REPORT

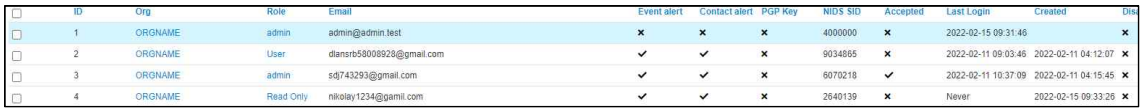
과 제 명	MISP
멘 토	Nikolay 멘토님
트 랙	디지털포렌식
이 름	서 성 환
마감일자	2021.2.18

차세대 보안리더
양성 프로그램

☐ Web construction and account information.

My MISP Web Site : https://3.144.179.151/

[그림 3] Login Site



	ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Accepted	Last Login	Created	Dis
☐	1	ORGNAME	admin	admin@admin.test	×	×	×	4000000	×	2022-02-15 09:31:46		×
☐	2	ORGNAME	User	dlansrb58008928@gmail.com	✓	✓	×	9034865	×	2022-02-11 09:03:46	2022-02-11 04:12:07	×
☐	3	ORGNAME	admin	sdj743293@gmail.com	✓	✓	×	6070218	✓	2022-02-11 10:37:09	2022-02-11 04:15:45	×
☐	4	ORGNAME	Read Only	nikolay1234@gamil.com	✓	✓	×	2640139	×	Never	2022-02-15 09:33:26	×

[그림 4] Account information

ID	PASSWD
nikolay1234@gmail.com	Nikolay1234!@#$

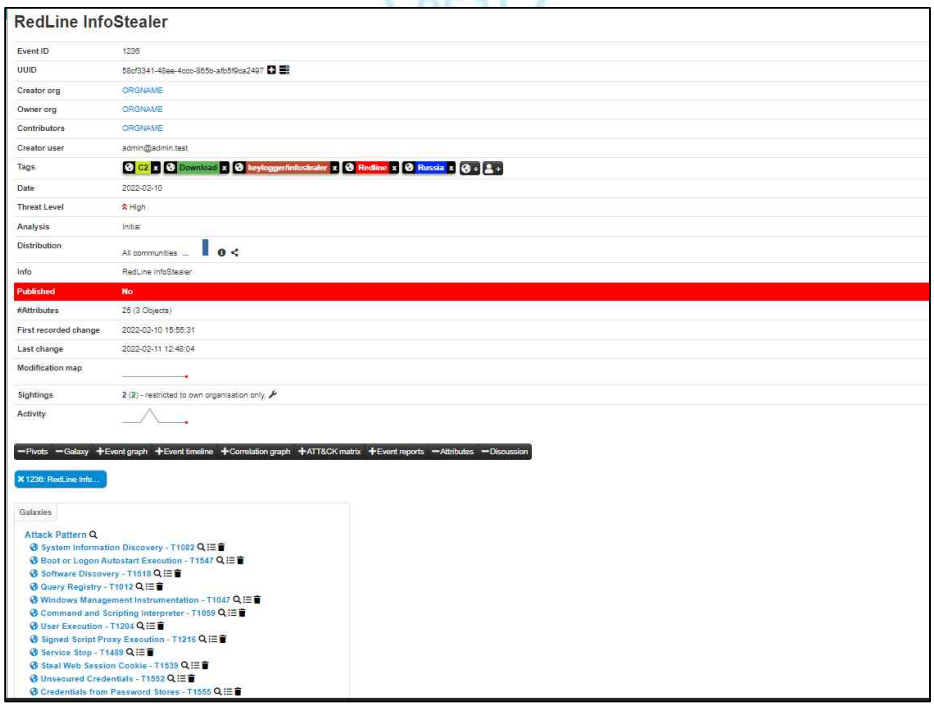
[표 2] Mentor's Account

○ I had to choose a tag according to the red line, the sample I chose, but I added it because there was no red line tag in the MISP. So I added a tag that I made myself.

909	✓	×	×	PowerView	×	×	2	1
415	✓	×	×	Powershell	×	×	1	2
880	✓	×	×	Powershell Empire	×	×	2	140
939	✓	×	×	PyXie	×	×	1	8
496	✓	×	×	RAT	×	×	0	3
732	✓	×	×	RAWINPUT	×	×	1	0
519	✓	×	×	REDLEAVES	×	×	0	17
404	✓	×	×	RTF	×	×	0	8
905	✓	×	×	Ransomware	×	×	2	0
1066	✓	×	×	Redline	✓	✓	0	0
921	✓	×	×	Remcos RAT	×	×	1	0
528	✓	×	×	Ruse: Job Application	×	×	1	0
1067	✓	×	×	Russia	✓	✓	0	0
938	✓	×	×	Ryuk	×	×	1	0
407	✓	×	×	SCRIPTLET	×	×	0	4
336	✓	×	×	SMB	×	×	0	6

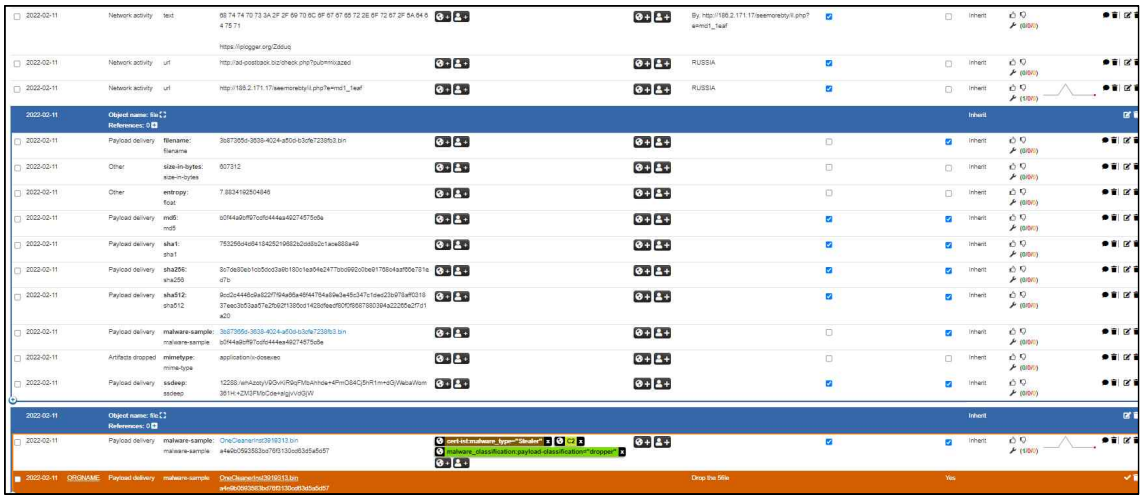
[그림 5] Tag List

○ Next, I registered the event for Red Line, an information-stealing malicious code that I had analyzed before.



[그림 6] Add Event

○ After the event registration, I registered and shared one of my samples, and I registered the results of my analysis and metadata information.

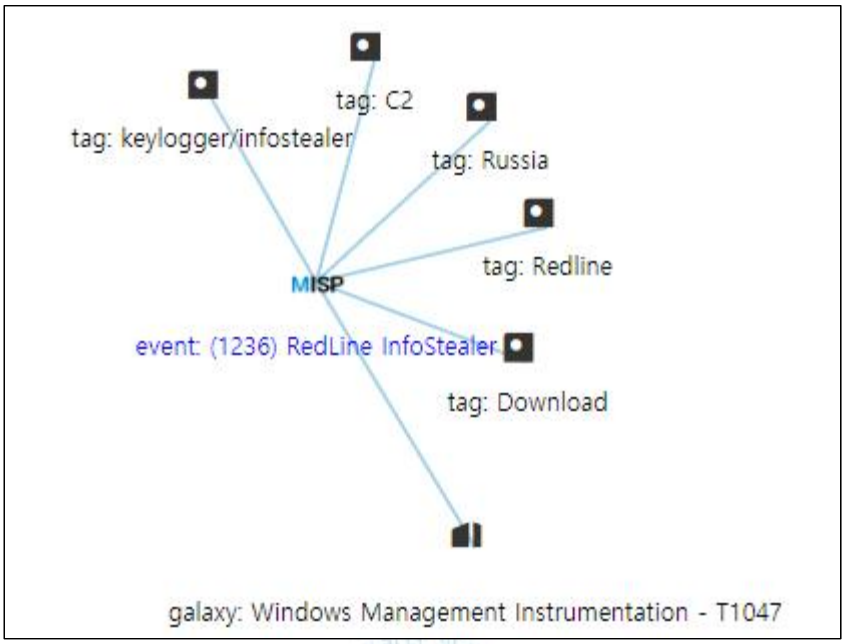


[그림 7] Add Event Info

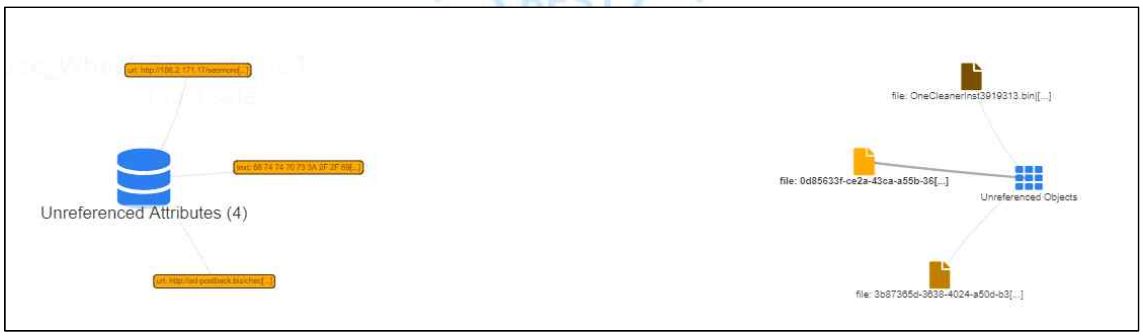
○ Also, as I analyzed before, I knew Mitre-Attack information about the malicious code, so I also enter this information.

[그림 8] Mitre-Attack

○ also briefly check the information about the events I added through the graph.



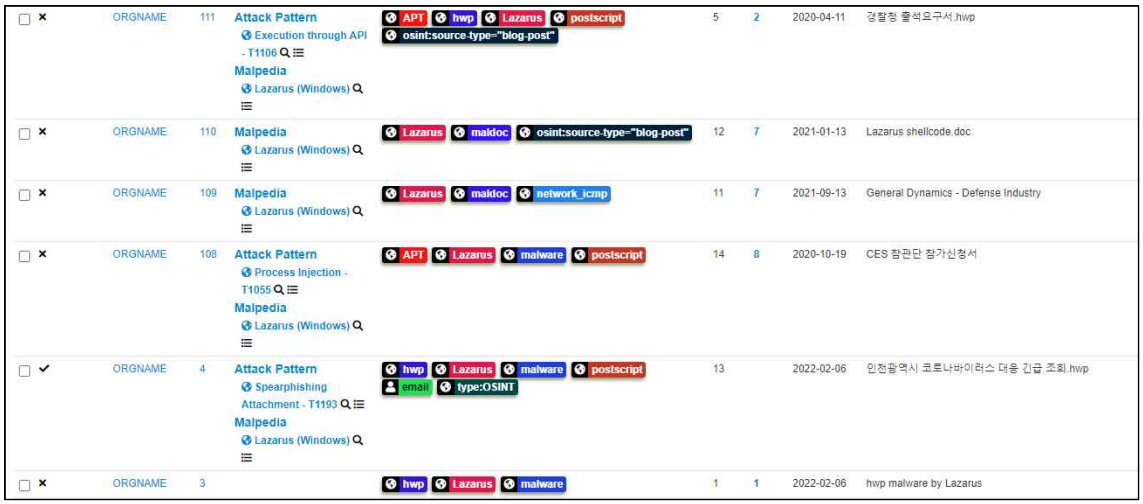
[그림 9] Event Graph 1



[그림 10] Event Graph 2

○ Exchange MISP information with other mentees.

- I visited Moongyu's MISP and there was Lazarus, a North Korean malicious code that I was previously interested in.



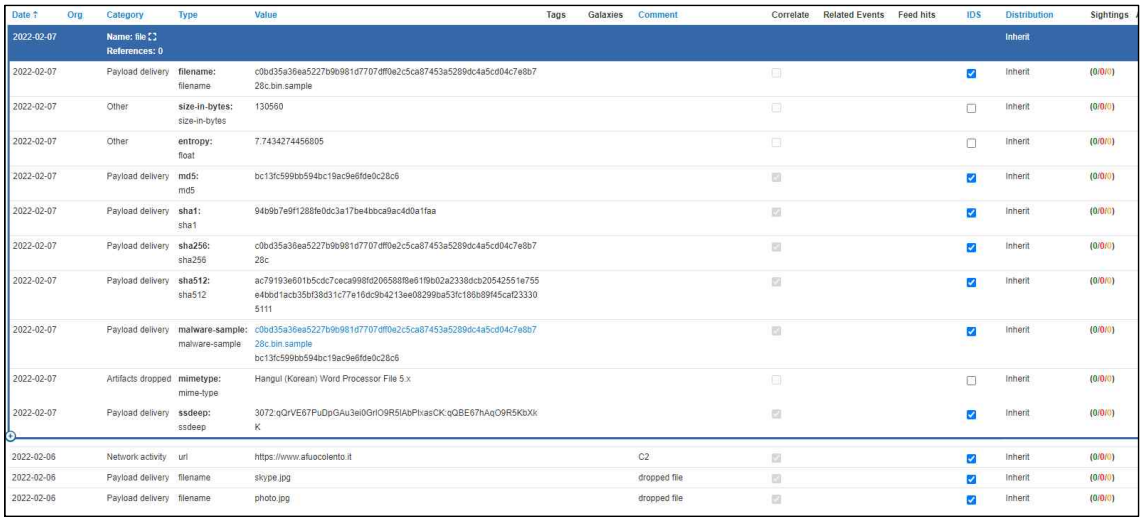
×	ORGNAME	111	Attack Pattern Execution through API - T1106 Malpedia Lazarus (Windows)	APT, hwp, Lazarus, postscript, osint:source-type="blog-post"	5	2	2020-04-11	경찰청 출석요구서.hwp
×	ORGNAME	110	Malpedia Lazarus (Windows)	Lazarus, maldoc, osint:source-type="blog-post"	12	7	2021-01-13	Lazarus shellcode.doc
×	ORGNAME	109	Malpedia Lazarus (Windows)	Lazarus, maldoc, network_icmp	11	7	2021-09-13	General Dynamics - Defense Industry
×	ORGNAME	108	Attack Pattern Process Injection - T1055 Malpedia Lazarus (Windows)	APT, Lazarus, malware, postscript	14	8	2020-10-19	CES 참관단 참가신청서
✓	ORGNAME	4	Attack Pattern Spearphishing Attachment - T1193 Malpedia Lazarus (Windows)	hwp, Lazarus, malware, postscript, email, type:OSINT	13		2022-02-06	인천광역시 코로나바이러스 대응 긴급 조회.hwp
×	ORGNAME	3		hwp, Lazarus, malware	1	1	2022-02-06	hwp malware by Lazarus

[그림 11] Moongyu's MISP

인천광역시 코로나바이러스 대응 긴급 조회.hwp

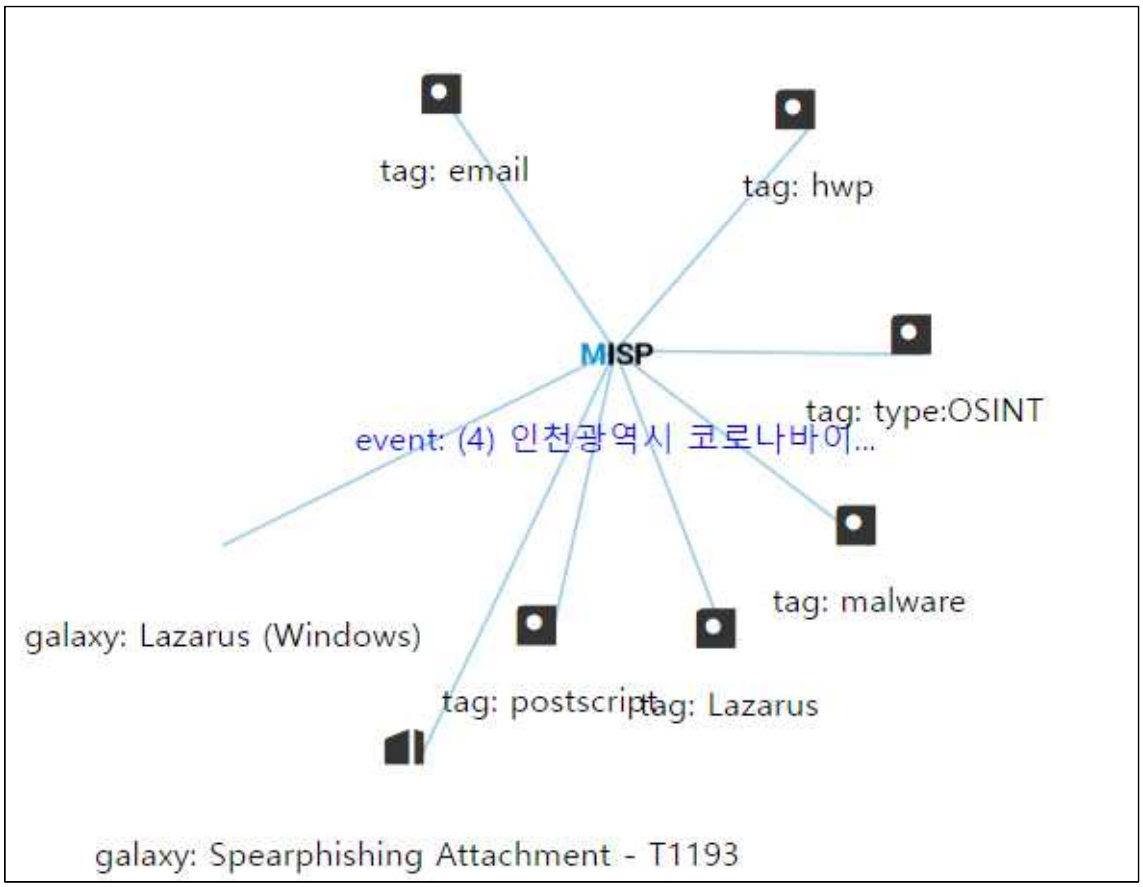
Event ID	4
UUID	5160476e-fc91-4b24-87d3-0ac4a5157d83
Creator org	ORGNAME
Creator user	admin@admin.test
Tags	hwp, Lazarus, malware, postscript, email, type:OSINT
Date	2022-02-06
Threat Level	Undefined
Analysis	Initial
Distribution	Connected communities
Info	인천광역시 코로나바이러스 대응 긴급 조회.hwp
Published	Yes (2022-02-11 04:01:54)
#Attributes	13 (1 Object)
First recorded change	2022-02-06 13:45:30
Last change	2022-02-07 01:14:29
Modification map	
Sightings	0 (0) - restricted to own organisation only.

[그림 12] One of Moonkyu's MISP Information.



Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings
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	ac79193e601b5cdc7ceca998fd206588f8e61f9b02a2338dcb20542551e7554e4bbd1acb35bf38d31c77e16dc9b4213ee08299ba53fc186b89f45caf233305111				☑			☑	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)

[그림 13] Lazarus Malware Information



[그림 14] Event Graph