Threat Intelligence Based Incident Correspondence Process Simulation Experiment Help Manual

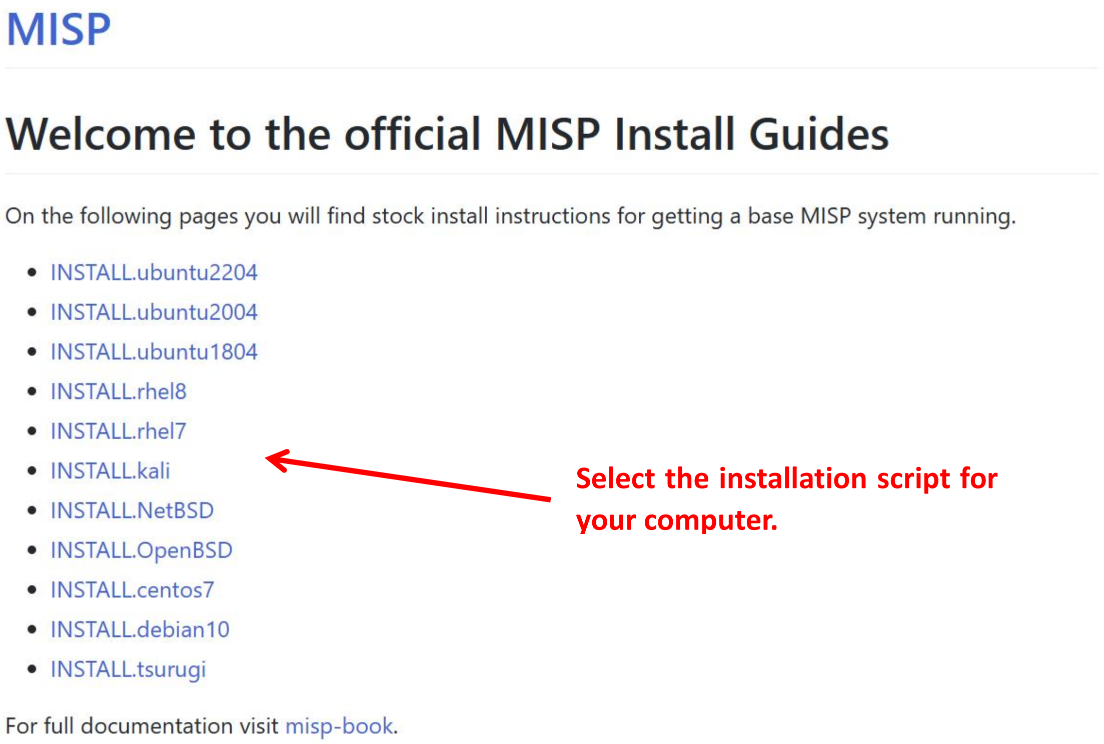
This lab manual is to help users test a machine's resilience to DDos attacks using a threat intelligence-based incident response process.

This project is open source in nature, and before you start testing, make sure that your testing actions are authorized and will not cause harm to any person or organization. Please ensure that you will not use the attack scripts designed by the author for any illegal purposes.

Finally, thank you for reading my research paper. I hope my research paper can provide you with research ideas and improve your organization's cyber defenses.

Part1.MISP Installation and Setup.

First, you need to use the installation link(https://misp.github.io/MISP/) provided by MISP to download the installation script that corresponds to the virtual environment you are using.This guide uses the ubuntu2004 virtual environment as an example.



MISP

Welcome to the official MISP Install Guides

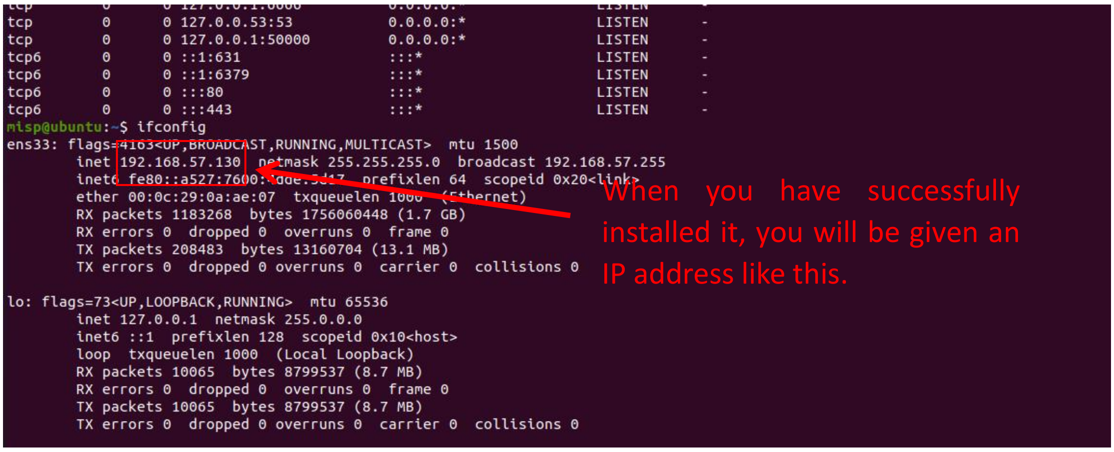
On the following pages you will find stock install instructions for getting a base MISP system running.

- INSTALL.ubuntu2204
- INSTALL.ubuntu2004
- INSTALL.ubuntu1804
- INSTALL.rhel8
- INSTALL.rhel7
- INSTALL.kali
- INSTALL.NetBSD
- INSTALL.OpenBSD
- INSTALL.centos7
- INSTALL.debian10
- INSTALL.tsurugi

For full documentation visit misp-book.

Select the installation script for your computer.

Correctly install the MISP on your virtual environment terminal and obtain the IP address of your MISP. Log in to the MISP initialization screen from your browser.Also, if the manual on the official website doesn't solve your problem, you can watch this Youtube installation video(https://www.youtube.com/watch?v=nZcTc60YsIs). This video will solve most of your problems with the installation part.



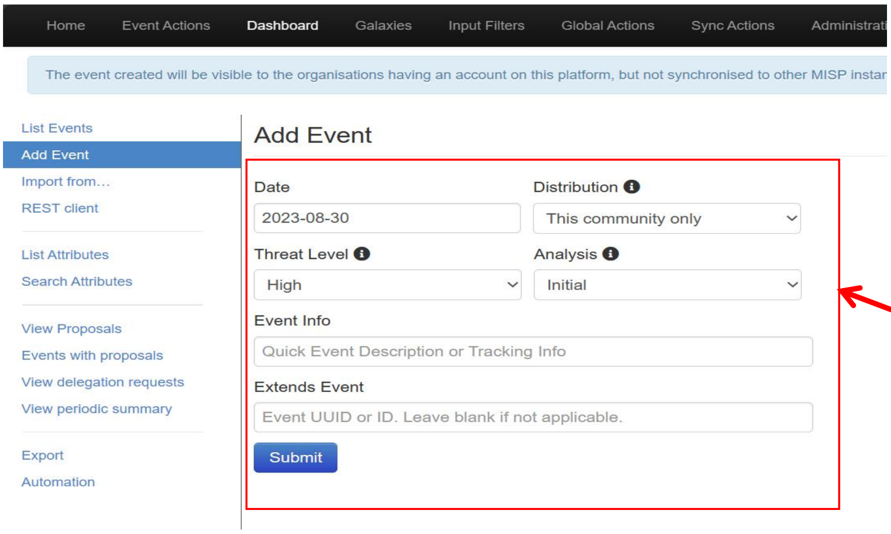
```
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:50000         0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:6379                :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      -
misp@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.57.130  netmask 255.255.255.0  broadcast 192.168.57.255
        inet6 fe80::a527:7600:dde:5d17  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0a:ae:07  txqueuelen 1000  (Ethernet)
        RX packets 1183268  bytes 1756060448 (1.7 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 208483  bytes 13160704 (13.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10065  bytes 8799537 (8.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10065  bytes 8799537 (8.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

When you have successfully installed it, you will be given an IP address like this.

Part2.Experimental preparation.

First, you need to create an Events on MISP for yourself or your organization. for uploading or downloading relevant threat intelligence.



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instar

Add Event

Date: 2023-08-30

Distribution: This community only

Threat Level: High

Analysis: Initial

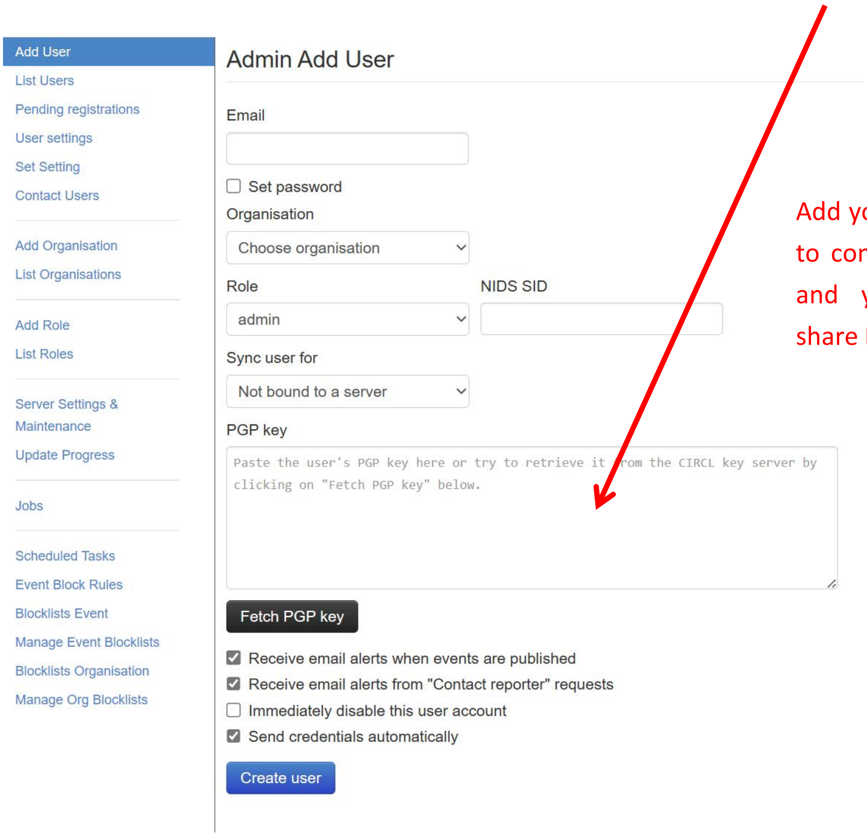
Event Info: Quick Event Description or Tracking Info

Extends Event: Event UUID or ID. Leave blank if not applicable.

Set the details of your Events here.

If you have a security team working with you on the experiment. You can set up an organization where members of the organization can share the MISP and adjustments to the status of events.

You and your security team colleagues can access your respective PGP keys at the bottom of the MISP page.



Admin Add User

Email:

□ Set password

Organisation: Choose organisation

Role: admin

NIDS SID:

Sync user for: Not bound to a server

PGP key: Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

☑ Receive email alerts when events are published

☑ Receive email alerts from "Contact reporter" requests

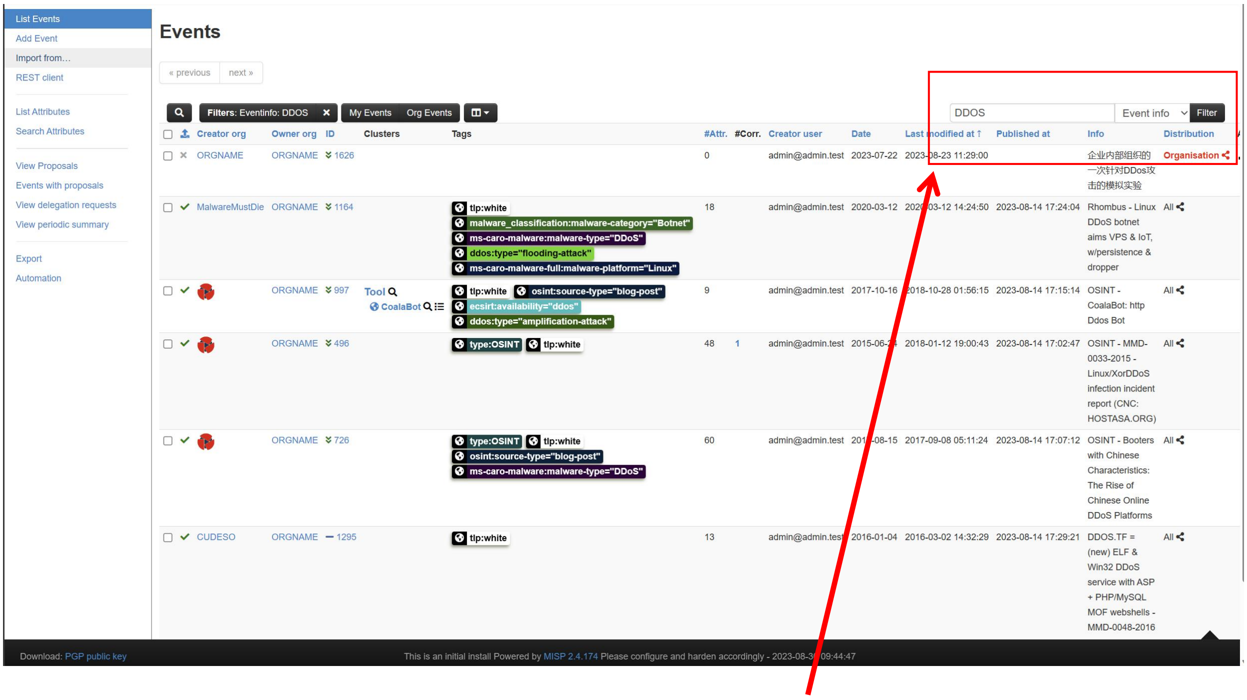
□ Immediately disable this user account

☑ Send credentials automatically

Add your coworker's PGP key here to complete the basic setup. You and your coworkers can then share Events with each other.

Part3.Acquisition of threat information

If you have a need to get threat intelligence, you can refer to the image below.On the left side of the MISP page, you can see the List Events button. In this screen you can see threat intelligence published by many organizations.



List Events
Add Event
Import from…
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests
View periodic summary

Export
Automation

Events

« previous | next »

Filters: Eventinfo: DDOS ✕ | My Events | Org Events

DDOS | Event info | Filter

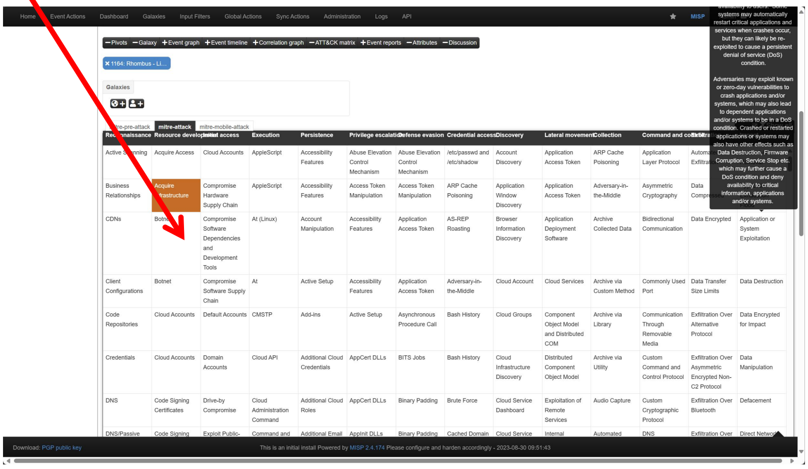
□		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at ↑	Published at	Info	Distribution
□	✕	ORGNAME	ORGNAME	1626			0		admin@admin.test	2023-07-22	2023-08-23 11:29:00		企业内部组织的一次针对DDos攻击的模拟实验	Organisation
□	✓	MalwareMustDie	ORGNAME	1164		tlp:white malware_classification:malware-category="Botnet" ms-caro-malware:malware-type="DDoS" ddos:type="flooding-attack" ms-caro-malware-full:malware-platform="Linux"	18		admin@admin.test	2020-03-12	2020-03-12 14:24:50	2023-08-14 17:24:04	Rhombus - Linux DDoS botnet aims VPS & IoT, w/persistence & dropper	All
□	✓		ORGNAME	997	Tool CoalaBot	tlp:white osint:source-type="blog-post" ecsirt:availability="ddos" ddos:type="amplification-attack"	9		admin@admin.test	2017-10-16	2018-10-28 01:56:15	2023-08-14 17:15:14	OSINT - CoalaBot: http Ddos Bot	All
□	✓		ORGNAME	496		type:OSINT tlp:white	48	1	admin@admin.test	2015-06-24	2018-01-12 19:00:43	2023-08-14 17:02:47	OSINT - MMD-0033-2015 - Linux/XorDDoS infection incident report (CNC: HOSTASA.ORG)	All
□	✓		ORGNAME	726		type:OSINT tlp:white osint:source-type="blog-post" ms-caro-malware:malware-type="DDoS"	60		admin@admin.test	2017-08-15	2017-09-08 05:11:24	2023-08-14 17:07:12	OSINT - Booters with Chinese Characteristics: The Rise of Chinese Online DDoS Platforms	All
□	✓	CUDESO	ORGNAME	1295		tlp:white	13		admin@admin.test	2016-01-04	2016-03-02 14:32:29	2023-08-14 17:29:21	DDOS.TF = (new) ELF & Win32 DDoS service with ASP + PHP/MySQL MOF webshells - MMD-0048-2016	All

Download: PGP public key

This is an initial install Powered by MISP 2.4.174 Please configure and harden accordingly - 2023-08-30 09:44:47

Retrieve the threat intelligence you need by searching the search bar for tags for the type of attack you want to learn about.

By searching, you will access threat intelligence information issued by a number of organizations.



Reconnaissance	Resource development	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control	Exfiltration	Impact
Active Scanning	Acquire Access	Cloud Accounts	AppleScript	Accessibility Features	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	ARP Cache Poisoning	Application Layer Protocol	Automated Exfiltration	
Business Relationships	Acquire Infrastructure	Compromise Hardware Supply Chain	AppleScript	Accessibility Features	Access Token Manipulation	Access Token Manipulation	ARP Cache Poisoning	Application Window Discovery	Application Access Token	Adversary-in-the-Middle	Asymmetric Cryptography	Data Compressed	
CDNs	Botnet	Compromise Software Dependencies and Development Tools	At (Linux)	Account Manipulation	Accessibility Features	Application Access Token	AS-REP Roasting	Browser Information Discovery	Application Deployment Software	Archive Collected Data	Bidirectional Communication	Data Encrypted	Application or System Exploitation
Client Configurations	Botnet	Compromise Software Supply Chain	At	Active Setup	Accessibility Features	Application Access Token	Adversary-in-the-Middle	Cloud Account	Cloud Services	Archive via Custom Method	Commonly Used Port	Data Transfer Size Limits	Data Destruction
Code Repositories	Cloud Accounts	Default Accounts	CMSTP	Add-ins	Active Setup	Asynchronous Procedure Call	Bash History	Cloud Groups	Component Object Model and Distributed COM	Archive via Library	Communication Through Removable Media	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Credentials	Cloud Accounts	Domain Accounts	Cloud API	Additional Cloud Credentials	AppCert DLLs	BITS Jobs	Bash History	Cloud Infrastructure Discovery	Distributed Component Object Model	Archive via Utility	Custom Command and Control Protocol	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Manipulation
DNS	Code Signing Certificates	Drive-by Compromise	Cloud Administration Command	Additional Cloud Roles	AppCert DLLs	Binary Padding	Brute Force	Cloud Service Dashboard	Exploitation of Remote Services	Audio Capture	Custom Cryptographic Protocol	Exfiltration Over Bluetooth	Defacement
DNS/Passive	Code Signing	Exploit Public-	Command and	Additional Email	AppInit DLLs	Binary Padding	Cached Domain	Cloud Service	Internal	Automated	DNS	Exfiltration Over	Direct Network

systems may automatically restart critical applications and services when crashes occur, but they can likely be re-exploited to cause a persistent denial of service (DoS) condition.

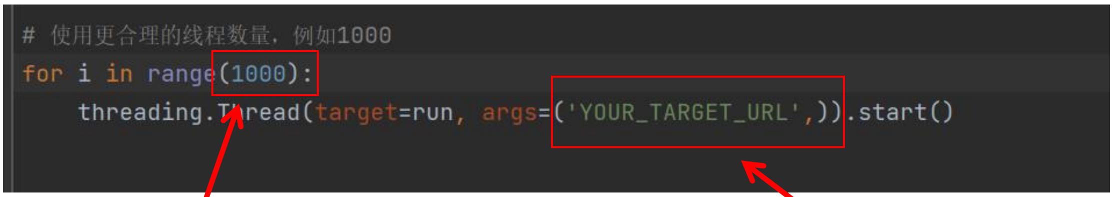
Adversaries may exploit known or zero-day vulnerabilities to crash applications and/or systems, which may also lead to dependent applications and/or systems to be in a DoS condition. Crashed or restarted applications or systems may also have other effects such as Data Destruction, Firmware Corruption, Service Stop etc. which may further cause a DoS condition and deny availability to critical information, applications and/or systems.

Download: PGP public key

This is an initial install Powered by MISP 2.4.174 Please configure and harden accordingly - 2023-08-30 09:51:43

Part4.DDos Attack Test

The author has created an open source DDos attack script for stress resistance testing for you or your organization. The author uploaded the attack script code to GitHub(https://github.com/MINGZEwantastudy/DDos-Attack-Scripts.git). If youneed it you can download and use it yourself.



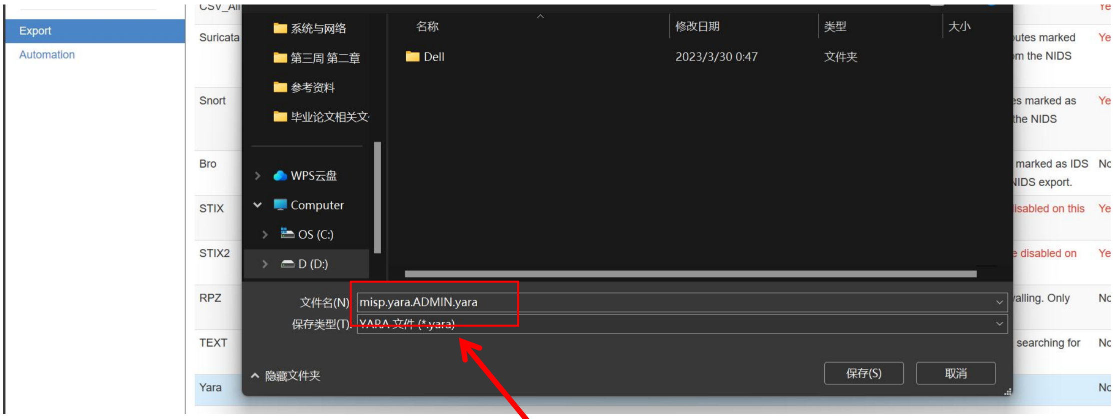
```
# 使用更合理的线程数量，例如1000
for i in range(1000):
    threading.Thread(target=run, args=('YOUR_TARGET_URL',)).start()
```

Add the URL of the target website you want to test here. the attack script also supports the specified interface in the website you are testing. If you want, you need to add more information according to the rules for setting up URLs.

Modify the number of threads according to the performance of your machine. An unreasonable number of threads may cause your computer to lag.

Part5.Import threat intelligence into your own IDS.

More your needs, you can feed the threat intelligence provided by MISP into your IDS. The downloadable questions support a variety of formats (please refer to the official MISP guide for details).



Dell 2023/3/30 0:47 文件夹

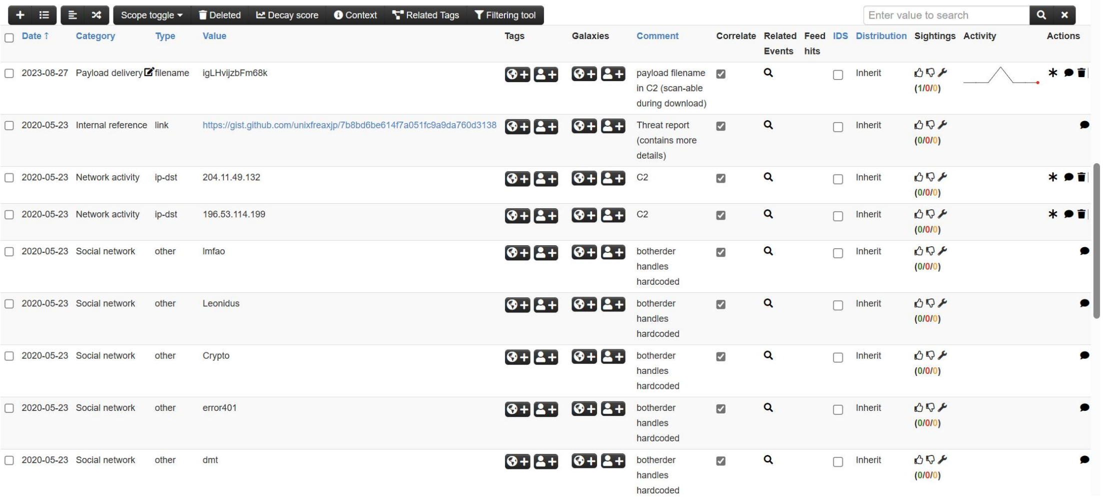
文件名(N): misp.yara.ADMIN.yara

保存类型(T): YARA 文件 (*.yara)

Be careful to use and select the question format that applies to your IDS!

Part6.Uploading Threat Intelligence

Finally, you can upload your threat intelligence to the Events you created earlier. Provide critical information to other members of the community. You can also rate the threat intelligence information posted by others.



☐	Date ↑	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐	2023-08-27	Payload delivery	filename	igLHvijzbFm68k			payload filename in C2 (scan-able during download)	☑			☐	Inherit	(1/0/0)		
☐	2020-05-23	Internal reference	link	https://gist.github.com/unixfreaxjp/7b8bd6be614f7a051fc9a9da760d3138			Threat report (contains more details)	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Network activity	ip-dst	204.11.49.132			C2	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Network activity	ip-dst	196.53.114.199			C2	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Social network	other	lmfao			botherder handles hardcoded	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Social network	other	Leonidus			botherder handles hardcoded	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Social network	other	Crypto			botherder handles hardcoded	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Social network	other	error401			botherder handles hardcoded	☑			☐	Inherit	(0/0/0)		
☐	2020-05-23	Social network	other	dmt			botherder handles hardcoded	☑			☐	Inherit	(0/0/0)		