



MISP

10th

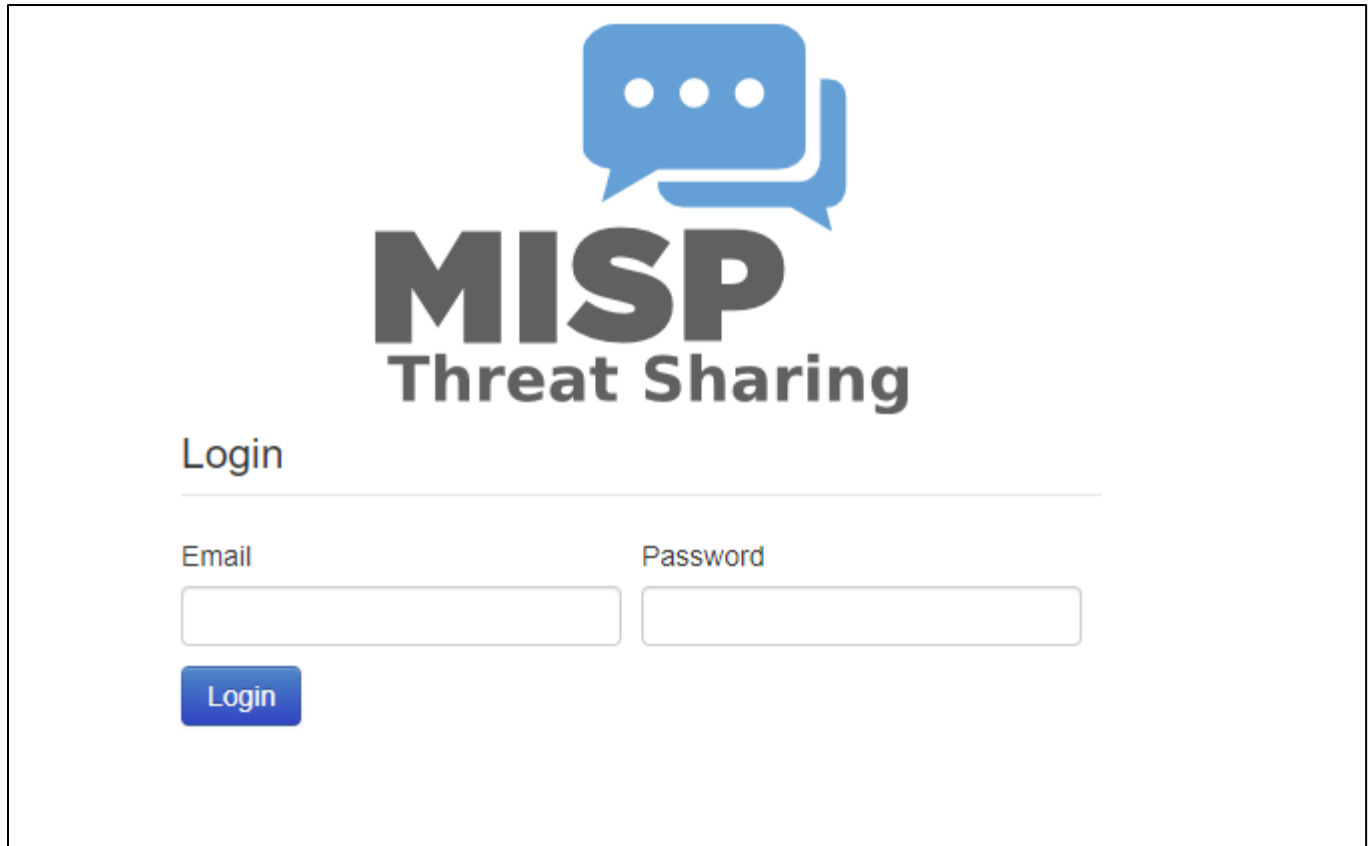
Name : MoonGyu Lee

Contents

Account Information	1
A description of the deployment.....	2
Use case of sharing based on the chosen campaign	3
MISP network	6

Account Information

Web address: <https://3.87.57.59/>



The image shows the login interface for MISP Threat Sharing. At the top center is a blue logo consisting of two overlapping speech bubbles. Below the logo, the text "MISP" is displayed in a large, bold, dark grey font, with "Threat Sharing" in a smaller, bold, dark grey font directly underneath. Below the text, the word "Login" is written in a dark grey font. A horizontal line separates the "Login" text from the input fields. There are two input fields: "Email" on the left and "Password" on the right. Below the "Email" field is a blue button with the word "Login" in white text.

[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 such 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		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
1	✓	✗	Lazarus				7	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
5	✓	✗	email				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
3	✓	✗	hwp				4	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
27	✓	✗	maldoc				2	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
2	✓	✗	malware				4	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
24	✓	✗	misp-galaxy:malpedia-"Lazarus (Windows)"				5	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
29	✓	✗	misp-galaxy:mitre-attack-pattern-"Appinit DLLs - T1103"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
28	✓	✗	misp-galaxy:mitre-attack-pattern-"Execution through API - T1106"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
25	✓	✗	misp-galaxy:mitre-attack-pattern-"Process Injection - T1055"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
23	✓	✗	misp-galaxy:mitre-attack-pattern-"Spearphishing Attachment - T1133"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
19	✓	✗	misp-galaxy:mitre-enterprise-attack-intrusion-set-"APT28"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
21	✓	✗	misp-galaxy:threat-actor-"APT 29"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
17	✓	✗	misp-galaxy:threat-actor-"APT 30"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
10	✓	✗	misp-galaxy:threat-actor-"Axiom"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷

[Figure 3 Tag list that I used]

16	✓	✗	misp-galaxy:threat-actor-"Equation Group"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
11	✓	✗	misp-galaxy:threat-actor-"Sofacy"				4	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
12	✓	✗	misp-galaxy:threat-actor-"Turla Group"				2	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
20	✓	✗	misp-galaxy:threat-actor-"WildNeutron"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
15	✓	✗	misp-galaxy:tool-"EquationDrug"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
14	✓	✗	misp-galaxy:tool-"Regin"				2	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
22	✓	✗	misp-galaxy:tool-"Trojan, Seaduke"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
13	✓	✗	misp-galaxy:tool-"Turla"				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
26	✓	✗	network_icmp				1	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
9	✓	✗	osint-source-type-"blog-post"				3	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
4	✓	✗	postscript				3	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
7	✓	✗	tip:green				18	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
8	✓	✗	tip:white				42	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷
6	✓	✗	type:OSINT				56	0		<input type="checkbox"/>	⏮ ⏭ ⏰ ⏴ ⏵ ⏶ ⏷

[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.

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

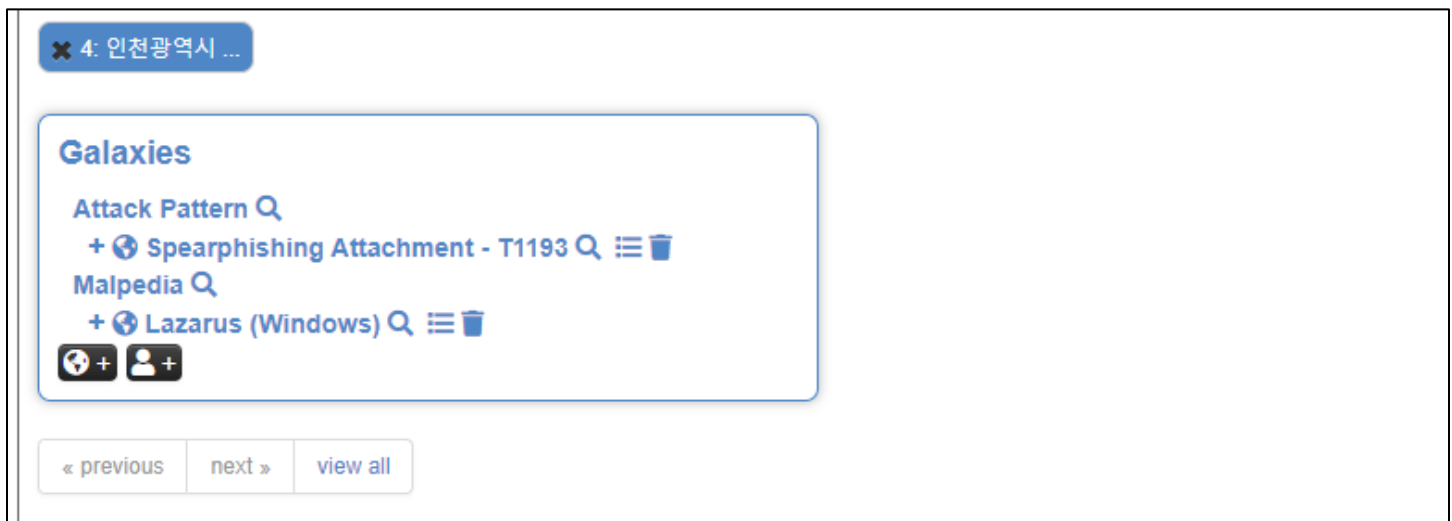
[Figure 5 List event]

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	ORNAME
Owner org	ORNAME
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.



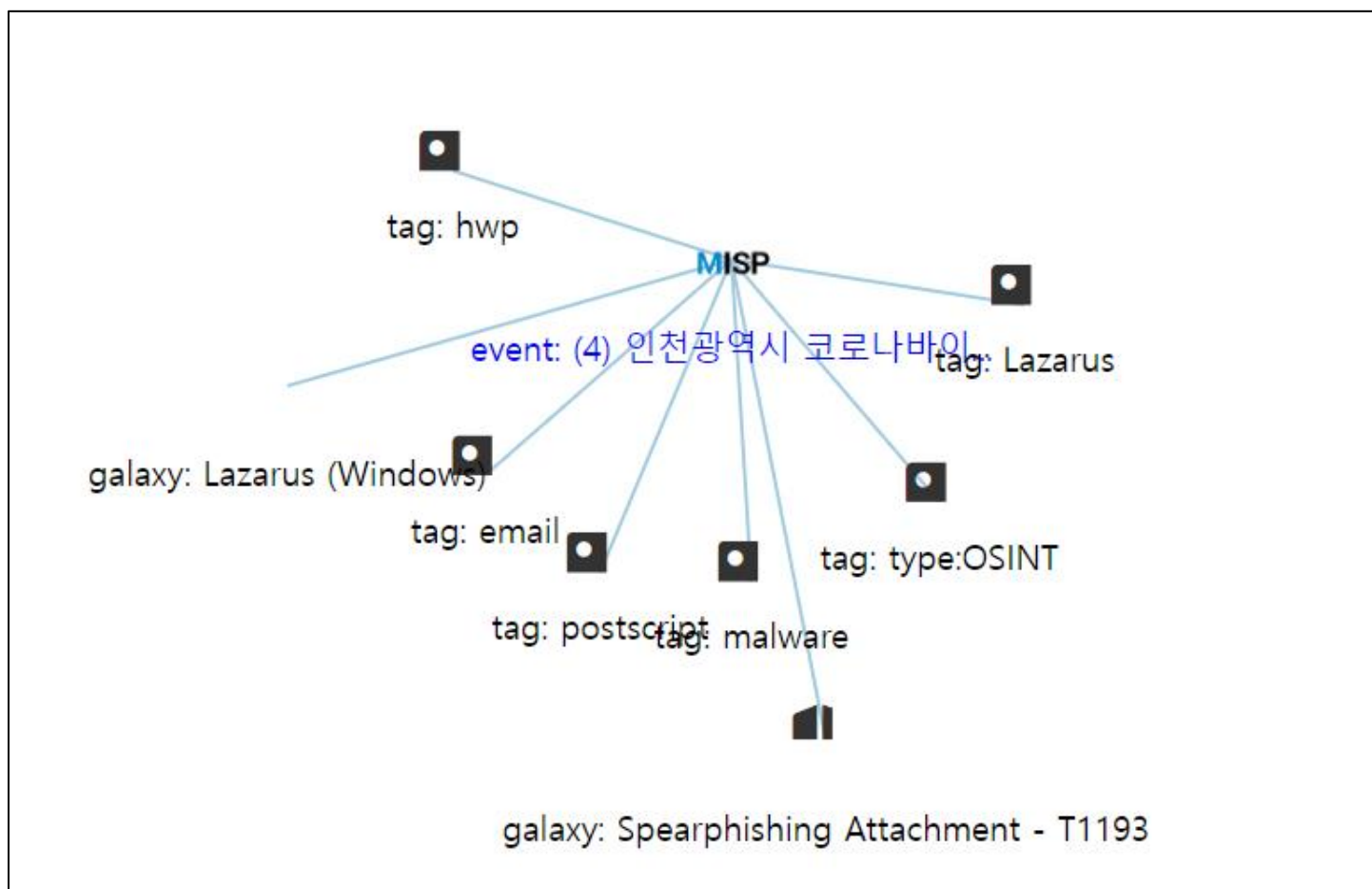
[Figure 7 Galaxies of MISP]

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 C2 References: 0					Inherit		
2022-02-07	Payload delivery	filename: c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b7				<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Other	size-in-bytes: 130560				<input type="checkbox"/>	Inherit	
2022-02-07	Other	entropy: 7.7434274456805				<input type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	md5: bc13fc599bb594bc19ac9e6fde0c28c6			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	sha1: 94b9e7e9f1288fe0dc3a17be4bbca9ac4d0a1faa			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	sha256: c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b7			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	sha512: ac79193e601b5cd7ceca998fd206588f8e61f9b02a2338dcb20542551e755e4bbd1acb35bf38d31c77e16dc9b4213ee08299ba53fc186b89f45ca1233305111			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	malware-sample: c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b7			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-07	Artifacts dropped	mimetype: Hangul (Korean) Word Processor File 5.x			<input type="checkbox"/>	<input type="checkbox"/>	Inherit	
2022-02-07	Payload delivery	ssdeep: 3072:qQrVE67PuDpGAu3e0GriO9R5IAbPksCK:qQBE67hAqO9R5KbXK			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-06	Network activity	url: https://www.afuocolento.it		C2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-06	Payload delivery	filename: skype.jpg		dropped file	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	
2022-02-06	Payload delivery	filename: photo.jpg		dropped file	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	

[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.

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at	Info
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1236	Attack Pattern Q		25		2022-02-10 2022-02-11 04:55:03	RedLine InfoStealer
			<ul style="list-style-type: none"> System Information Discovery - T1002 Q Boot or Logon Autostart Execution - T1547 Q Software Discovery - T1518 Q Query Registry - T1012 Q Windows Management Instrumentation - T1047 Q Command and Scripting Interpreter - T1059 Q User Execution - T1204 Q Signed Script Proxy Execution - T1216 Q Service Stop - T1489 Q Steal Web Session Cookie - T1539 Q Unsecured Credentials - T1552 Q Credentials from Password Stores - T1555 Q 						
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1235		5509	1	2022-02-10	2022-02-10 15:42:40	Phishtank online valid phishing t
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1		0		2022-02-10	2022-02-10 14:20:26	Test
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1234	Surveillance Vendor Q		336		2022-01-30	2022-01-30 10:40:06	OSINT - Cyrox Spyware Indic
			Cyrox Q						Compromise
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1233	Malware Q		1501	3	2022-01-30	2022-01-30 10:21:11	OSINT -
			Pegasus for iOS - 50289 Q						AmnestyTech/Investigations/ma
			Surveillance Vendor Q						07-18_nso/pegasus stlx2
			NSO group Q						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1232	Botnet Q		770		2022-01-28	2022-01-28 14:25:35	Compromised host delivering m
			Mirai Q						(Mirai)
			Tool Q						
			Mirai Q						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1231	Enterprise Attack - Intrusion Set Q		102		2022-01-28	2022-01-28 11:13:31	OSINT - North Korea's Lazarus
			Lazarus Group - G0032 Q						leverages Windows Update clie
			Threat Actor Q						in latest campaign
			Lazarus Group Q						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1230	Misinformation Pattern Q		1345		2022-01-28	2022-01-28 08:28:40	Disinformation - The GRU's gaiz
			Facilitate State Propaganda Q						Russian-speaking websites
			Create Master Narratives Q						
			Create fake websites Q						
			Search Engine Optimization Q						

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

MSFT - MSTIC - Destructive malware targeting Ukrainian organizations	
Event ID	1229
UUID	8cc5335e-915b-4e16-837d-49143e6987b4
Creator org	CIRCL
Tags	
Date	2022-01-16
Threat Level	? Undefined
Analysis	Completed
Distribution	All communities
Info	MSFT - MSTIC - Destructive malware targeting Ukrainian organizations
Published	Yes (2022-02-10 15:41:14)
#Attributes	20 (7 Objects)
First recorded change	2022-01-16 15:21:45
Last change	2022-01-16 15:59:12
Modification map	
Sightings	0 (0) - restricted to own organisation only.

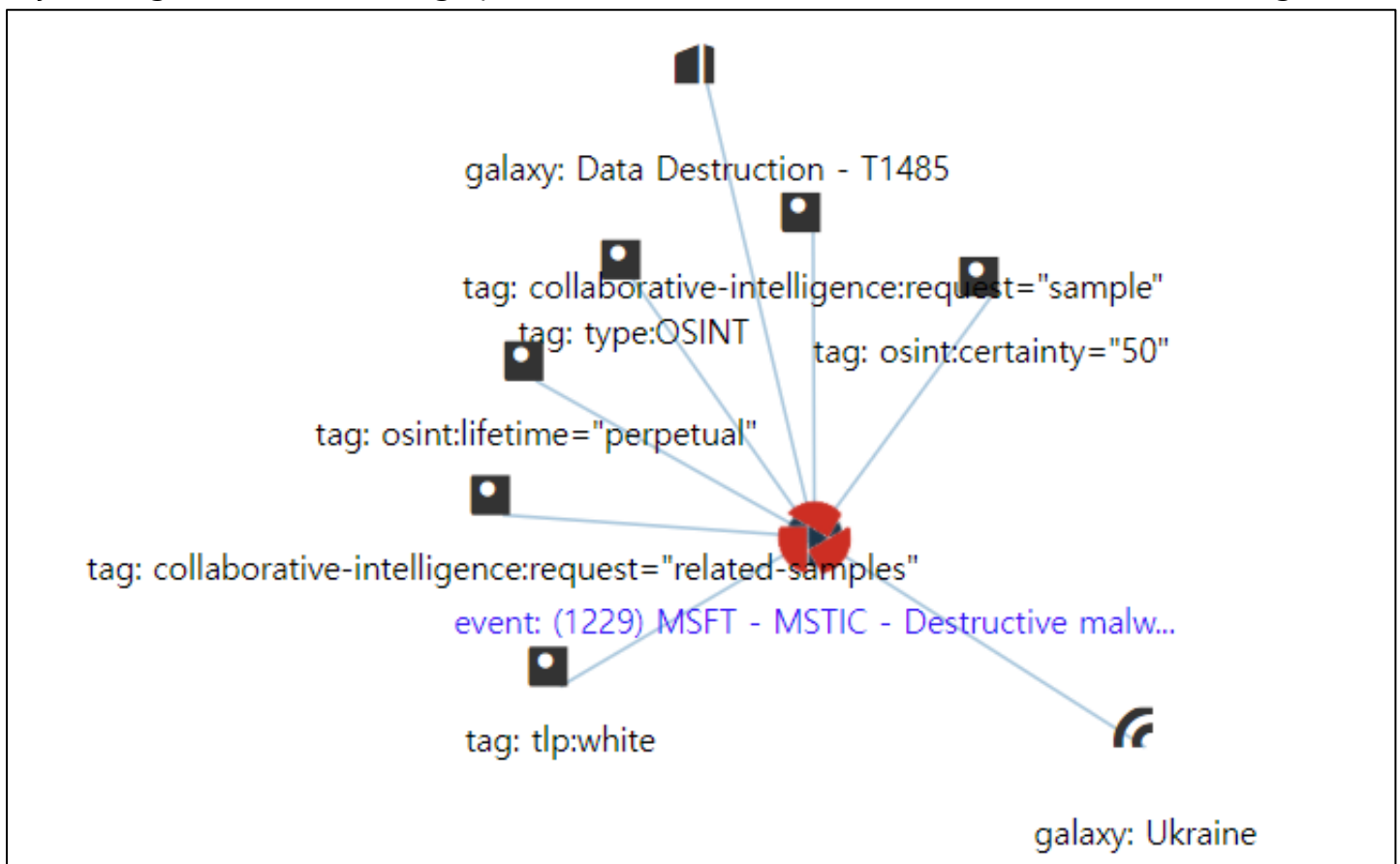
[Figure 11 Malware targeting Ukrainian organizations]

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	a196cbb8fcb97fb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Payload delivery	filename: filename	stage1.exe	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Other	state: text	Malicious	<input type="checkbox"/>	<input type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Object name: file [🔍]	References: 0	Hash of stage2.exe	Inherit			
2022-01-16	Payload delivery	sha256: sha256	dcbbae5a1c91dbbb7dc6dc5dd1eb1169f5329958d38b58c3f69384081c9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Payload delivery	filename: filename	stage2.exe	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Other	state: text	Malicious	<input type="checkbox"/>	<input type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Object name: command-line [🔍]	References: 0					
2022-01-16	Other	value: text	cmd.exe /Q /c start c:\stage1.exe 1> %127.0.0.1\ADMIN___[TIMESTAMP] 2>&1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit	🔍 (0/0/0)
2022-01-16	Other	text	Address: 1AVNM68g6PGPFcJufKATa4VLnzg8ptvBalance: 0.0001185800 BTC (+0.0001185800 BTC / -0.0000000000 BTC)Transaction: 1 (previewing up to 5 most recent)=====14 Jan 2022 14:01:25 UTC 0.00011858 BTC 5.11 USD 4.48 EUR	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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]