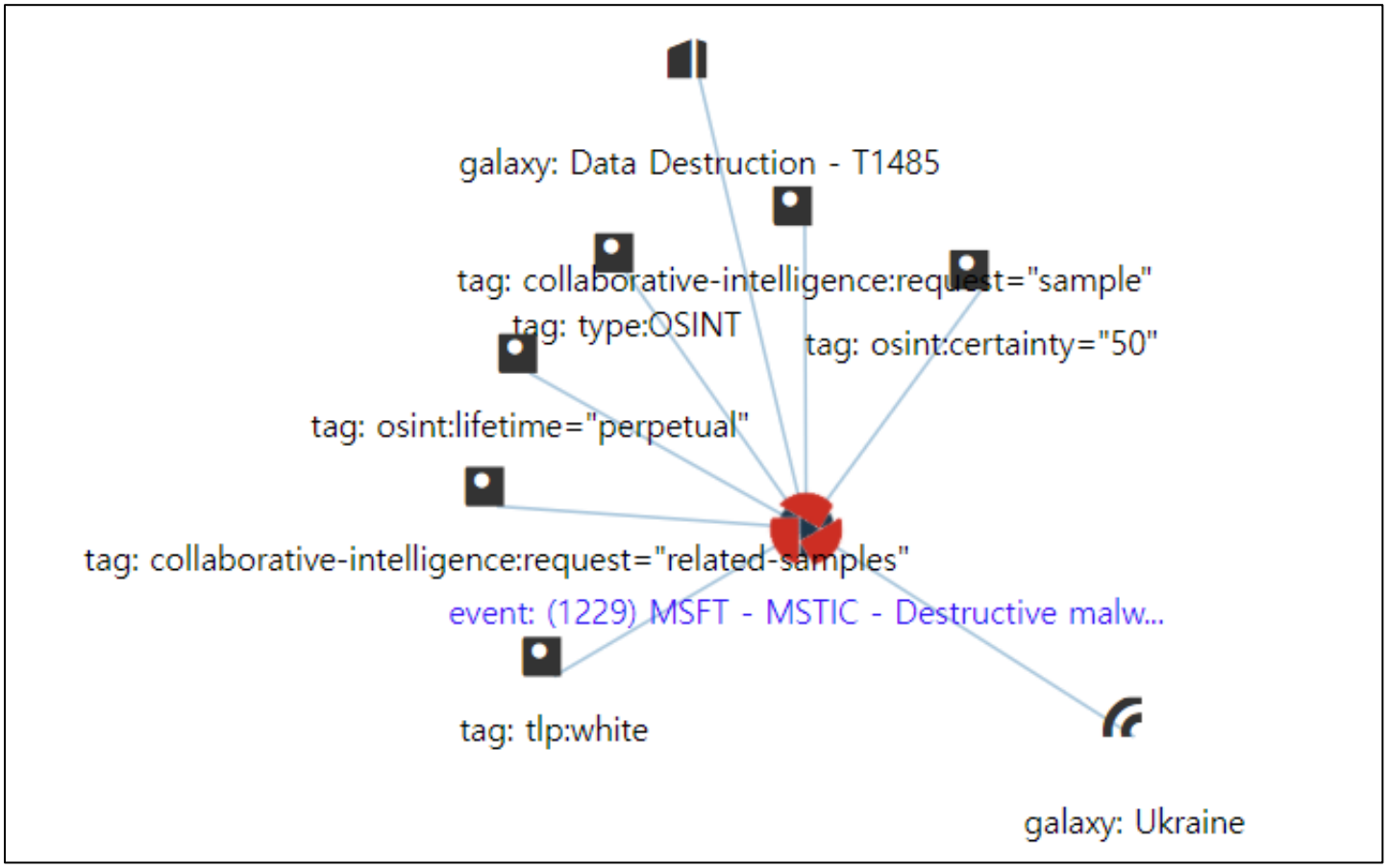
[Figure 11 Malware targeting Ukrainian organizations]

Among these IOCs, the commandline stood out. It appears to be a command downloaded from the malicious drop file c2 and executed.

2022-01-16	Object name: file References: 0				Hash of destructive malware stage1.exe		Inherit	
2022-01-16	Payload delivery	sha256: sha256	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92				Inherit	(0/0/0)
2022-01-16	Payload delivery	filename: filename	stage1.exe				Inherit	(0/0/0)
2022-01-16	Other	state: text	Malicious				Inherit	(0/0/0)
2022-01-16	Object name: file References: 0				Hash of stage2.exe		Inherit	
2022-01-16	Payload delivery	sha256: sha256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78				Inherit	(0/0/0)
2022-01-16	Payload delivery	filename: filename	stage2.exe				Inherit	(0/0/0)
2022-01-16	Other	state: text	Malicious				Inherit	(0/0/0)
2022-01-16	Object name: command-line References: 0						Inherit	
2022-01-16	Other	value: text	cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1				Inherit	(0/0/0)
2022-01-16	Other	description: text	Example Impacket command line showing the execution of the destructive malware. The working directory has varied in observed intrusions.				Inherit	(0/0/0)
2022-01-16	Other	text	Address: 1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfvBalance: 0.0001185800 BTC (+0.0001185800 BTC / -0.0000000000 BTC)Transactions: 1 (previewing up to 5 most recent)==========#1 14 Jan 2022 14:01:25 UTC 0.00011858 BTC 5.11 USD 4.48 EUR		1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv: Enriched via the btc_steroids module		Inherit	(0/0/0)

[Figure 12 IOCs]

By looking at the correlation graph, information about this case could be identified at a glance.



[Figure 13 Correlation Graph]