ISP’s DDoS Protection Strategies: DDoS Mitigation and Botnet C2 Blocking

Siarhei Matashuk
CCIE # 27340
Technical Consultant @ Genie Networks

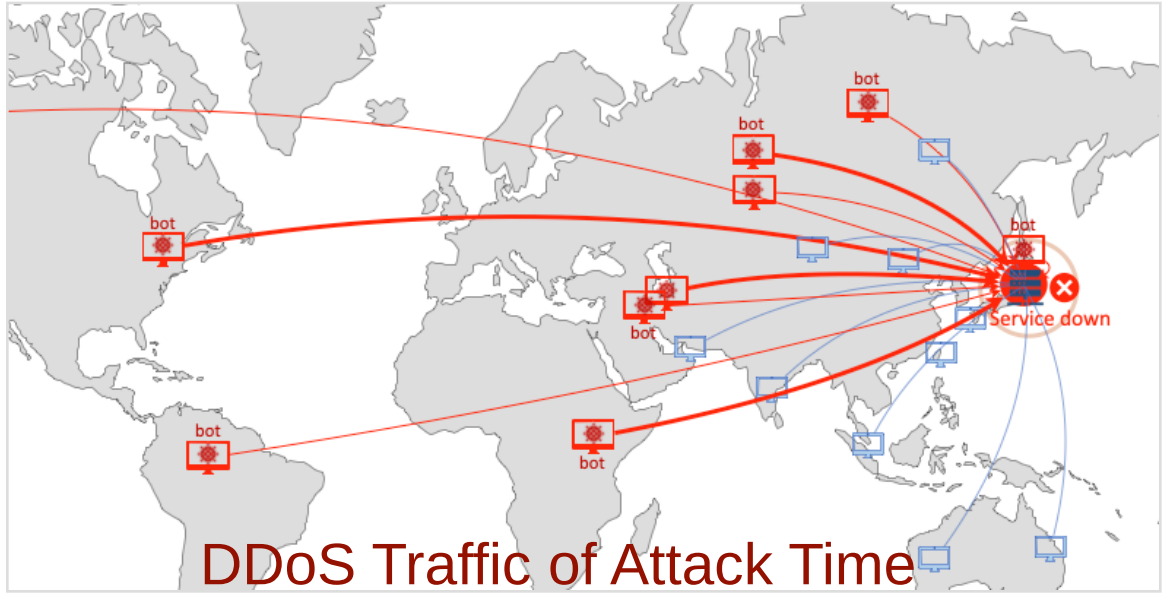
DDoS Mitigation Policy + Botnet C2 Blocking Policy

DDoS Mitigation Policy at attack time

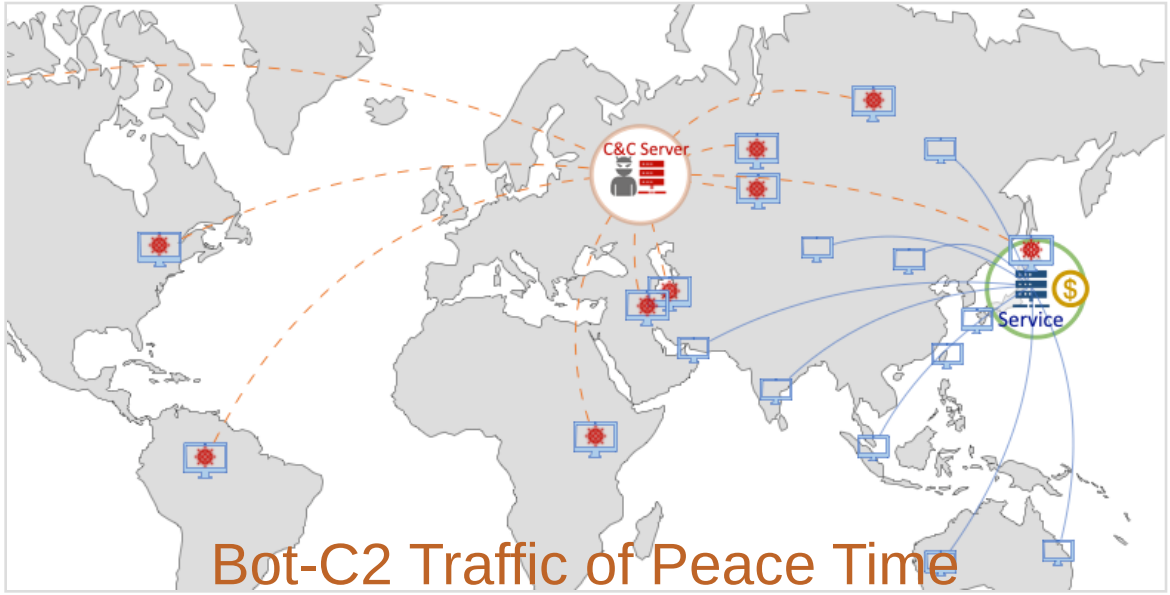
- When a victim is under attack, mitigate the DDoS traffic by dropping the victim traffic or redirecting it to a scrubbing center.
- Large volume, relatively rare

Botnet C2 Blocking Policy (prevention)

- To eliminate the attacks in advance, drop the C&C server traffic all the time to prevent the bots from getting controlled.
- Low-Volume, continuous



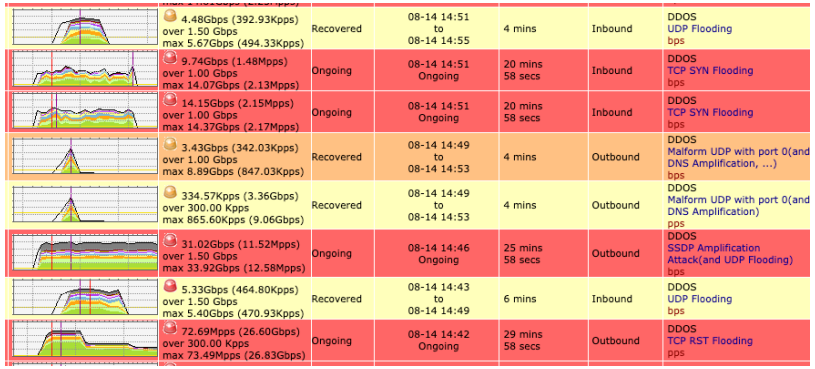
DDoS Traffic of Attack Time



Bot-C2 Traffic of Peace Time

Traffic Scale of DDoS Attack and Botnet C2 Connection

Monitoring example in a large-scale ISP :

	Traffic Behavior	Traffic Amount	Frequency
General Traffic	-	average traffic: 60 Tbps	-
DDoS Attack Traffic	Burst huge traffics 	per event: 5 ~ 500 Gbps/event total attack traffic: 2.6 Tbps	500 ~ 1000 events a day
Botnet C2 Traffic	Occasional short connects 	per connect: 60K ~ 20M bps	~ 15,000 conns. a week

Botnet C2 Blocking

ISP's DDoS Protection Strategies

Mitigation - when the DDoS attack is on going

- **strategy:** drop or filter traffic toward victim IP
- drop or redirect the attacking traffic of the victim IP via BGP/FlowSpec route
- attacking traffic attributes may vary from DDoS event to event
- attacking traffic attributes may vary during the DDoS event time
- **policy lifetime:** 20-30 mins or for even hours, which is aligned with the DDoS attack event

Prevention - when the c2 server attempts to contact his bots

- **strategy:** drop C2 servers' traffic
- drop the traffic to or from the C2 server IP addresses via BGP FlowSpec route
- **policy lifetime:** should be lasting for weeks

How to get the Bot-C2 Server IP List?

Known Bot-C2 Server IP List

- **source:** from known threat intel sharing sources, such as abuse.ch, AlienVault, FireHOL
- **update frequency:** update IP lists from the threat feeds every 15 mins or every hour
- monitoring activities via traffic flows per 5 minutes | past 30 days
- purging inactive C2 servers from the IP list

Unknown Bot-C2 Server Detection aided by AI-ML

- Bot-C2 server IP addresses are changing, Attackers use
- Besides security experts, AI-ML techniques can help to detect bot-C2 connections
- **source:** detect new bot-C2 servers based on learned bot-C2 connection behaviors
- **detection frequency:** per day | per week

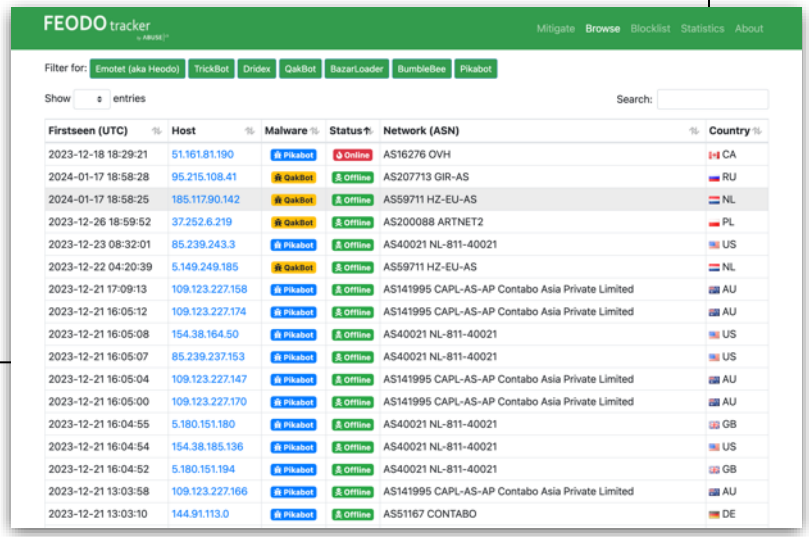
Collecting Bot-C2 Server IP List from Threat Feeds

Known Threat Intel Sources for reference:

- abuse.ch | Fighting malware and botnets
- Feodo Tracker | Browse Botnet C&Cs (abuse.ch)
- ThreatFox | Share Indicators Of Compromise (IOCs) with suspicious IP addresses
- AlienVault - Open Threat Exchange
- FireHOL IP Lists | IP Blacklists | IP Blocklists | IP Reputation
- DigitalSide Threat-Intel
- US CISA: Identification and Disruption of QakBot Infrastructure | CISA
- Free threat intelligence feeds - threatfeeds.io
- VirusTotal

Share Threat IP List / C2 IP List e.g. FEODO Tracker

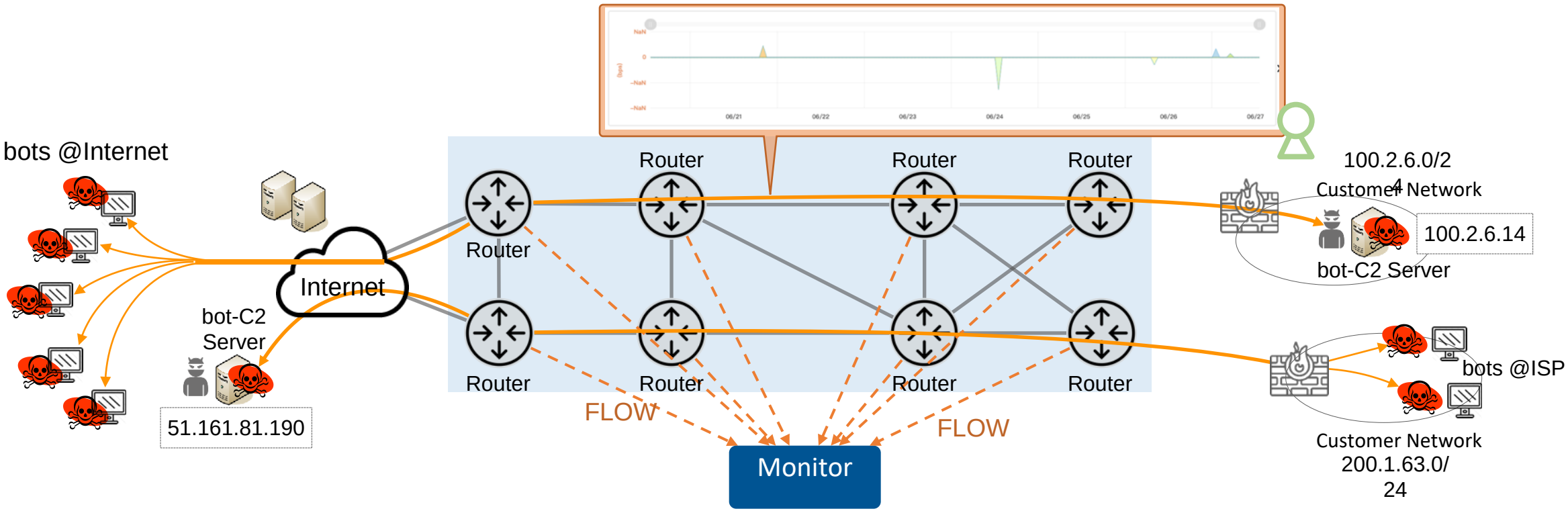
```
################################################################
# abuse.ch Feodo Tracker Botnet C2 IP Blocklist (IPs only)     #
# Last updated: 2024-05-27 20:05:51 UTC                        #
#                                                              #
# Terms Of Use: https://feodotracker.abuse.ch/blocklist/       #
# For questions please contact feodotracker [at] abuse.ch      #
################################################################
#
# DstIP
192.9.135.73
51.161.81.190
37.252.6.219
172.232.185.9
172.232.188.170
172.234.244.189
192.9.135.73
# END 7 entries
```



ISP Provides Botnet Monitoring Service

Monitor bot-C2 traffic and activities for each customer network:

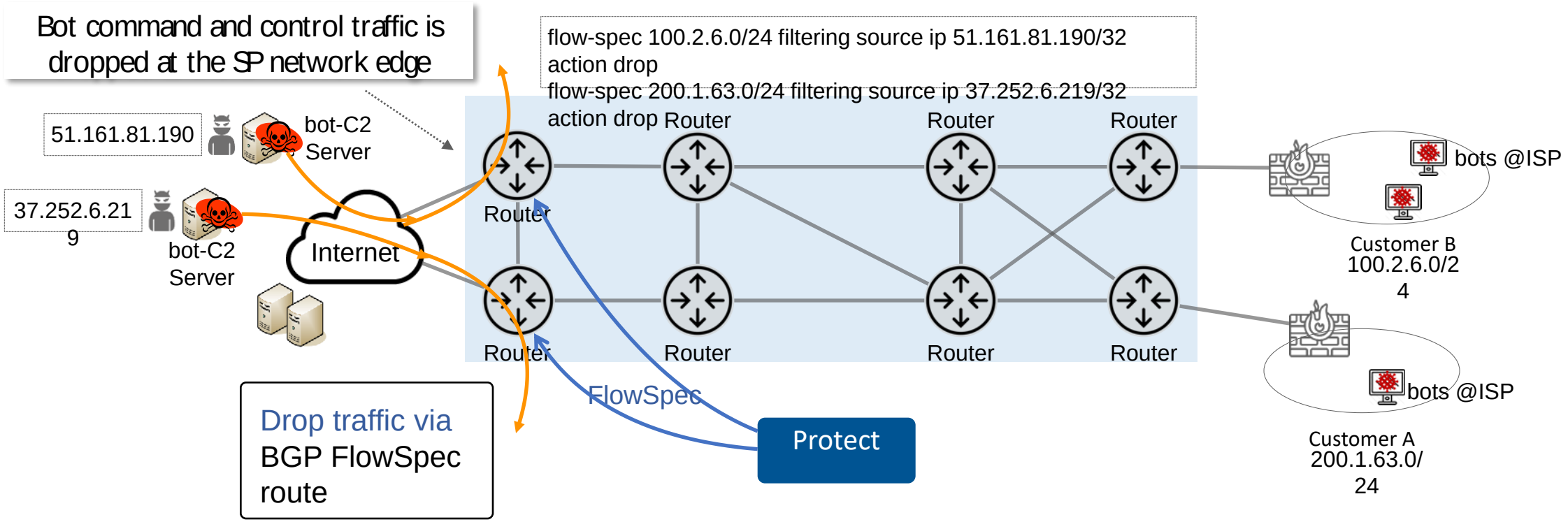
- The ISP finds active bot-C2 connections by monitoring traffic flows
- The ISP provides the bot-C2 activity report with IP addresses and attributes to the customers



ISP's Botnet C2 Blocking Strategy

The ISP drops bot-C2 traffic via BGP FlowSpec for C2 servers from Internet:

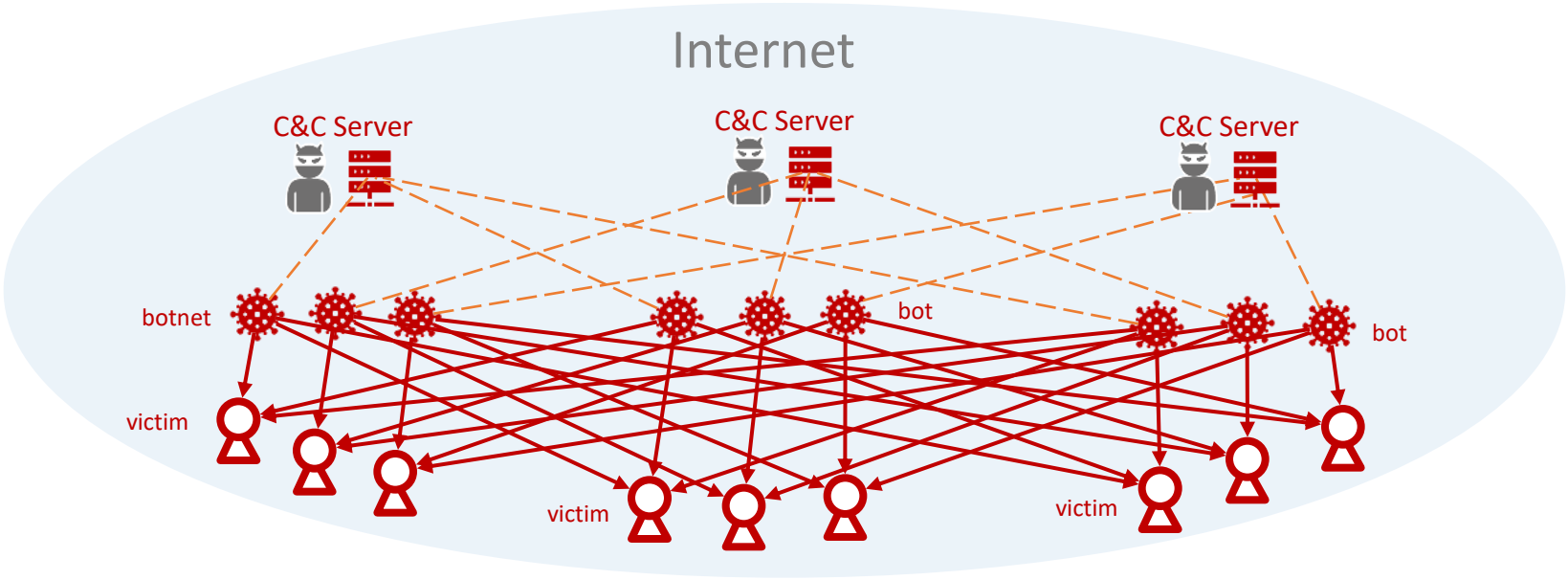
- The ISP monitors active bot-C2 connections of the customers
- The ISP provides bot-C2 traffic-blocking service for the customers via FlowSpec
- The ISP sends BGP FlowSpec routes filtered by source bot-C2 server IP (or IP+port) with drop action



Does Botnet C2 Blocking Policy Take Effect ?

Botnet C2 blocking policy benefits the whole Internet, not the ISP itself.

- Botnet and C&C Servers are distributed over the whole Internet.
- Applying botnet C2 blocking policy does NOT protect the ISP from DDoS attacks.
- Applying botnet C2 blocking policy is to eliminate the malicious traffic for the Internet.

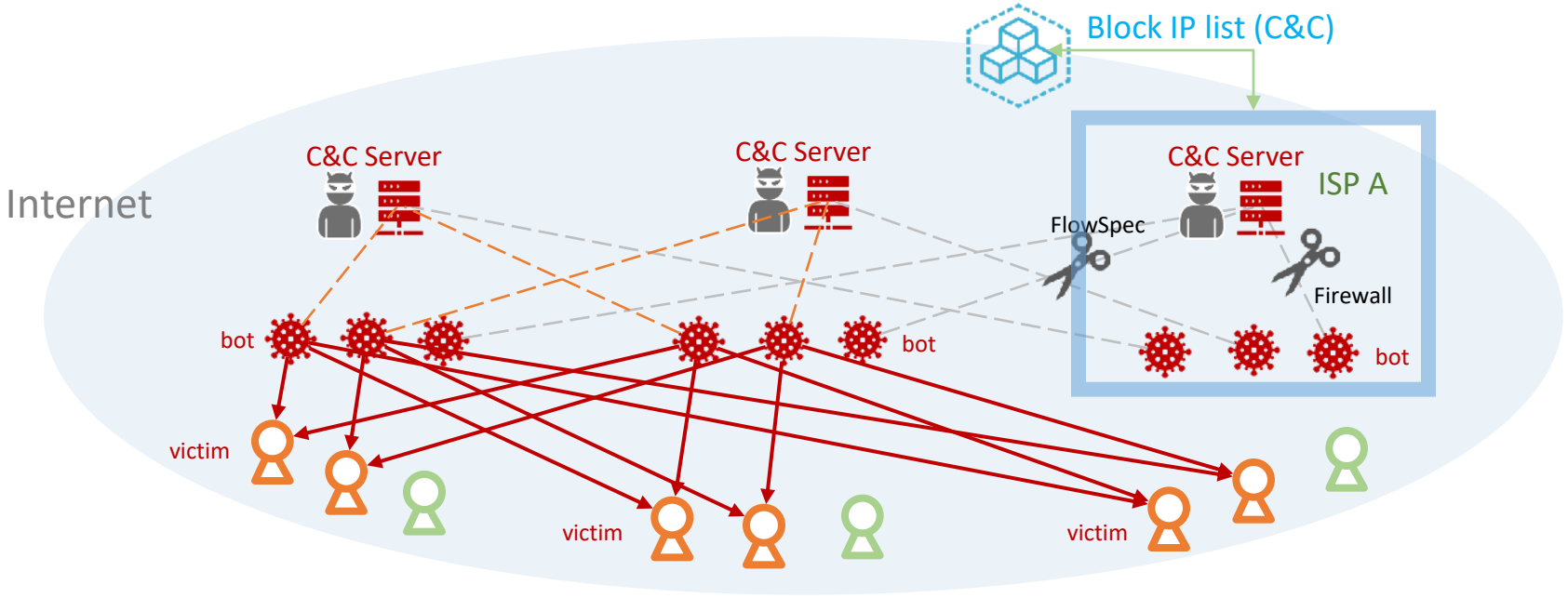


Does Botnet C2 Blocking Policy Take Effect ?

Botnet C2 Blocking Policy

- collecting and sharing C&C Server IP information with the ISP networks
- blocking connections between the C&C servers and the bots
- to eliminate the attacks in advance

Example: ISP A starts to disconnect C&C Server traffic; some bots fail to attack

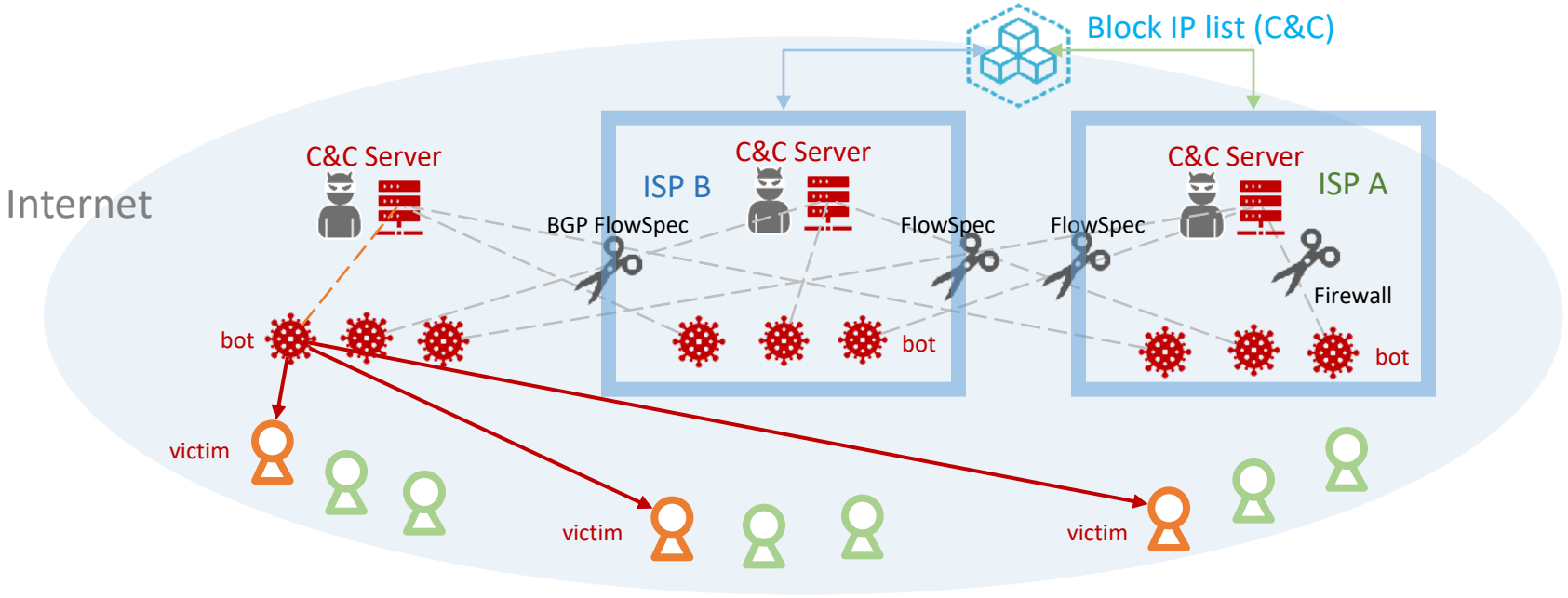


Does Botnet C2 Blocking Policy Take Effect ?

Botnet C2 Blocking Policy

- collecting and sharing C&C Server IP information with the ISP networks
- blocking connections between the C&C servers and the bots
- to eliminate the attacks in advance

Example: More ISPs apply Bot-C2 blocking policy to disconnect Bot-C2 servers

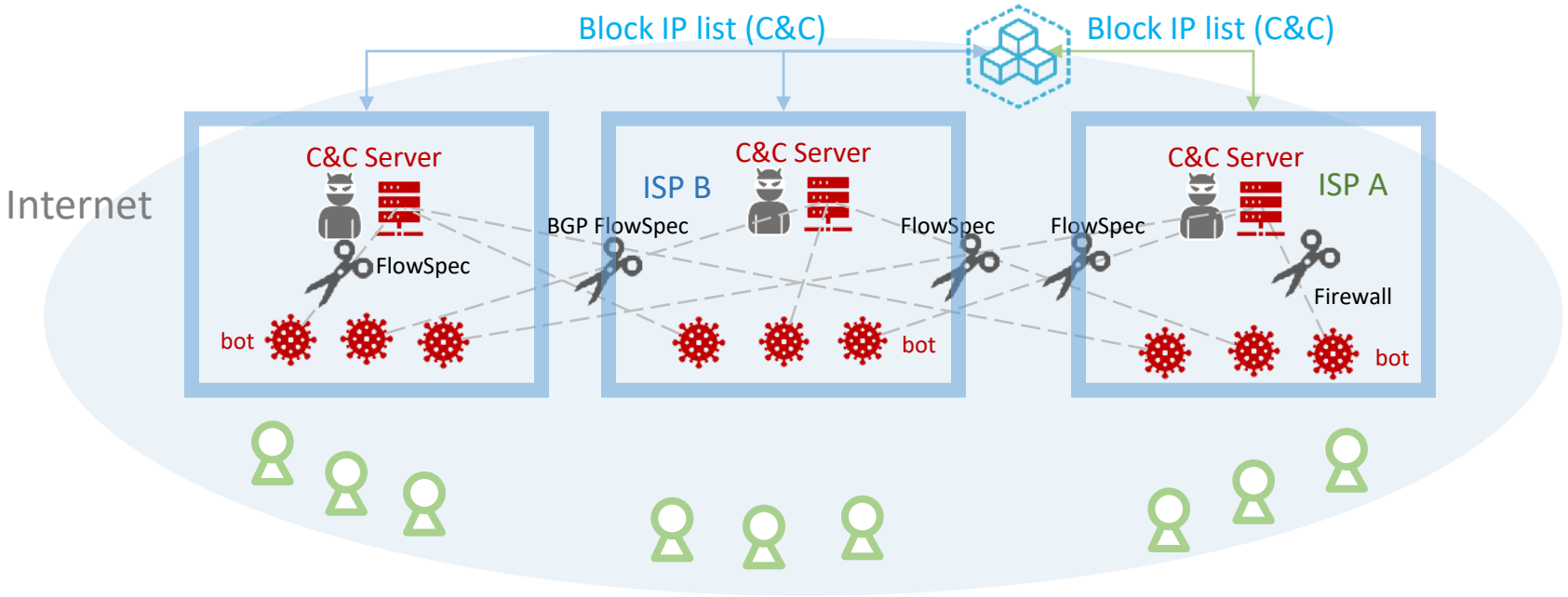


Implementing Botnet C2 Blocking Policy Benefits the Internet

Botnet C2 Blocking Policy

- collecting and sharing C&C Server IP information with the ISP networks
- blocking connections between the C&C servers and the bots
- to eliminate the attacks in advance

Example: A lot ISPs block the Bot-C2 traffic to force most bots being inactive



Traffic Scale of DDoS Attack and Botnet C2 Connection

Monitoring example in a large-scale ISP :

	events	Per-event Traffic Amount	Total Traffic Amount
Inbound DDoS Attack	~250 events a day	300 Gbps/event	~1.6 Tbps
Inbound DDoS Attack (C2 block applied)	~250 events a day	300 Gbps/event	~1.5 Tbps
DDoS Attacks from inside	~350 events a day	60 Gbps/event	0.7 Tbps
DDoS Attacks from inside (C2 block applied)	~200 events a day ▽	40 Gbps/event ▽	0.5 Tbps ▽
Outbound DDoS Attack	~400 events a day	20 Gbps/event	0.3 Tbps
Outbound DDoS Attack (C2 block applied)	~300 events a day ▽	16 Gbps/event ▽	0.2 Tbps ▽

AI-aided Unknown Bot-C2 Detection

C2 Server IP addresses are Changing

There are unknown C&C servers because:

- Botnet and C&C Servers are growing
- Bots are easily switching to another C&C Server thru dynamic DNS queries
- Not enough security experts to monitor and examine the infected host traffic
- Domain Generation Algorithms (DGA), Fast Flux

C2 Server list should be updated frequently

Using machine learning to find unknown C2 servers:

- Continuously monitor botnet traffic,
- and keep C2 Server List updated via AI machine learning.

Using AI-ML to Predict Unknown C2 Servers

Using machine learning for unknown Bot-C2 server detection:

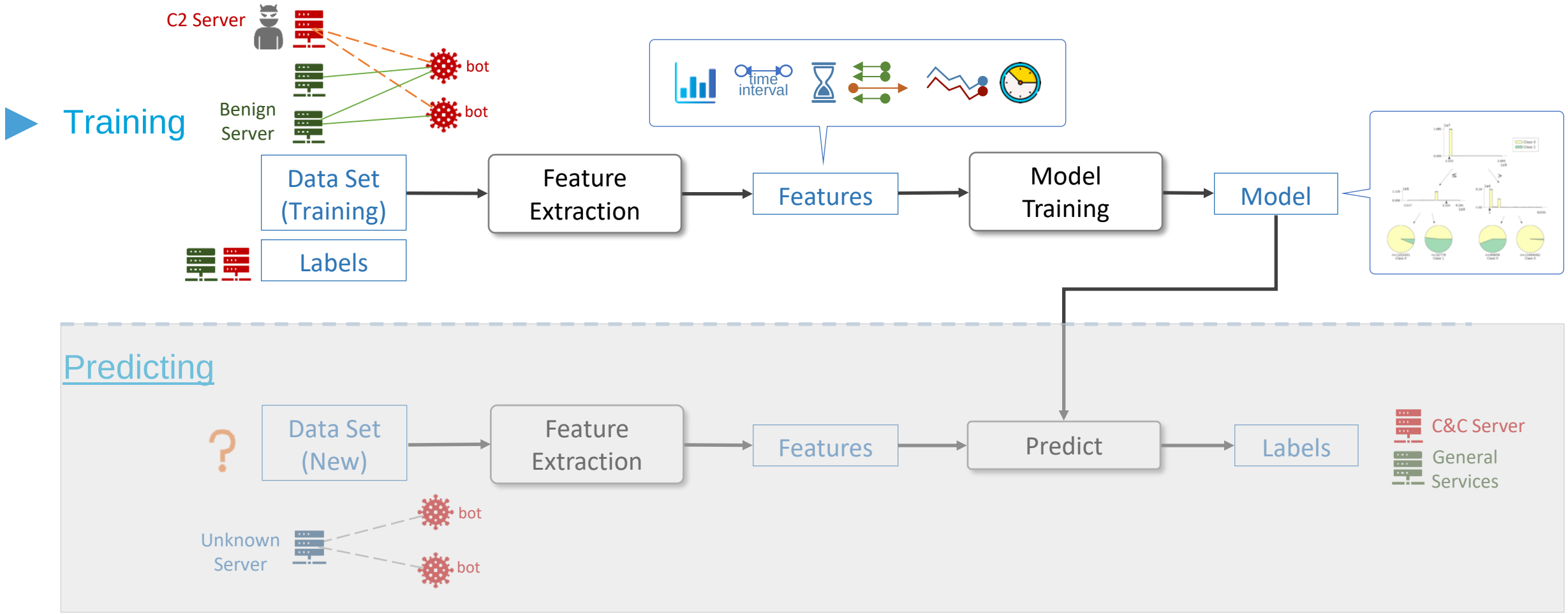
- Data sets are generated from collected flows on a daily basis

- Training sets come from the flows of known C2 servers and benign servers
- Model is trained by flow traffic statistics features

- Predict Bot-C2 connection from collected flows on a daily basis
- C2 server list is auto updated and maintained by continuous C2 server detection

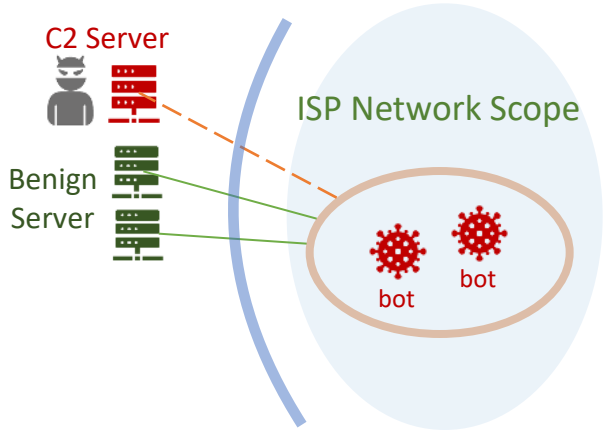
Train C2 Server Connection Model by ML

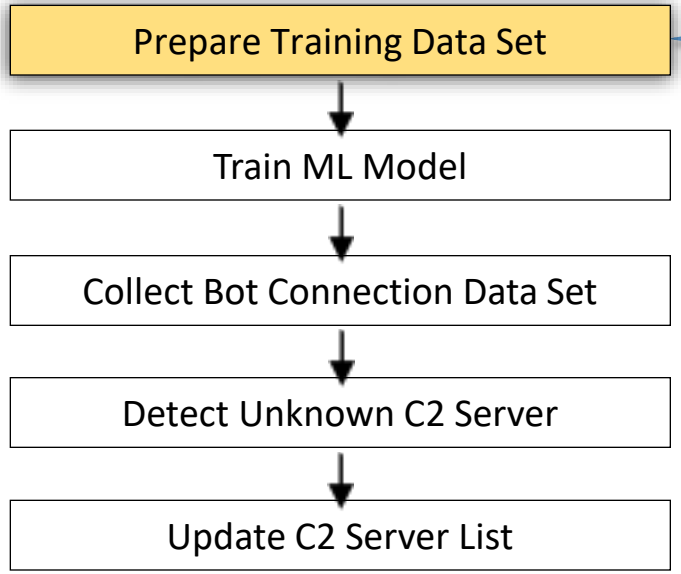
Detect Unknown C2



AI learns connection behaviors of both bot-C2 servers and benign servers, and generates the model.

Server Connection Data Set





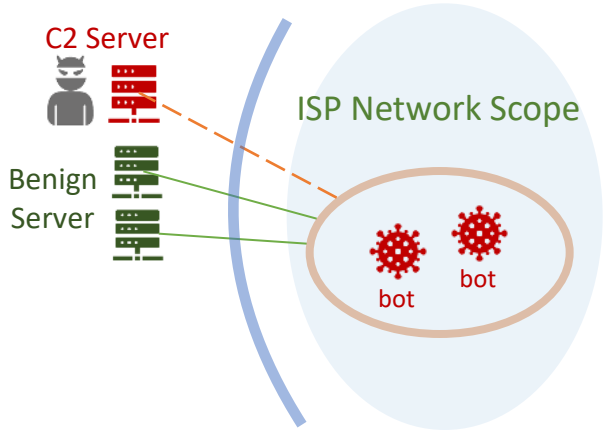
C2 Server Connection Data Set (for training purpose)

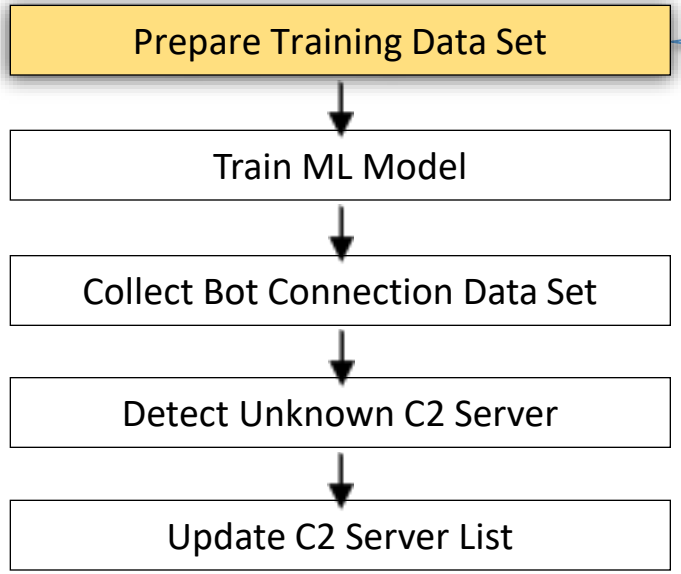
- Traffic to/from C2 Servers

Benign Server Connection Data Set (for training purpose)

- Traffic to/from Benign Servers

Data Set Record





Server Connection Data Set Record

- A record in the Server Connection Data Set should be tuples of flow record fields with statistics of traffic to identify a bidirectional IP/Port pair.

Monitor Bidirectional IP Flows in One Day

- Server IP address
- Client(Bot) IP address
- Server Port
- Client Port

Data Set Record - Statistics Features

Server IP	SPort	Client IP	CPort	Total Packets	Total Bytes	Total Flows	Packet Mean	Packet Std	Byte Mean	Byte Std	Pkt Auto-correlation Mean (5min)	Pkt Auto-correlation Std (5min)	Byte Auto-correlation Mean (5min)
192.0.101.22	201	192.0.101.32	119	34.56G	25.92G	2.88K	12.00M	0	9.00M	0	1	0	1
6:a:0:65::29	229	6:c0:0:65::29	129	17.28M	16.42M	1.44K	12.00K	0	11.40K	0	1	0	1

Flow Size

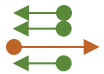
- bytes/packets
- mean / standard deviation

Auto-correlation

- bytes/packets
- calculate from time series of flow size mean value per 300 sec, ordering by time.
- mean / standard deviation

Inter-Arrival

- time series of first seen time difference between consecutive connections
- minimum / maximum / median /standard deviation



Unmatched flow density

- time series of unmatched flow number: abs diff between incoming and outgoing flows (period in 300 sec)
- mean time / standard deviation

Duration

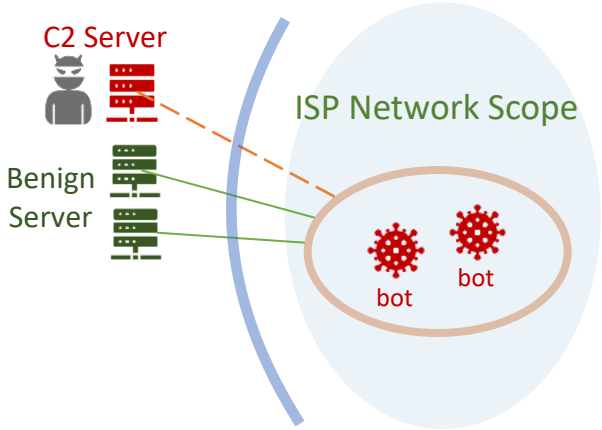
- mean / standard deviation

Temporal Features

- time series of flow volume per hour
- mean / standard deviation

Train Bot-C2 Connection Model by ML (RF)

Detect Unknown C2



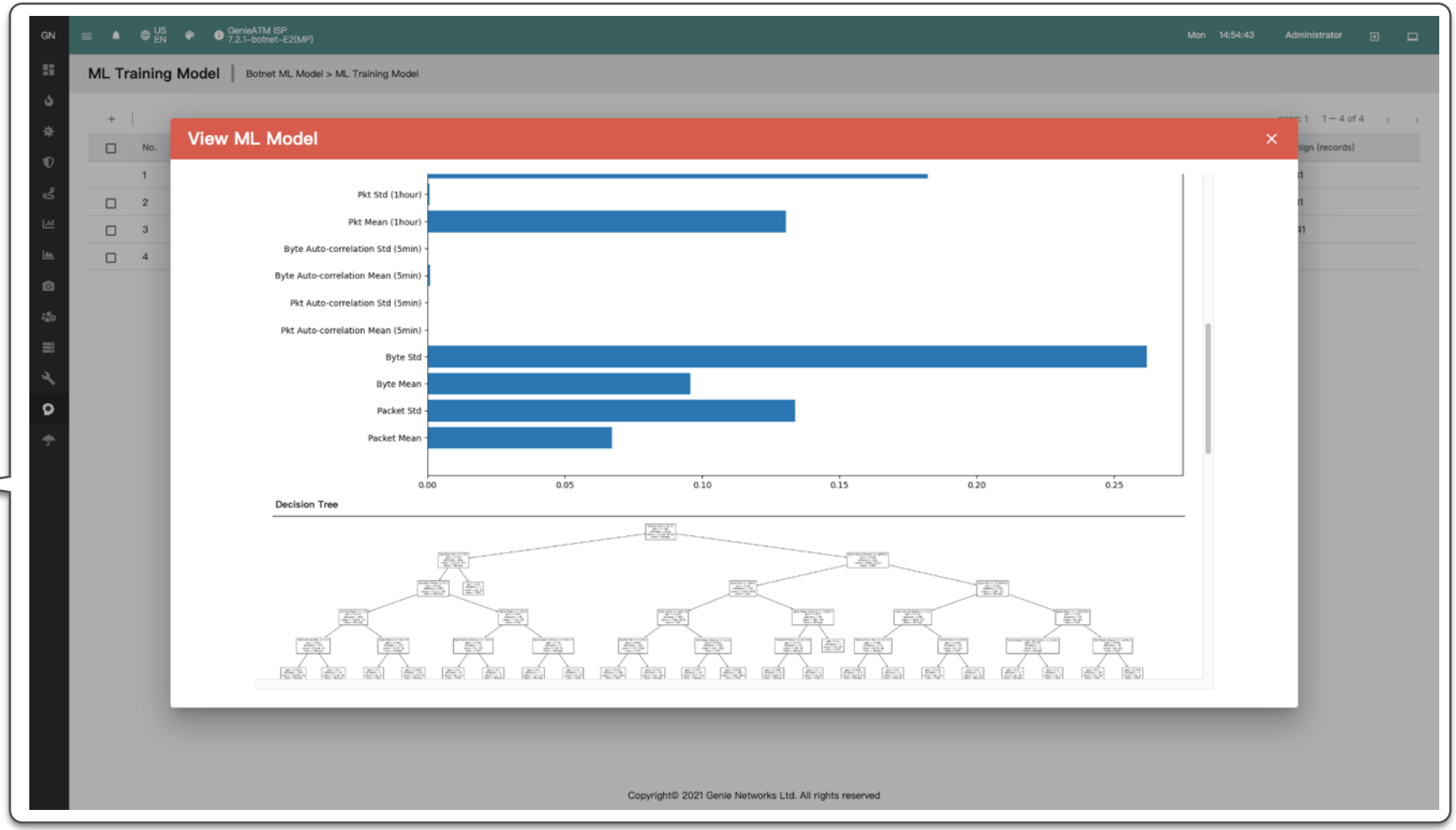
Prepare Training Data Set

Train ML Model

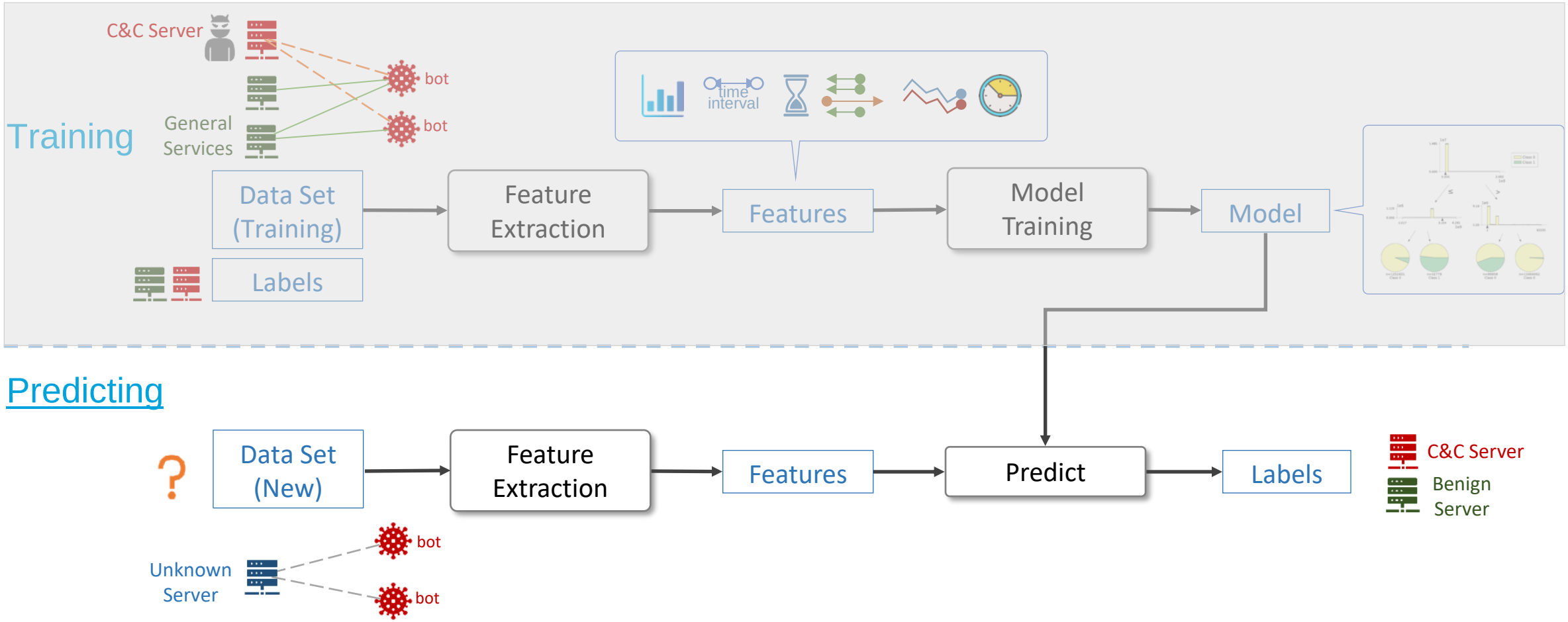
Collect Bot Connection Data Set

Detect Unknown C2 Server

Update C2 Server List

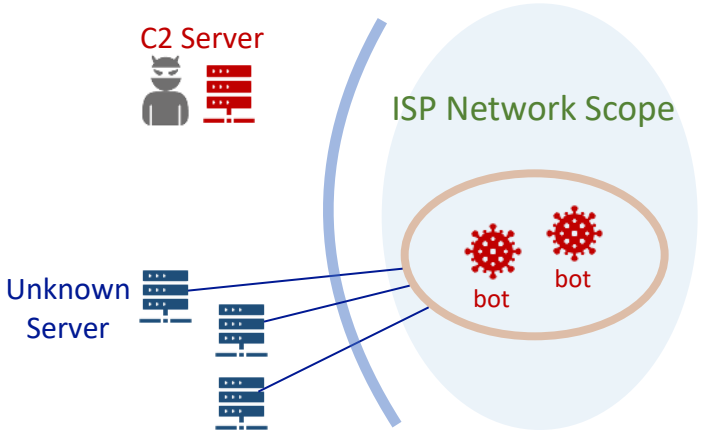


Predict Unknown C2 Servers by ML



For new collected data sets, AI tries to detect if the connection behavior is similar to bot-C2.

Collect Bot Connection Data Set



Prepare Training Data Set

↓

Train ML Model

↓

Collect Bot Connection Data Set

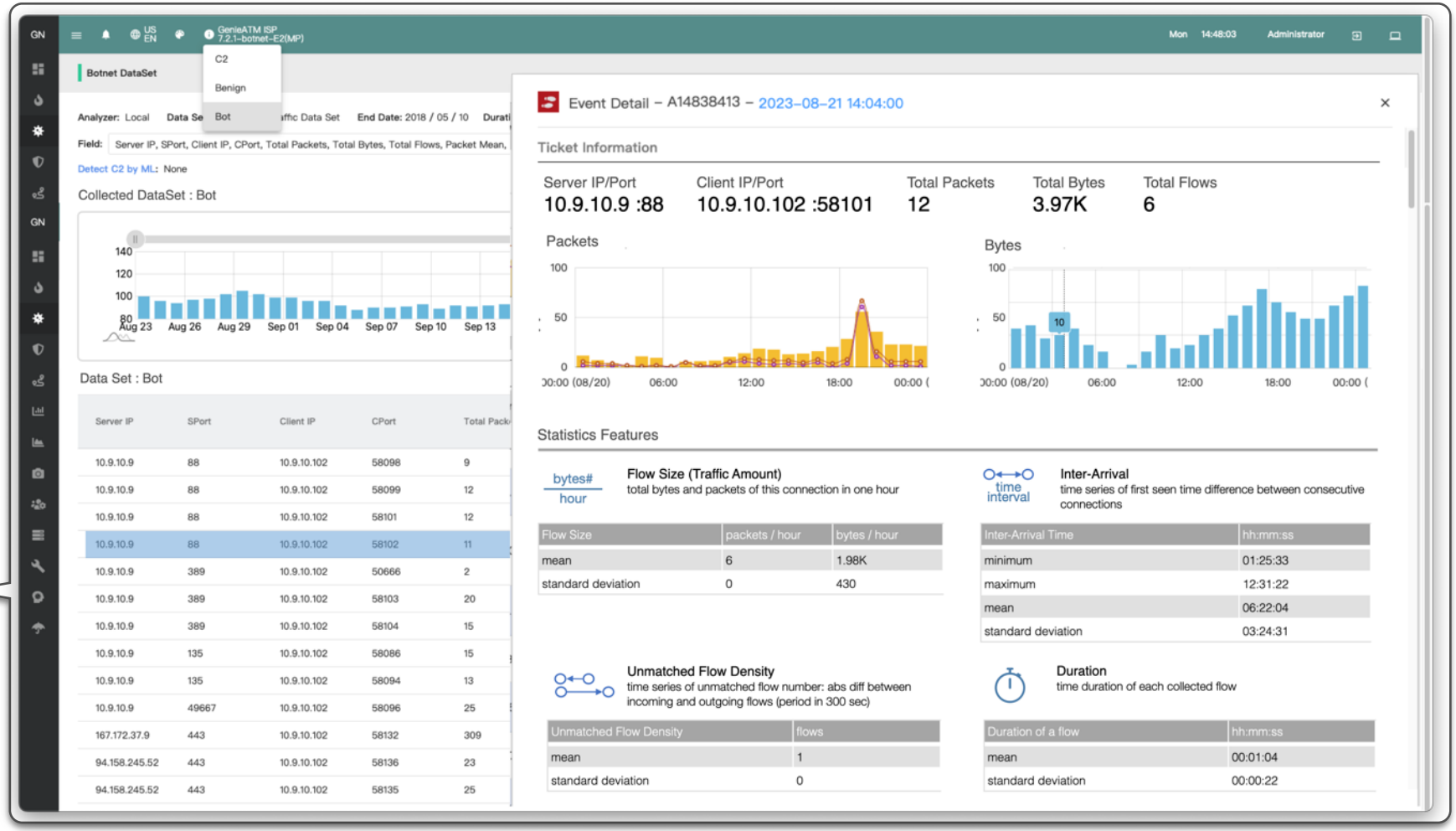
↓

Detect Unknown C2 Server

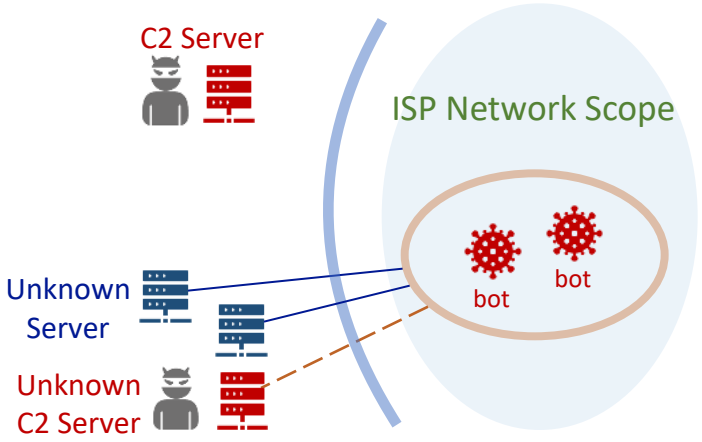
↓

Update C2 Server List

Bot Traffic Data Set (for C2 detection purpose)



Detect Unknown C2 Server in the Data Set



Prepare Training Data Set

↓

Train ML Model

↓

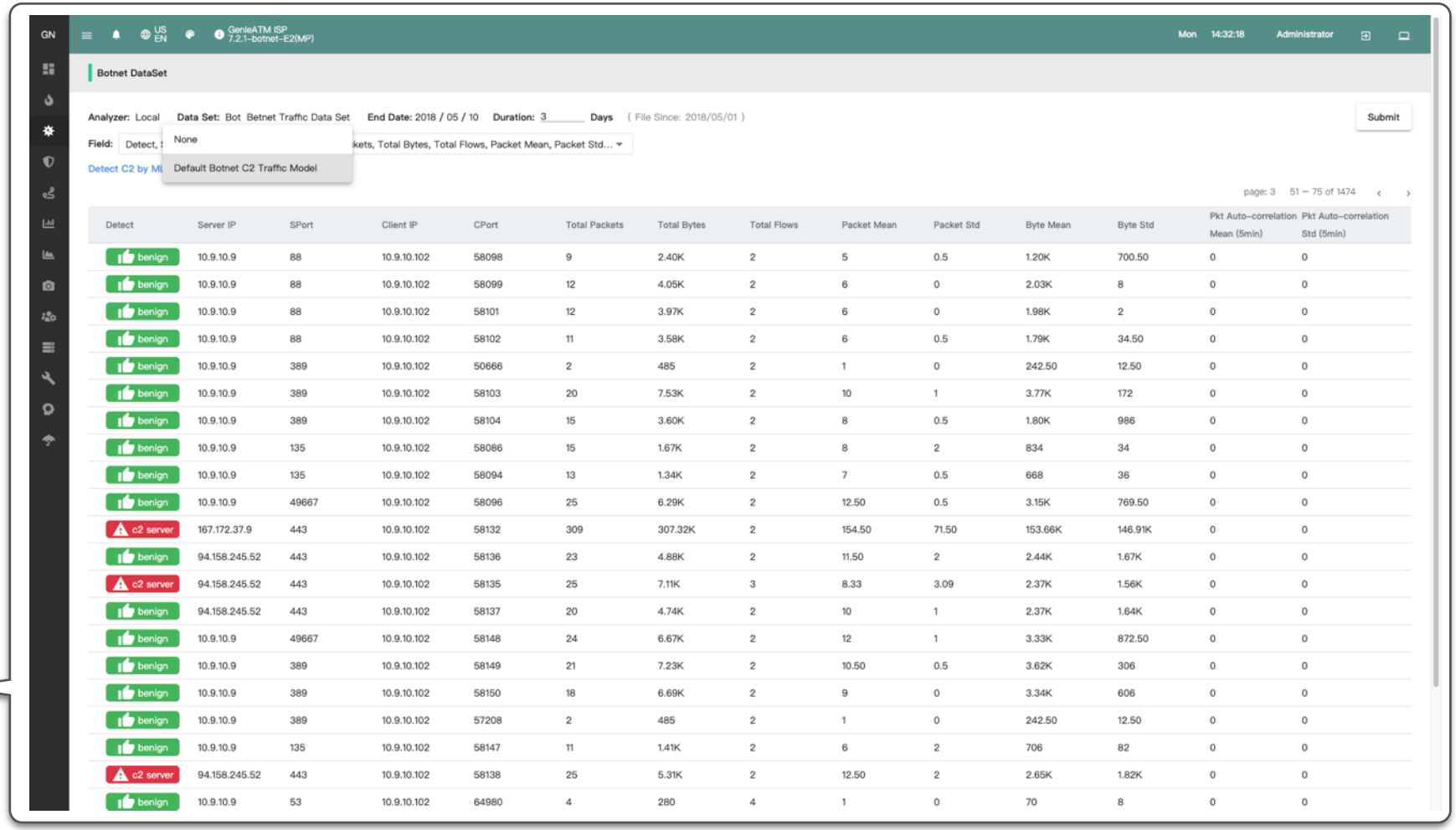
Collect Bot Connection Data Set

↓

Detect Unknown C2 Server

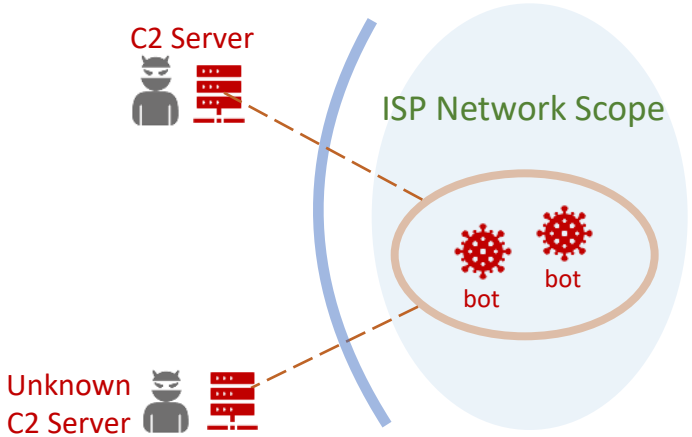
↓

Update C2 Server List



Detect	Server IP	SPort	Client IP	CPort	Total Packets	Total Bytes	Total Flows	Packet Mean	Packet Std	Byte Mean	Byte Std	Pkt Auto-correlation Mean (5min)	Pkt Auto-correlation Std (5min)
benign	10.9.10.9	88	10.9.10.102	58098	9	2.40K	2	5	0.5	1.20K	700.50	0	0
benign	10.9.10.9	88	10.9.10.102	58099	12	4.05K	2	6	0	2.03K	8	0	0
benign	10.9.10.9	88	10.9.10.102	58101	12	3.97K	2	6	0	1.98K	2	0	0
benign	10.9.10.9	88	10.9.10.102	58102	11	3.58K	2	6	0.5	1.79K	34.50	0	0
benign	10.9.10.9	389	10.9.10.102	50666	2	485	2	1	0	242.50	12.50	0	0
benign	10.9.10.9	389	10.9.10.102	58103	20	7.53K	2	10	1	3.77K	172	0	0
benign	10.9.10.9	389	10.9.10.102	58104	15	3.60K	2	8	0.5	1.80K	986	0	0
benign	10.9.10.9	135	10.9.10.102	58086	15	1.67K	2	8	2	834	34	0	0
benign	10.9.10.9	135	10.9.10.102	58094	13	1.34K	2	7	0.5	668	36	0	0
benign	10.9.10.9	49667	10.9.10.102	58096	25	6.29K	2	12.50	0.5	3.15K	769.50	0	0
c2 server	167.172.37.9	443	10.9.10.102	58132	309	307.32K	2	154.50	71.50	153.66K	146.91K	0	0
benign	94.158.245.52	443	10.9.10.102	58136	23	4.88K	2	11.50	2	2.44K	1.67K	0	0
c2 server	94.158.245.52	443	10.9.10.102	58135	25	7.11K	3	8.33	3.09	2.37K	1.56K	0	0
benign	94.158.245.52	443	10.9.10.102	58137	20	4.74K	2	10	1	2.37K	1.64K	0	0
benign	10.9.10.9	49667	10.9.10.102	58148	24	6.67K	2	12	1	3.33K	872.50	0	0
benign	10.9.10.9	389	10.9.10.102	58149	21	7.23K	2	10.50	0.5	3.62K	306	0	0
benign	10.9.10.9	389	10.9.10.102	58150	18	6.69K	2	9	0	3.34K	606	0	0
benign	10.9.10.9	389	10.9.10.102	57208	2	485	2	1	0	242.50	12.50	0	0
benign	10.9.10.9	135	10.9.10.102	58147	11	1.41K	2	6	2	706	82	0	0
c2 server	94.158.245.52	443	10.9.10.102	58138	25	5.31K	2	12.50	2	2.65K	1.82K	0	0
benign	10.9.10.9	53	10.9.10.102	64980	4	280	4	1	0	70	8	0	0

Update Unknown C2 Server to the List



Prepare Training Data Set

↓

Train ML Model

↓

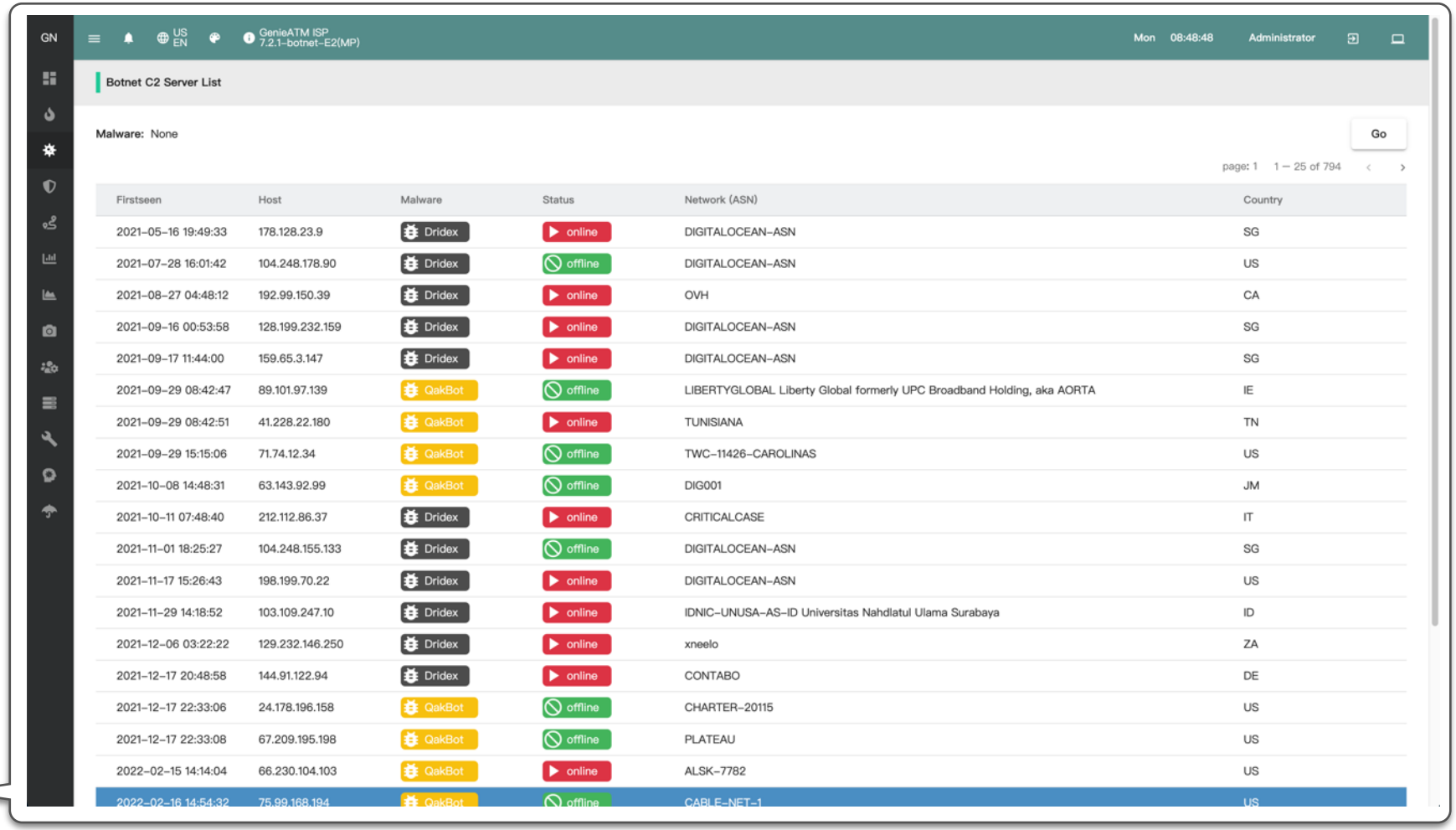
Collect Bot Connection Data Set

↓

Detect Unknown C2 Server

↓

Update C2 Server List



Firstseen	Host	Malware	Status	Network (ASN)	Country
2021-05-16 19:49:33	178.128.23.9	Dridex	online	DIGITALOCEAN-ASN	SG
2021-07-28 16:01:42	104.248.178.90	Dridex	offline	DIGITALOCEAN-ASN	US
2021-08-27 04:48:12	192.99.150.39	Dridex	online	OVH	CA
2021-09-16 00:53:58	128.199.232.159	Dridex	online	DIGITALOCEAN-ASN	SG
2021-09-17 11:44:00	159.65.3.147	Dridex	online	DIGITALOCEAN-ASN	SG
2021-09-29 08:42:47	89.101.97.139	QakBot	offline	LIBERTYGLOBAL Liberty Global formerly UPC Broadband Holding, aka AORTA	IE
2021-09-29 08:42:51	41.228.22.180	QakBot	online	TUNISIANA	TN
2021-09-29 15:15:06	71.74.12.34	QakBot	offline	TWC-11426-CAROLINAS	US
2021-10-08 14:48:31	63.143.92.99	QakBot	offline	DIG001	JM
2021-10-11 07:48:40	212.112.86.37	Dridex	online	CRITICALCASE	IT
2021-11-01 18:25:27	104.248.155.133	Dridex	offline	DIGITALOCEAN-ASN	SG
2021-11-17 15:26:43	198.199.70.22	Dridex	online	DIGITALOCEAN-ASN	US
2021-11-29 14:18:52	103.109.247.10	Dridex	online	IDNIC-UNUSA-AS-ID Universitas Nahdlatul Ulama Surabaya	ID
2021-12-06 03:22:22	129.232.146.250	Dridex	online	xneelo	ZA
2021-12-17 20:48:58	144.91.122.94	Dridex	online	CONTABO	DE
2021-12-17 22:33:06	24.178.196.158	QakBot	offline	CHARTER-20115	US
2021-12-17 22:33:08	67.209.195.198	QakBot	offline	PLATEAU	US
2022-02-15 14:14:04	66.230.104.103	QakBot	online	ALSK-7782	US
2022-02-16 14:54:32	75.99.168.194	QakBot	offline	CABLE-NET-1	US

Unknown C2 Server List Updates

Tracking the IP connections of known C2 server IP addresses, and find out if there's any new unknown C2 Servers thru learned ML models

- Emotet, QakBot, Truebot, TrickBot Malware, Pikabot, BumbleBee, BazarLoader, Dridex, …

The predicted botnet C2 servers, are classified as Unknown C2 Server:

- bot-C2 ML learning models: 10+
- monitoring activities of last week | last 30 days
- data set collection: per day
- detection period: per day
- predicting new C2 Server IP: uncertain; 1 ~ 10+ per day | accumulated 100+ per month
- updated: per hour | per day

Conclusion - ISP's DDoS Protection Strategies

DDoS Mitigation

- auto detecting DDoS victim IP addresses / IP segments
- auto aggregating traffic attributes from tracked attacking traffic
- AI-aided auto-generating FlowSpec policy rules of DDoS mitigation
- mitigating DDoS traffic at attack time

Botnet C2 Blocking

- collecting and updating bot-C2 server IP addresses
- AI-aided finding unknown Bot-C2 server IP addresses
- blocking Bot-C2 servers at all time

THANK YOU!

www.genie-networks.com