### INSTALL GUIDE

# ·III · Recorded Future®

Recorded Future® for MISP, v2.0

### **Table of Contents**

Overview	3
Prerequisites	3
Input your API Token	3
Software Versions	3
MISP Extension Module Installed	3
Enable Enrichment Module	4
Configuring Feeds	5
Setting Up a Feed	5
Importing All Feeds In Bulk	9
Creating an Event from a Feed	9
IDS Flag	11
Troubleshooting	11
Extension Module	11
APPENDIX A: Supported Security Control Feeds	13
APPENDIX B: Supported IP RiskLists	14
APPENDIX C: Supported DOMAIN RiskLists	15
APPENDIX D: Supported URL RiskLists	16
APPENDIX E: Supported HASH RiskLists	17
APPENDIX F: Supported Vulnerability RiskLists	18
APPENDIX G: Supported Threat Lists	19

### **Overview**

This guide describes the steps involved in integrating Recorded Future as both a Feed and Extension Module within MISP. Please note that expansive permissions are required within MISP to complete this integration.

Please contact your MISP administrator if you have insufficient permissions.

### **Prerequisites**

#### Input your API Token

See Managing API Tokens on the Support Site for more information.

#### **Software Versions**

MISP 2.4.x

#### **MISP Extension Module Installed**

To confirm that the misp-modules services has been installed correctly and is running, follow these steps:

1. Go to Administration > Server Settings & Maintenance



#### 2. Enter the Diagnostics tab

Home Event Actions	Galaxies Input Filters Global Actions Sync Actions A	dministration Audit	
Add User List Users	Server Settings & Maintenance		
Pending registrations	Overview MISP settings (20) Encryption settings (5) Proxy	y settings (5) Security settings (1) Plugin settings (327 \Lambda) Diagnostics	lanage files 🔹 Workers 🛓
User settings	Test	Value	Description
Contact Lieure	Overall health	Critical, your MISP instance requires immediate attention.	The overall health of your instance depends on the
Contact Osers	Critical settings incorrectly or not set	2 incorrect settings.	MISP will not operate correctly or will be unsecure
Add Organisation	Recommended settings incorrectly or not set	275 incorrect settings.	Some of the features of MISP cannot be utilised ur
List Organisations	Optional settings incorrectly or not set	81 incorrect settings.	There are some optional tweaks that could be don
	Critical issues revealed by the diagnostics	0 issues detected.	Issues revealed here can be due to incorrect direct
Add Role	To edit a setting, simply double click it.		
Server Settings & Maintenance			

3. Scroll down to the Module System section and confirm the status is OK



### **Enable Enrichment Module**

Running any type of extension module in MISP requires the misp-modules service to be installed. Instructions for installing the misp-modules service can be found in the official MISP modules documentation here. Installing the misp-modules service automatically installs the Recorded Future expansion module.

To confirm that the Recorded Future enrichment module is installed, follow these steps:

1. Go to Administration > Server Settings & Maintenance

Home Event Actions	Galaxies Input Filters Global Actions Sync Actions	Administration Audit	
List Events	Events	List Users	
Add Event	Events	List User Settings	
Import from		Set User Setting	
REST client	« previous next »	Add User	
		Contact Users	
List Attributes	Q My Events Org Events	User Registrations	
Search Attributes	Published Creator org Owner org Id Clu	List Organisations	#Attr. #Corr. Email
View Proposals	ORGNAME ORGNAME 1	Add Organisations	2 admin@admin.test
Events with proposals			
View delegation requests	Page 1 of 1, showing 1 records out of 1 total, starting on record 1, $\epsilon$	List Roles	
		Add Roles	
Export	« previous next »		
Automation		Server Settings & Maintenance	
		Jobs	
		Scheduled Tasks	
		Event Block Rules	

2. Enter the Plugin settings tab and expand the Enrichment settings

Home Event Actions	Galaxies Input Filters Global Actions Sync Actions Administration Audit
Add User	Convex Cattings & Maintenance
List Users	Server Settings & Maintenance
Pending registrations	Overview MISP settings (20) Encryption settings (5) Proxy settings (5) Security settings (1) Plugin settings (327 \Lambda) Diagnostics Manage files 🔶 Worke
User settings Set Setting	Enrichment
Contact Users	Import
Add Organisation	Export
List Organisations	Cortex
Add Role	Sightings
	RPZ
Server Settings & Maintenance	Kalka
Inbox	ZeroMQ

3. Scroll down the expanded enrichment settings and look for the Recorded Future specific settings (such as Plugin.Enrichment\_recordedfuture\_enabled)

Recommended Plugin.Enrichment_cytomic_orion_upload_tag	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_cytomic_orion_delete_tag	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_cytomic_orion_upload_ttlDays	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_cytomic_orion_upload_threat_level_id	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_cytomic_orion_limit_upload_events	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_cytomic_orion_limit_upload_attributes	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_censys_enrich_enabled false	Enable or disable the censys_enrich module.	Valu
Recommended Plugin.Enrichment_censys_enrich_restrict No organisation selected.	Restrict the censys_enrich module to the given organisation.	Valu
Recommended Plugin.Enrichment_censys_enrich_api_id	Set this required module specific setting.	Valu
Recommended Plugin.Enrichment_censys_enrich_api_secret	Set this required module specific setting.	Vak
Recommended Plugin.Enrichment_trustar_enrich_enabled false	Enable or disable the trustar_enrich module.	Val
Recommended Plugin.Enrichment_trustar_enrich_restrict No organisation selected.	Restrict the trustar_enrich module to the given organisation.	Val
Recommended Plugin.Enrichment_trustar_enrich_user_api_key	Set this required module specific setting.	Val
Recommended Plugin.Enrichment_trustar_enrich_user_api_secret	Set this required module specific setting.	Val
Recommended Plugin.Enrichment_trustar_enrich_enclave_ids	Set this required module specific setting.	Val
Recommended Plugin.Enrichment_recordedfuture_enabled true	Enable or disable the recorded/luture module.	
Recommended Plugin.Enrichment_recordedfuture_restrict No organisation selected.	Restrict the recordedfuture module to the given organisation.	Vak
Recommended Plugin.Enrichment_recordedfuture_token	Set this required module specific setting.	

### **Configuring Feeds**

The Recorded Future MISP Feeds make use of the built in feeds functionality in MISP to allow anyone with a Recorded Future API key to download different lists of indicators and/or vulnerabilities associated with specific Recorded Future risk rules.

#### Setting Up a Feed

1. Go to Sync Actions  $\rightarrow$  List Feeds

Home Event Actions	Galaxies Input Filters Global Actions	Sync Actions Administration	Audit	
List Events Add Event	Events	Import Server Settings List Servers		
Import from REST client	« previous next »	List Feeds List Feed Caches Search Feed Caches List SightingDB Connections		
Search Attributes	Published Creator org Owner of	List Communities	Tags	#Attr. #Corr. E
View Proposals		E 1		4 a

#### 2. Go to Add Feed

Home Event Actions	Galaxies	Input F	lters Globa	Actions S	ync Actions Administr	ration Aud	lit			
List Feeds	-									
Search Feed Caches	⊢ee	ds								
Add Feed ⊱	Generat	e feed looku	o caches or fetch	n feed data (ena	bled feeds only)					
Import Feeds from JSON										
Feed overlap analysis matrix	Load d	efault feed m	etadata	ache all feeds	Cache freetext/CSV feeds	Cache MISP	P feeds Feto	ch and store all fe	eed data	
Export Feed settings	« prev	vious nex	t »	All feeds	Fnahled feeds					
		Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL
		1	×	×	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/ osint
1		2	×	×	The Botvrij.eu Data	misp	Botvrij.eu	,	network	https://www.botvrij.eu/da osint
	Page 1	of 1, showing	2 records out of	f 2 total, starting	on record 1, ending on 2					
	« prev	vious nex	tt »							
	1									

#### 3. This brings you to the feed configuration page

Home Event Actions	
List Feeds Search Feed Caches	Add MISP Feed
Add Feed Import Feeds from JSON Feed overlap analysis matrix Export Feed settings	Add a new MISP feed source.  Enabled Caching enabled Caching enabled Name
	Feed name
	Provider
	Name of the content provider
	Input Source
	Network
	URL
	URL of the feed
	Source Format MISD Energy
	Any headers to be passed with requests (for example: Authorization)
	Line break separated list of headers in the "headername: value" format
	Add Basic Auth
	Distribution
	All communities •
	Default Tag
	None
	Filter rules: Modify
	Add

4. Toggle the Enabled box



<u></u>

6. Enter feed URL (this is what decides what feeds you will download). A list with all available feeds is available in the Appendix Section.

URL

https://api.recordedfuture.com/gw/misp/feed/domain\_recentCovidLure

Any headers to be passed with requests (for example: Authorization)	
X-RFToken:	
	1

8. Press Submit once the feed has been configured

Home Event Actions	Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API	*	Misp-demo 🖂	
	Name			
	Feed name			
	Provider			
	Name of the content provider			
	Input Source			
	Network 🗸			
	URL			
	URL of the feed			
	Source Format			
	MISP Feed ~			
	Any headers to be passed with requests (for example: Authorization)			
	Line break separated list of headers in the "headername: value" format			
	Add Basic Auth			
	Distribution			
	All communities ~			
	Default Tag			
	None ~			
	Filter rules:			
	Modify			
	Submit			

#### Importing All Feeds In Bulk

1. Recorded Future provides a dedicated JSON file to import all available feeds into MISP. The file is available at the following URL: https://api.recordedfuture.com/gw/misp/feed/import

The file can be downloaded by running the following command, where your Recorded Future token needs to be entered:

#### curl -X GET -H "Content-Type: application/json" -H "accept: application/json" -H "X-RFToken: XXX" 'https://api.recordedfuture.com/gw/misp/feed/import'

2. To import the Recorded Future feeds, select the Import Feeds from JSON option on the side menu. Paste MISP feed metadata JSON, that was previously downloaded, into the text box and click the Add button.

3. Edit the created feed and enable the ones that are relevant for the organization.

Add a new MISP feed source.	
Enabled	Caching enabled
Lookup visible	

4. For each on of the enabled feed and enter a Recorded Future API token in the format: X-RFToken:abc123\*\*\*\*\*\*\*\*\*



#### Creating an Event from a Feed

1. Click the fetch all events button on the newly added feed

	Defa	ult feeds	Custom feet	ds All feeds	Enable	ed feeds										Enter val	ue to se	arch	Filter
8	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions
6	1	×	×	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	×	×	×	All communiti	15	×	Not cached	08.10
6	2	×	×	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/leed-osint		Feed not enabled	×	×	×	All communiti	25	×	Not cached	Q 🗷 📫 🕰
C	3	~	×	Recent COVID-19- Related Domain Lure: Malicious	misp	Recorded Future		network	https://api.recordedhuture.com/mispfeedidomain_recentCovidSpam	X. RFToken		×	×	×	All communiti	rs	×	Not cach id	오 옷

2. If the feed has been configured correctly it will start downloading

	Home	Event Actions	Galaxies	Input Filters	Global Actions	Sync Actions	Administration	Audit	
1	Pull queued for background execution.								
Lis	st Feeds		· .						
Se	earch Feed	Caches	Feed	S					
Ac	ld Feed		Generate f	eed lookup cache	es or fetch feed data	(enabled feeds on	ly)		

#### 3. Go to Event Actions $\rightarrow$ List Events

Home	Event Actions Galaxies	Input Filters Global Actions Sync Actions Administration Audit
List Feeds	List Events 🔚	
Search Feed	Add Event	IS
Add Feed	List Attributes	feed lookup caches or fetch feed data (enabled feeds only)
Import Feeds	Search Attributes	
Feed overlap	REST client	ault feed metadata Cache all feeds Cache freetext/CSV feeds Cache MISP feeds Fetch and store all feed data
Export Feed	View Proposals Events with proposals	sus next »
	View delegation requests	ult feeds Custom feeds All feeds Enabled feeds
-		Enabled Caching Name Format Provider Org Source URL

4. The event created by the feed should now be present in the list of events (it can take a few minutes for the event to populate)

Home Event Actions	
List Events Add Event	Events
Import from REST client	c provide a non-section of the section of the se
List Attributes	Q My Events Org Events
Search Attributes	Published Creator org Dwner org Id Clusters Tags #Attr. #Corr. Email Date Info
View Proposals	K RF ORGNAME 2020-07-10 Recorded Future - domain - Recent COVID-19-Related Domain Lute: Suspicious
Events with proposals View delegation requests	Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1
Export	« grevious next »
Automation	

Home Event Actions	Galaxies Input Fi	ilters Global Action	ns Sync Actions Administration	Audit					*	MISP Adr	min 🖂 Log out
	+ = =	X Scope toggle	Teleted Lat Decay score	SightingDB O Context V Related Tags V Filtering tool					Enter v	alue to search	¢ ×
	Date † O	rg Category	ype Value	Tags	Galaxies C	omment Correlate	Related Feed Events hits	IDS I	Distribution	Sightings Activi	ity Actions
	2020-07-10	Network activity	lomain corona-vaccine.world Q	recorded future risk-values "Recent COVID 19 Related Donnain Later: Suspicious"      recorded future risk-values "Historical Typosograd Similarly - Typo or Homograph"     recorded future risk-values "Historical Typosograd Similarly - Typo or Homograph"     recorded future risk-values "Historical Typosograph"	Ø+ ≗+ ×	×		8	inherit	순 약 분 (ololo)	*****
	2020-07-10	Network activity	lomain cpanel.coronavirustiji.online 🍳	© recorded-future:risk-score="25" ≥ © recorded-future:risk-rule="Recent COVID-19-Related Domain Lure: Suspicious" ≥ ⊙+ ≜+	<b>⊗</b> + <b>≗</b> +			8	Inherit	i⇔ i⊋ ≯ (0/0/0)	*****
	2020-07-10	Network activity	lomain ipv6.muarajawacovid19.xyz 🔍	<sup>®</sup> recorded-future:risk-score="25" X <sup>®</sup> recorded-future:risk-suize="Recent COVID-19-Related Domain Lure: Suspicious" X	<b>⊗</b> + <b>±</b> +	×		8	Inherit	ið \$\$ ₽ (0/0/0)	* • • • • • •
	2020-07-10	Network activity	lomain www.covid-19testkit.xyz 🔍	<sup>®</sup> recorded-future:risk-score="25" X <sup>®</sup> recorded-future:risk-rule="Recent COVID-19-Related Domain Lure: Suspicious" X <sup>®</sup>	<b>⊗</b> + <b>≗</b> +	×		8	Inherit	ið 😳 🖌 (0/0/0)	* • 1 * 6 1
	2020-07-10	Network activity	iomain cpanel.amazon-updatefor- covid19.gize.com Q	<sup>®</sup> recorded-future:risk-score="22" × <sup>®</sup> recorded-future:risk-rule="Recent COVID-19-Related Domain Lure: Suspicious" × <sup>®</sup>	<b>⊗</b> + <b>≗</b> +	×		8	Inherit	ic) © ⊁ (0/0/0)	
	2020-07-10	Network activity	lomain mail.coronavirusnow.online Q	O recorded-future.risk-score="25" X	(3) + ▲ +	×		8	Inherit	ić © ⊁ (0/0/0)	*****
	2020-07-10	Network activity	lomain cpcontacts.amazon-update- covid19-germany.glize.com Q	<sup>®</sup> recorded-future:risk-score="25" X <sup>®</sup> recorded-future:risk-sube="Recent COVID-19-Related Domain Lure: Suspicious" X <sup>®</sup>	<b>⊗</b> + <b>≗</b> +	×		8	Inherit	ið 😳 🖌 (0/0/0)	
	2020-07-10	Network activity	lomain techvscovid19.site 🔍	3 recorded-future:risk-score="25" x 3 recorded-future:risk-rule="Recert COVID-19-Related Domain Lure: Suspicious" x ⊗+ L+	<b>⊗</b> + <b>≗</b> +	×		8	Inherit	ið © ⊁ (0/0/0)	******
	2020-07-10	Network activity	lomain covid- 19commercialcleaning.services @	© recorded-future.risk-score="25" k © recorded-future.risk-sule="Recent COVID-19-Related Domain Lure: Suspicious" X ⊙+ =+	<b>⊗</b> + <b>≗</b> +	×		8	Inherit	ið i⊋ ⊁ (0/0/0)	
	2020-07-10	Network activity	lomain www.coronavivus.online 🔍	🔇 recorded-future:risk-score="25" 💈 😚 recorded-future:risk-rule="Record COVID-19-Related Domain Lure: Suspicious" 🖬 🚱 🔒 💵	<b>⊗</b> + <b>≗</b> +	8		8	Inherit	ich ⊈ ≯ (0/0/0)	•••••

5. Clicking the event will show all the attributes (indicators) included in the specific feed

6. Each attribute is tagged with Recorded Future risk scoring and triggered risk rules

2020-07-10	Network activity	domain	corona-vaccine.world Q	Image: Strategy and Strate
2020-07-10	Network activity	domain	cpanel.coronavirusfiji.online 🍳	recorded-future:risk-score="25" x         recorded-future:risk-rule="Recent COVID-19-Related Domain Lure: Suspicious" x         + <td< td=""></td<>
2020-07-10	Network activity	domain	ipv6.muarajawacovid19.xyz 🔍	Image: State of the second
2020-07-10	Network activity	domain	corona-vaccine.world Q	<ul> <li>recorded-future:risk-rule="Recent COVID-19-Related Domain Lure: Suspicious" x</li> <li>recorded-future:risk-rule="Historical Typosquat Similarity - Typo or Homograph" x</li> <li>recorded-future:risk-rule="Newly Registered Certificate With Potential for Abuse - Typo or Homograph" x</li> </ul>

### **IDS Flag**

According to the MISP core format data standard, the to\_ids flag represents whether the attribute is meant to be actionable. The following list of feeds will have the to\_ids flag enabled by default which we recommend to be used for detection or correlation actions:

- Default Domain Risk List: Risk Score 90+
- Recent C&C DNS Name
- Actively Communicating C&C Server
- Default IP Risk List: Risk Score 90+
- Recently Active Targeting Vulnerabilities in the Wild
- SCF C2 Communicating Ips
- SCF Weaponized Domains
- SCF Exploits Itw Hashes
- Validated C&C Server

### Troubleshooting

#### **Extension Module**

If you can't find the Recorded Future app settings this means that you either have an older version of the misp-modules service installed. To manually install the Recorded Future expansion module on top of an existing misp-modules installation, follow these steps:

1. Locate the misp-modules directory on your MISP server

# root@misp-int-dev-01:/opt/misp/misp-modules# pwd /opt/misp/misp-modules

2. Copy the Recorded Future script into the expansion modules folder

root@misp-int-dev-01:/op	ot/misp/misp-modules# cp	<pre>/tmp/recordedfuture.py misp_modul</pre>	les/modules/expansio	n/	
root@misp-int-dev-01:/op	ot/misp/misp-modules# ls	<pre>misp_modules/modules/expansion/</pre>			
apiosintds.py	cve_advanced.py	google_search.py	macvendors.py	ransomcoindb.py	urlhaus.py
apivoid.py	cve.py	greynoise.py	malwarebazaar.py 🖕	ch] py	urlscan.py
assemblyline_query.py	cytomic_orion.py	hashdd.py	<pre>module.py.skeleton</pre>	recordedfuture.py	virustotal_public.py
assemblyline_submit.py	dbl_spamhaus.py	hibp.py	ocr_enrich.py	reveracuia.py	virustotal.py
backscatter_io.py	_dnsdb_query	initpy	ods_enrich.py	securitytrails.py	_vmray
bgpranking.py	dns.py	intel471.py	odt_enrich.py	shodan.py	vmray_submit.py
<pre>btc_scam_check.py</pre>	docx_enrich.py	intelmq_eventdb.py.experimental	onyphe_full.py	sigma_queries.py	vulndb.py
btc_steroids.py	domaintools.py	ipasn.py	onyphe.py	sigma_syntax_validator.py	vulners.py
censys_enrich.py	eql.py	іргер.ру	otx.py	sophoslabs_intelix.py	whois.py
circl_passivedns.py	eupi.py	joesandbox_query.py	passivetotal.py	sourcecache.py	wiki.py
circl_passivessl.py	farsight_passivedns.py	joesandbox_submit.py	pdf_enrich.py	<pre>stix2_pattern_syntax_validator.py</pre>	xforceexchange.py
countrycode.py	geoip_asn.py	lastline_query.py	pptx_enrich.py	threatcrowd.py	xlsx_enrich.py
crowdstrike_falcon.py	geoip_city.py	lastline_submit.py	qrcode.py	threatminer.py	yara_query.py
cuckoo_submit.py	geoip_country.py	macaddress_io.py	_ransomcoindb	trustar_enrich.py	yara_syntax_validator.py
root@misp-int-dev-01:/op	ot/misp/misp-modules#				

4. Stop the misp-modules service

root@misp-int-dev-01:/opt/misp/misp-modules# service misp-modules stop
root@misp-int-dev-01:/opt/misp/misp-modules#

5. Re-install the misp-modules (command depends on your environment and distribution,

see misp-modules documentation)

root@misp-int-dev-01:/opt/misp/misp-modules# /opt/misp/venv/bin/pip3.6 install -I -r REQUIREMENTS

root@misp-int-dev-01:/opt/misp/misp-modules# /opt/misp/venv/bin/pip3.6 install .

6. Start the misp-modules service

root@misp-int-dev-01:/opt/misp/misp-modules# service misp-modules start
root@misp-int-dev-01:/opt/misp/misp-modules#

### **APPENDIX A: Supported Security Control Feeds**

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
SCF - C2 Communicating lps	https://api.recordedfuture.com/gw/ misp/feed/scf_c2_communicating_ips	Very Malicious	Recorded Future Internet Scanning collects live information about internet hosts and Network Traffic Analysis observes the midpoint between the adversary and their victims as they build, stage, and launch attacks. The Command and Control dataset fuses those two methods to identify and track IPs that we have scanned as positive C2 and then observed communications to understand how the C2 is interacting with infected machines as well as being controlled by the adversary. This method has been used to produce unique Intelligence where we can observe and track Command and Control activity at Internet scale.
SCF - Weaponized Domains	https://api.recordedfuture.com/gw/ misp/feed/scf_weaponized_domains	Very Malicious	Recorded Future Domain Analysis observes the entire Domain Weaponization lifecycle from Domain registration, resolution to IP address, Certificate provisioning, Mail Server configuration, and URL propagation to assess risk of malicious activity. There are pockets of the Internet that allow adversaries to enjoy economies of scale due to free, anonymous, and unmonitored services. The Weaponized Domains and URLs datasets identifies domains and URLs with live activity in those Service Providers and connects them with a Bad Actor threat model to present a set of Domains that have a risk of being malicious even before a URL has ever been seen in the wild and as well as a set of Domains and URLs that been verified as malicious.
SCF - Exploits Itw Hashes	https://api.recordedfuture.com/gw/ misp/feed/scf_exploits_itw_hashes	Very Malicious	Recorded Future Malware Hunting analyzes billions of malware samples to identify important samples that have static and behavioral characteristics that make them important to Intelligence and Security teams. The Exploits in the Wild dataset identifies SHA-256 hashes and vulnerabilities where we have observed recent malware activity in the wild. This technique uses submissions to popular malware repositories as a rough proxy for propagation in the wild since we believe that the majority of the submission activity to malware repositories is done automatically by security tools and Antivirus vendors as samples are discovered on endpoints, in email, or on networks. This method has been used to produce unique Intelligence where we have observed Malware known to exploit Vulnerabilities activity in the Wild (ITW).

### **APPENDIX B: Supported IP Risk Lists**

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default IP Risk List: Risk Score 90+	https://api.recordedfuture.co m/gw/ misp/feed/ip_default	Very Malicious	Indicators with a Risk Score of 90 and higher
			Observing C2 communications with infected machines or adversary control by Recorded Future Network Traffic Analysis
Actively Communicating C&C	https://api.recordedfuture.co m/gw/ misp/feed/ip_recentActiveCnc	Verv Malicious	[ATT&CK] Tactic: Command and Control
Server			Mitigated to Suspicious level by whitelisting of the IP Address. Also mitigated to Suspicious level by metadata published in the threat list indicating low confidence in the finding.
Validated C&C Server	https://api.recordedfuture.com /gw/	Very Malicious	Recently detected or reported C2 that was further validated as a running C2 by Insikt Group using proprietary methodology.
	misp/teed/ip_recentValidatedCnc		[ATT&CK] Tactic: Command and Control
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/ misp/feed/ip_recentAnalystNote	Malicious	Primary Indicator in an Insikt Group Note [ATT&CK] Tactic: Command and Control
Phishing Host	https://api.recordedfuture.com/gw/	Malicious	Reported as host of an active phishing URL [ATT&CK] Technique: Spear Phishing Link
	misp/feed/ip_phishingHost		Mitigated to Suspicious level by whitelisting of the IP Address

### **APPENDIX C: Supported DOMAIN RiskLists**

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Domain Risk List: Risk Score 90+	https://api.recordedfuture.com/gw/ misp/feed/domain_default	Very Malicious	Indicators with a Risk Score of 90 and higher
Recent C&C DNS Name https://api.recordedfuture.com/gw/ misp/feed/domain_recentCncSite		Very Malicious	DNS Name associated with malicious Command and Control [ATT&CK] Technique: Application Layer Protocol, DNS
Recently Detected https://api.recordedfuture. Malware Operation recentMalwareSiteDetected		Malicious	This rule provides high confidence that the domain distributed or was connected to malware. [ATT&CK] Tactic: Initial Access, Tactic: Command and Control
Recently Detected Phishing Techniques	https://api.recordedfuture. com/gw/misplfeed/domain_ recentPhishingSiteDetected	Malicious	This rule provides high confidence that the domain was involved in phishing activities. [ATT&CK] Technique: Spearphishing Link
Recently Reported Fraudulent Content	https://api.recordedfuture. com/gw/misp/feed/domain_ recentFraudulentContent	Malicious	Domain has been reported to convince victims to send money/bitcoin for items that look legitimate. [ATT&CK] Technique: Spearphishing via Service
Recently Active Weaponized Domain	https://api.recordedfuture. com/gw/misp/feed/domain_ recentWeaponizedDomain	Malicious	Domain activity observed in connection to Bad Actor tracked by Recorded Future Domain Analysis [ATT&CK] Technique: Spearphishing Link, Tactic: Command and Control
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/ misp/feed/domain_recentAnalystNote	Malicious	Involved in an Insikt Group Note [ATT&CK] Tactic: Initial Access, Tactic: Command and Control, Technique: Malicious Link
Recent COVID-19-Related Domain Lure: Malicious	https://api.recordedfuture.com/gw/ misp/feed/domain_recentCovidLure	Malicious	Domain with COVID-19 related naming characteristics which is convicted as malicious by technical analysis. [ATT&CK] Tactic: Initial Access, Tactic: Execution
Recent Phishing Lure: Malicious	https://api.recordedfuture. com/gw/misp/feed/domain_ recentPhishingLureMalicious	Malicious	This rule provides high confidence conviction for active domains that appear to be phishing lures. This is a recently changed domain that contains an internet service brand names within the last 90 days. [ATT&CK] Tactic: Initial Access, Tactic: Execution

### **APPENDIX D: Supported URL RiskLists**

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default URL Risk List: Risk Score 70+	https://api.recordedfuture.com/gw/ misp/feed/url_default	Very Malicious & Malicious	Indicators with a Risk Score of 70 and higher
Recently Detected Malware Distribution	https://api.recordedfuture. com/gw/misp/feed/url_ recentMalwareSiteDetected	Malicious	Site distributes malware [ATT&CK] Technique: User Execution
Recently Detected Phishing Techniques	https://api.recordedfuture. com/gw/misp/feed/url_ recentPhishingSiteDetected	Malicious	Site contains logos, images, text, and other attributes to steal user credentials. [ATT&CK] Technique: Spearphishing Link
Recently Reported by DHS AIS	https://api.recordedfuture.com/gw/ misp/feed/url_recentDhsAis	Malicious	Reported by DHS Automated Indicator Sharing
Recently Reported by Insikt Group	https://api.recordedfuture.com/gw/ misp/feed/url_recentAnalystNote	Malicious	Recently Reported as a Threat in Insikt Group Reporting
Active Phishing URL	https://api.recordedfuture.com/gw/ misp/feed/url_phishingUrl	Malicious	URL reported as an active phish [ATT&CK] Technique: Spearphishing Link

### APPENDIX E: Supported HASH RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Hash Risk List: Risk Score 80+	https://api.recordedfuture.com/gw/ misp/feed/hash_default	Very Malicious & Malicious	Indicators with a Risk Score of 80 and higher
Recently Active Targeting Vulnerabilities in the Wild	https://api.recordedfuture.com/gw/ misp/feed/hash_recentActiveMalware	Malicious	Malware known to exploit a vulnerability observed in the wild by Recorded Future Malware Hunting in the last 28 days [ATT&CK] Tactic: Execution
Observed in Underground Virus Testing Sites	https://api.recordedfuture. com/gw/misp/feed/hash_ observedMalwareTesting	Malicious	Potentially undetectable malware observed on darkweb, collected from No-Distribute Scanners [Pre-ATT&CK] Technique: Test malware to evade detection
Malware SSL Certificate Fingerprint	https://api.recordedfuture.com/gw/ misp/feed/hash_malwareSsl	Malicious	Fingerprint hash for an SSL Certificate that is linked to Malware [Pre-ATT&CK] Technique: SSL certificate acquisition for domain
Reported by Insikt Group	https://api.recordedfuture.com/gw/ misp/feed/hash_analystNote	Malicious	Involved in an Insikt Group Note [ATT&CK] Tactic: Execution, Tactic: Persistence

### APPENDIX F: Supported Vulnerability RiskLists

SCF	MISP URL	SEVERITY	DESCRIPTION AND MITIGATING FACTORS
Default Vuln Risk List: Risk Score 90+	https://api.recordedfuture.com/gw/ misp/feed/vulnerability_default	Very Critical	Vulnerabilities with a Risk Score of 90 and higher
Exploited in the Wild by Recently Active Malware	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ recentMalwareActivity	Very Critical	Malware known to exploit a vulnerability recently observed in the wild by Recorded Future Malware Hunting or by Recorded Future Vulnerability Analysis [ATT&CK] Tactic: Execution
NIST Severity: Critical	https://api.recordedfuture.com/gw/ misp/feed/vulnerability_nistCritical	Critical	Assigned a Critical CVSS score in the National Vulnerability Database [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs Note: For normalization, Risk Scoring assumed the minimum Temporal Score for CVSSv3 since our other Risk Rules will provide the Temporal component
Exploited in the Wild by Malware	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ malwareActivity	Critical	Malware known to exploit a vulnerability observed in the wild by Recorded Future Malware Hunting [ATT&CK] Tactic: Execution
Recent Verified Proof of Concept Available Using Remote Execution	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ recentPocVerifiedRemote	Critical	Verified Proof of Concept exploit code is available using Remote Execution protocols
Historically Exploited in the Wild by Malware	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ historicMalwareActivity	High	Malware known to exploit a vulnerability historically observed in the wild by Recorded Future Malware Hunting [ATT&CK] Tactic: Execution
Recently Reported by Insikt Group	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ recentAnalystNote	High	Insikt reporting on the severity, threats, or actors leveraging the Vulnerability [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs
NIST Severity: High	https://api.recordedfuture.com/gw/ misp/feed/vulnerability_nistHigh	High	Assigned a High CVSS score in the National Vulnerability Database [Pre-ATT&CK] Technique: Research relevant vulnerabilities/CVEs Note: For normalization, Risk Scoring assumed the minimum Temporal Score for CVSSv3 since our other Risk Rules will provide the Temporal component
Recent Verified Proof of Concept Available	https://api.recordedfuture.com/ gw/misp/feed/vulnerability_ recentPocVerified	High	SCF - Exploits Itw Hashes

### **APPENDIX G: Supported Threat Lists**

List Name	MISP URL	ІОС Туре	DESCRIPTION AND MITIGATING FACTORS
Log4j Related Scanners	https://api.recordedfuture. com/gw/misp/feed/custom_ip_ log4jRelatedScanners	IP	This list includes all servers Recorded Future has observed probing for log4j instances to identify vulnerable systems. This includes legitimate security vendors attempting to identify vulnerable systems as well as malicious activity.
Log4j Malicious Scanners	https://api.recordedfuture. com/gw/misp/feed/custom_ip_ log4jMaliciousScanners	IP	This list contains IPs that have been observed scanning for CVE-2021-44228 (Log4Shell) with potential malicious activity. It includes scanners that have been observed attempting to directly load payloads and repetitively send exploit payloads without providing indications of who is conducting the activity. Follow on payloads from these IPs have included coin miners, backdoors, and IOT botnets.

#### ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,700 businesses and government organizations across more than 75 countries.

www.recordedfuture.com



© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.