Denial of Service Attacks

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Denial of service attacks

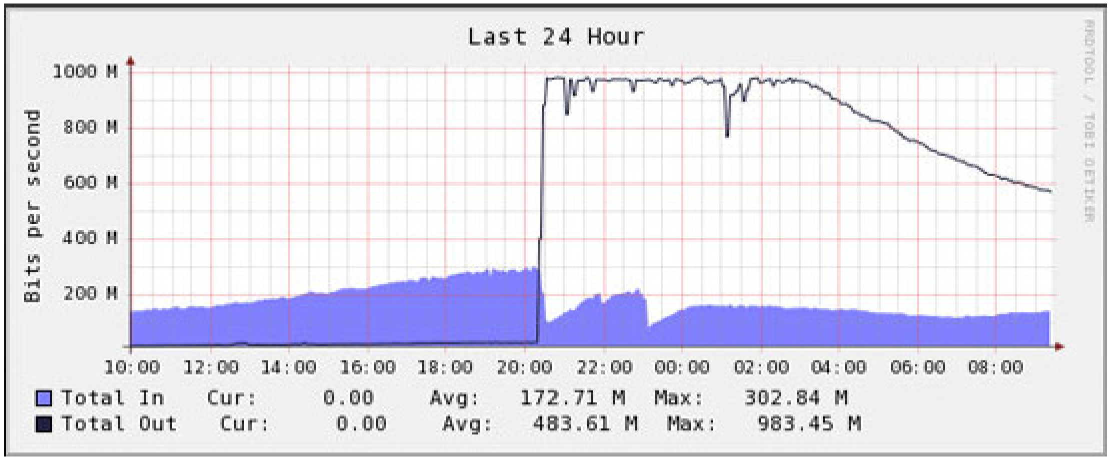
- Attack on service availability
- Saturate the resources of the victim with the amount of traffic or the number of requests so that it becomes unresponsive.
- Some examples:
  - Volumetric attacks – huge traffic throughput
  - TCP state exhaustion attack
  - Application attack
- Distributed DoS – synchronous attack to one target from a large number of systems (bots)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Volumetric attacks

- Send large amount of traffic towards the victim saturating completely the outgoing link
- Some examples – mirai on Deutsche Telecom
- Usually executed as DDoS



ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DoS attack amplification

- Set of bots spoof src IP addr, put the IP address of the victim and send DNS request
- DNS server responds to the victim
- Request is 60 bytes, response around 512 bytes – 8x amplification
- Botnet with 5000 bots for 1Mbps of generated DNS request traffic per bot – 40Gbps of DNS response traffic

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

TCP state exhaustion attacks

- SYN flood attack
  - Attacker sends packets with TCP SYN and fake src IP address
  - Victim creates a state and waits for the handshake to complete, which never happens
- Service request flood attack
  - Server (e.g. web app) is flooded with service request leading to the exhaustion of all resources

```
hping3 target --flood
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Other DoS attacks

- Fragmentation attacks
- Application level service request floods
- Peer to peer DoS attack through a bug in the Direct Connect DC++ p2p protocol – malicious hubs were able to redirect users to any target address.
- Permanent DoS attack - hardware sabotage (including encrypting), phlashing, planting corrupted firmware

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Some DoS tools

- **DoSHTTP** - an HTTP flood DoS tool. It can target URLs, and it uses port designation.
- **UDPFlood** - UDP packets at a specified rate and to a specific network.
- **Jolt2** - IP packet fragmentation DoS tool can send large numbers of fragmented packets to a Windows host.
- **Targa** This eight-in-one tool can perform DoS attacks using one or many of the included options. Attacks Targa is capable of are land, WinNuke, and teardrop attacks.

ISSES

Co-funded by the Erasmus+ Programme of the European Union

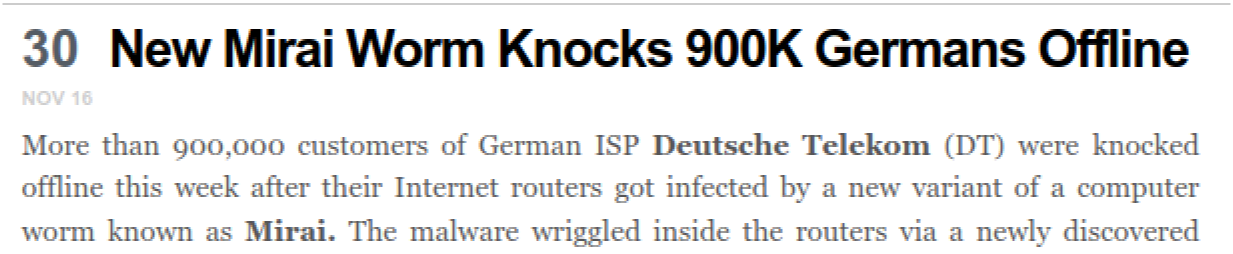
DISTRIBUTED DOS

Botnets

- Bots are machines infected with some virus or trojan, being managed by a Bot master
- Communication models:
  - Push model: master broadcasts his commands
  - Pull model: bots (periodically) ask for a command
- Centralized architecture: One central Command and Control (C&C) centre manages all bots
  - C&C management channel (well known ports)
    - IRC
    - DNS
    - …
- P2p architecture

ISSES Co-funded by the Erasmus+ Programme of the European Union

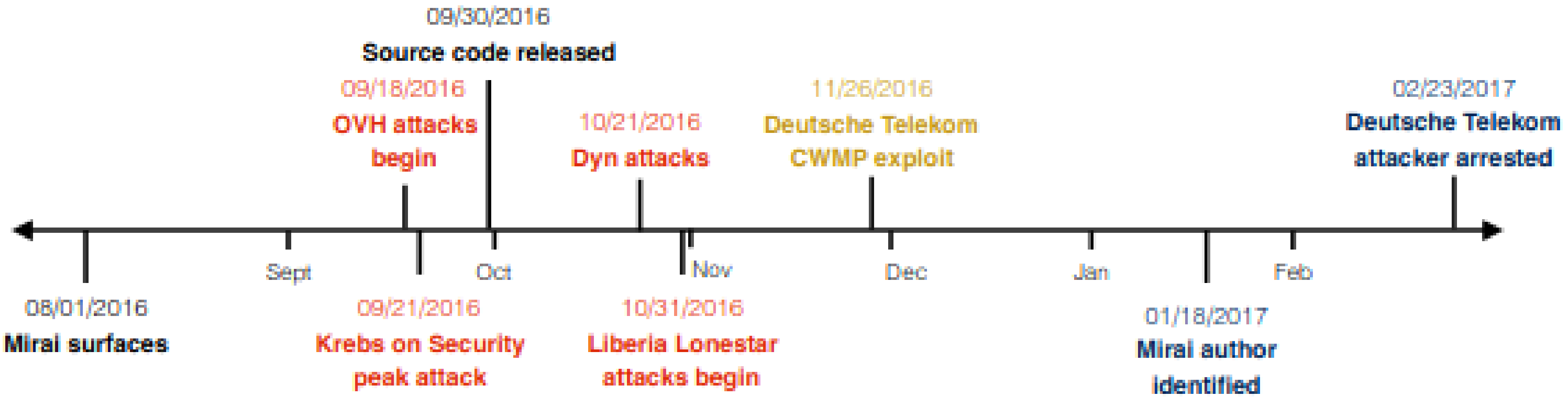
Mirai case study



30 New Mirai Worm Knocks 900K Germans Offline

NOV 16

More than 900,000 customers of German ISP **Deutsche Telekom** (DT) were knocked offline this week after their Internet routers got infected by a new variant of a computer worm known as **Mirai.** The malware wriggled inside the routers via a newly discovered



08/01/2016
Mirai surfaces

09/18/2016
OVH attacks begin

09/21/2016
Krebs on Security peak attack

09/30/2016
Source code released

10/21/2016
Dyn attacks

10/31/2016
Liberia Lonestar attacks begin

11/26/2016
Deutsche Telekom CWMP exploit

01/18/2017
Mirai author identified

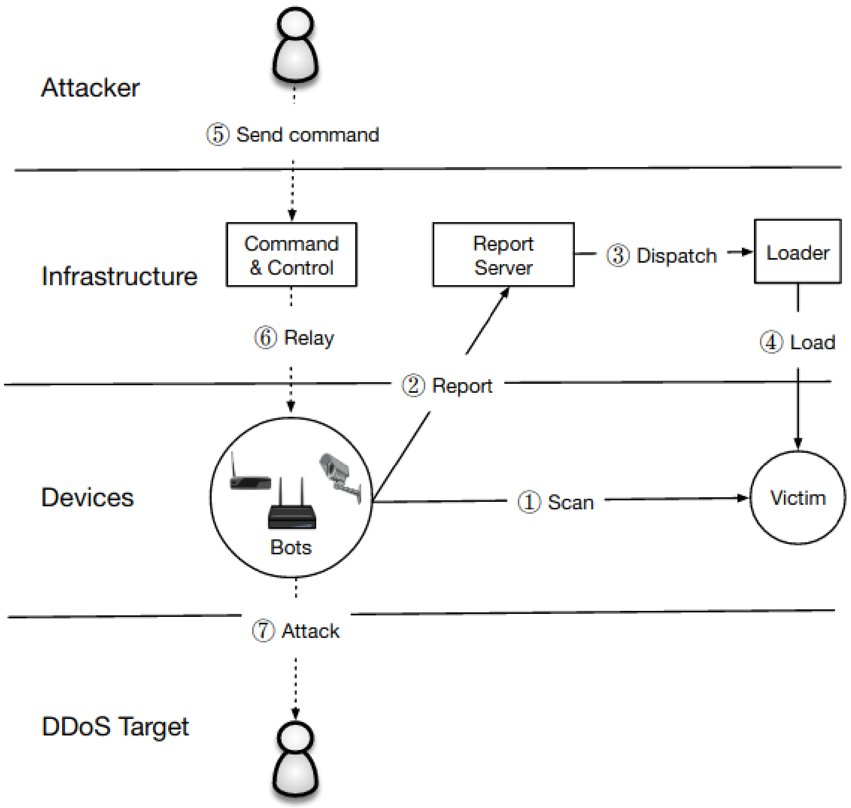
02/23/2017
Deutsche Telekom attacker arrested

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Mirai infection

1. Bots scan other victims (TCP 23 and 2323) and attempt default password login
2. Bot informs report server upon successful login
3. Report server sends malware for the victims OS
4. Malware is loaded into the victim



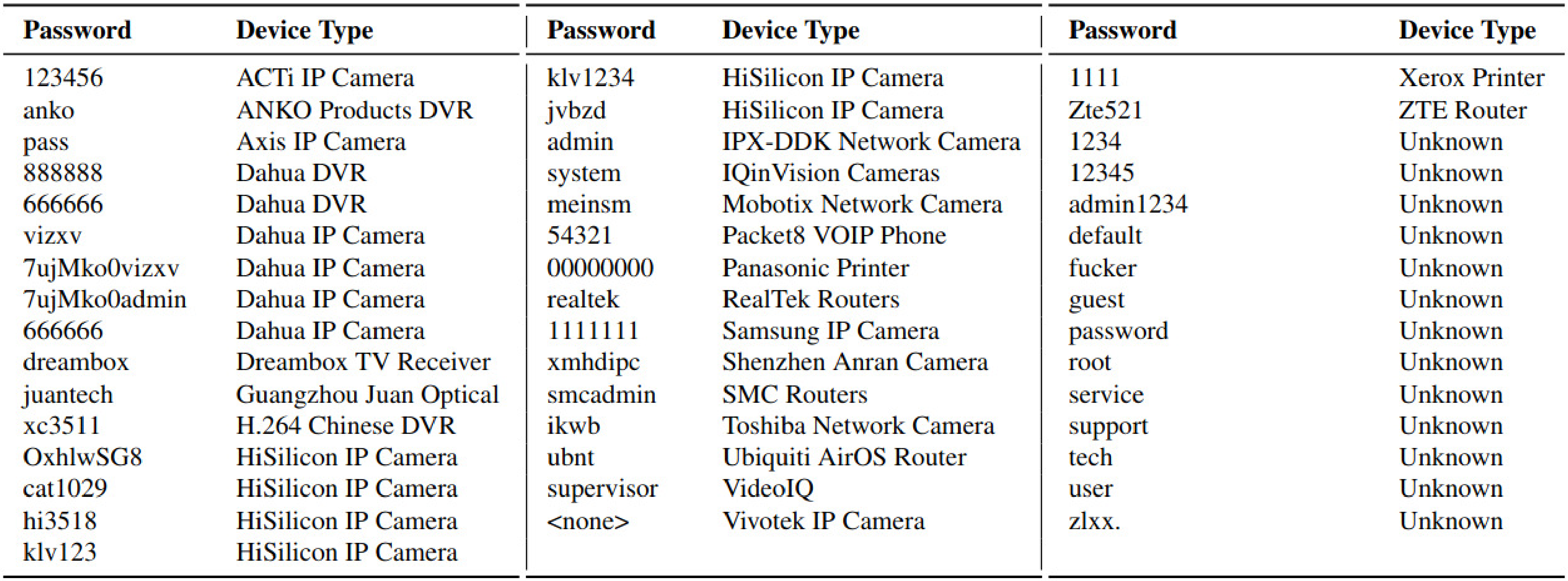
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Mirai operations

- Target devices: IoT cameras, DVR, home routers, modems
- Mirai is a modification of Bashlite
- Mirai used 62 username/password pairs
- Mirai deleted itself after running – no Mirai after restart
- The most common platforms: MIPS 32-bit, ARM 32-bit, and x86 32-bit —which account for 74%

ISSES Co-funded by the Erasmus+ Programme of the European Union

Mirai passwords

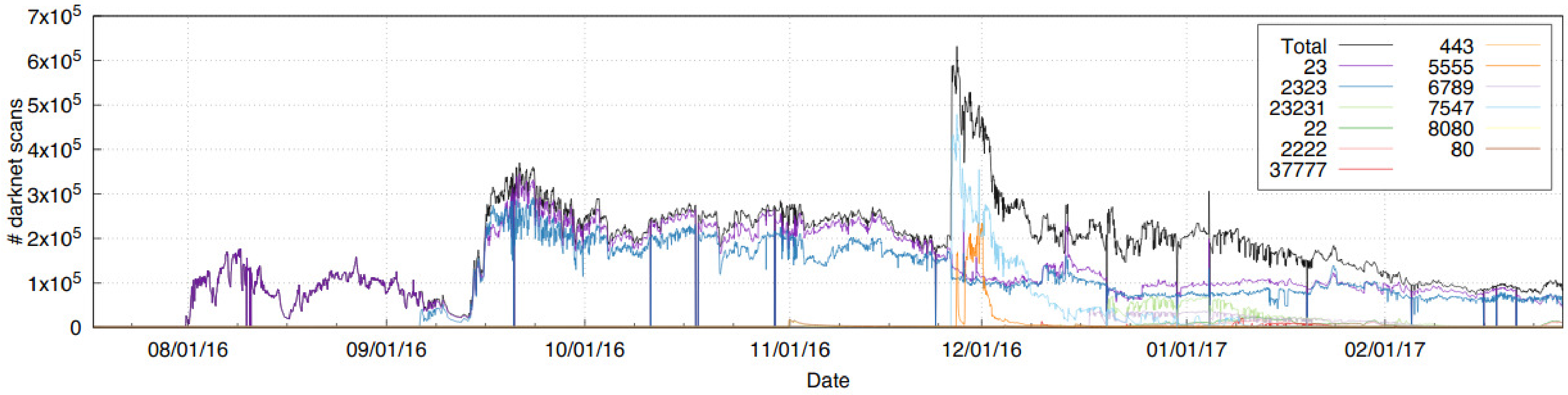


Password	Device Type
123456	ACTi IP Camera
anko	ANKO Products DVR
pass	Axis IP Camera
888888	Dahua DVR
666666	Dahua DVR
vizxv	Dahua IP Camera
7ujMko0vizxv	Dahua IP Camera
7ujMko0admin	Dahua IP Camera
666666	Dahua IP Camera
dreambox	Dreambox TV Receiver
juantech	Guangzhou Juan Optical
xc3511	H.264 Chinese DVR
OxhlwSG8	HiSilicon IP Camera
cat1029	HiSilicon IP Camera
hi3518	HiSilicon IP Camera
klv123	HiSilicon IP Camera
klv1234	HiSilicon IP Camera
jvbzd	HiSilicon IP Camera
admin	IPX-DDK Network Camera
system	IQinVision Cameras
meinsm	Mobotix Network Camera
54321	Packet8 VOIP Phone
00000000	Panasonic Printer
realtek	RealTek Routers
1111111	Samsung IP Camera
xmhdipc	Shenzhen Anran Camera
smcadmin	SMC Routers
ikwb	Toshiba Network Camera
ubnt	Ubiquiti AirOS Router
supervisor	VideoIQ
<none>	Vivotek IP Camera
1111	Xerox Printer
Zte521	ZTE Router
1234	Unknown
12345	Unknown
admin1234	Unknown
default	Unknown
fucker	Unknown
guest	Unknown
password	Unknown
root	Unknown
service	Unknown
support	Unknown
tech	Unknown
user	Unknown
zlxx.	Unknown

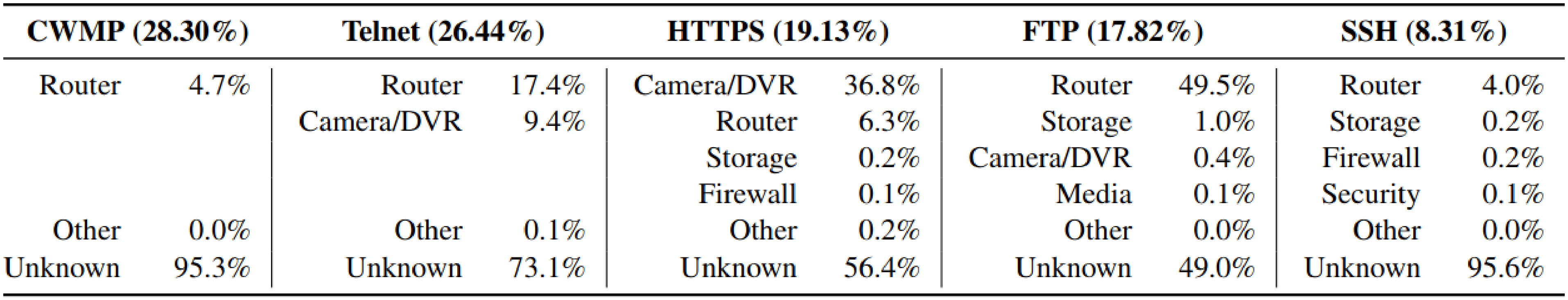
ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Mirai infected devices



CPE WAN Management Protocol



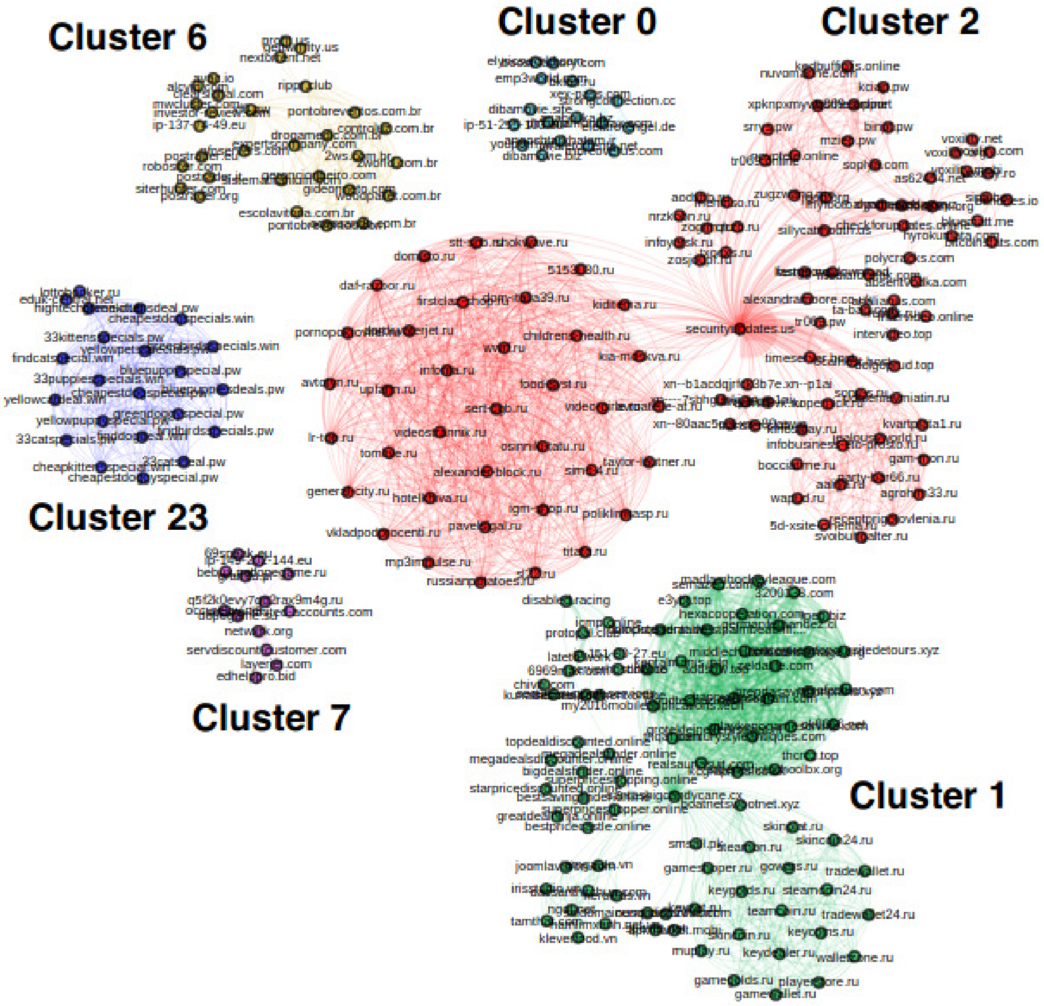
CWMP (28.30%)		Telnet (26.44%)		HTTPS (19.13%)		FTP (17.82%)		SSH (8.31%)	
Router	4.7%	Router	17.4%	Camera/DVR	36.8%	Router	49.5%	Router	4.0%
		Camera/DVR	9.4%	Router	6.3%	Storage	1.0%	Storage	0.2%
				Storage	0.2%	Camera/DVR	0.4%	Firewall	0.2%
				Firewall	0.1%	Media	0.1%	Security	0.1%
Other	0.0%	Other	0.1%	Other	0.2%	Other	0.0%	Other	0.0%
Unknown	95.3%	Unknown	73.1%	Unknown	56.4%	Unknown	49.0%	Unknown	95.6%

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Mirai C&C

- 33 independent clusters with no shared infrastructure
- Multiple botnet operators
- Largest cluster 112 C&C domains and 92 IP addresses



ISSES
Co-funded by the Erasmus+ Programme of the European Union

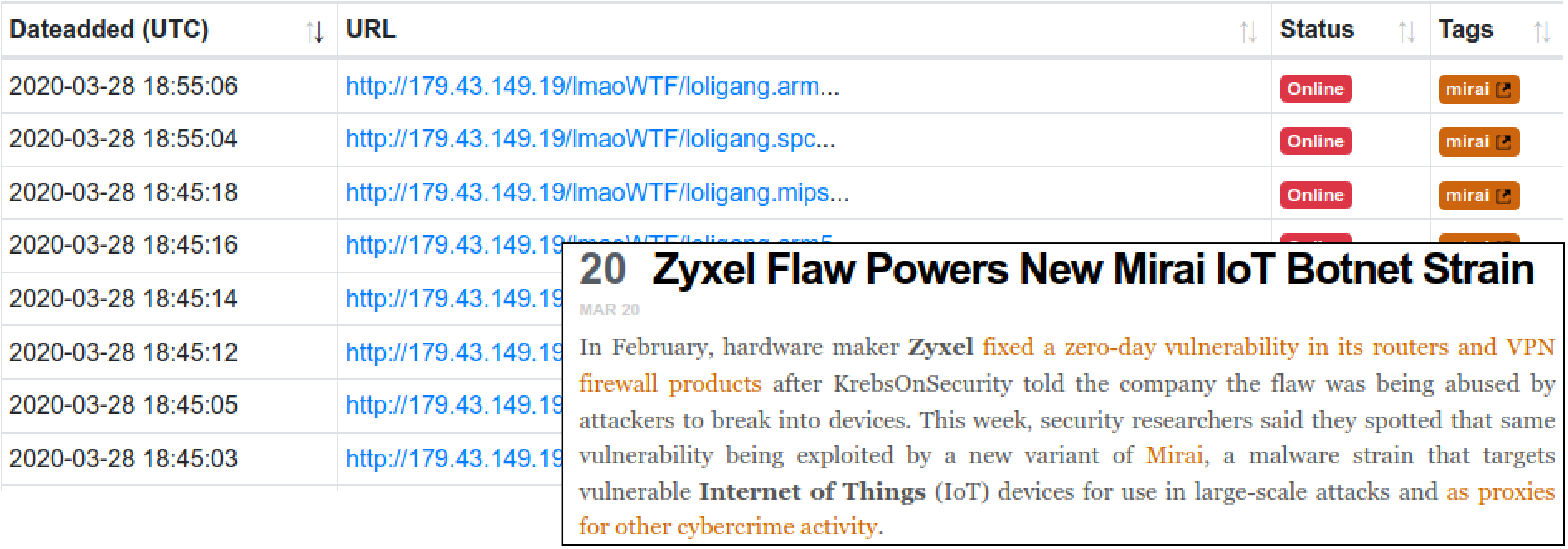
Mirai evolution

- 7.8.2016-30.9.2016. – 24 different variants of Mirai
- Changed from IP-based to DNS-based C&C
- Making reverse engineering more difficult
- Nov 2016 – scanning ports 7545 and 5555 added (CWMP)
- Nov 2016 - Feb 2017 48 new username/password combinations
- Added the list of domains to avoid (DoD, FBI,…)
- One version started to use DGA

Co-funded by the
Erasmus+ Programme
of the European Union

What about today?

- New mirai (and of other “old” botnet malware) derivatives are added daily



Dateadded (UTC)	URL	Status	Tags
2020-03-28 18:55:06	http://179.43.149.19/lmaoWTF/loligang.arm...	Online	mirai
2020-03-28 18:55:04	http://179.43.149.19/lmaoWTF/loligang.spc...	Online	mirai
2020-03-28 18:45:18	http://179.43.149.19/lmaoWTF/loligang.mips...	Online	mirai
2020-03-28 18:45:16	http://179.43.149.19/lmaoWTF/loligang.arm5		
2020-03-28 18:45:14	http://179.43.149.19		
2020-03-28 18:45:12	http://179.43.149.19		
2020-03-28 18:45:05	http://179.43.149.19		
2020-03-28 18:45:03	http://179.43.149.19		

20 Zyxel Flaw Powers New Mirai IoT Botnet Strain

MAR 20

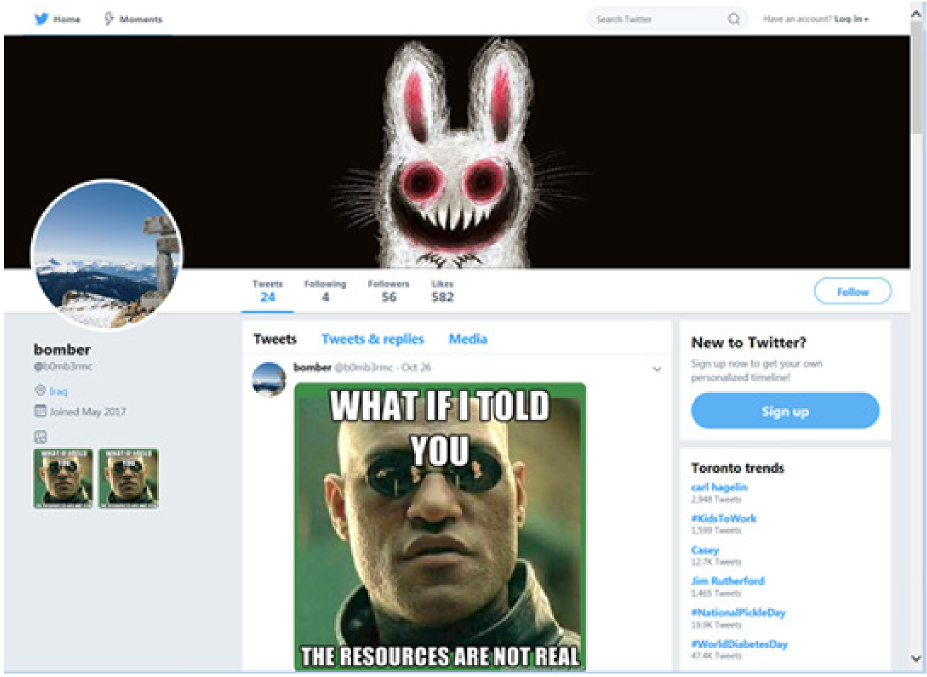
In February, hardware maker **Zyxel** fixed a zero-day vulnerability in its routers and VPN firewall products after KrebsOnSecurity told the company the flaw was being abused by attackers to break into devices. This week, security researchers said they spotted that same vulnerability being exploited by a new variant of Mirai, a malware strain that targets vulnerable **Internet of Things** (IoT) devices for use in large-scale attacks and as proxies for other cybercrime activity.

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Other botnet C&C

- P2P (Zeus, Sality, Confiker)
- Hybrid (Miner, later versions of Zeus)
- IRC (GTBot)
- Twitter malicious memes (sociobot, TROJAN.MSIL.BERBOMTHUM.AA)



bomber
@b0mb3rmc
Iraq
Joined May 2017

bomber @b0mb3rmc · Oct 26

New to Twitter?
Sign up now to get your own personalized timeline!

Toronto trends
carl hagelin
2,948 Tweets
#KidsToWork
1,599 Tweets
Casey
12.7K Tweets
Jim Rutherford
1,465 Tweets
#NationalPickleDay
19.9K Tweets
#WorldDiabetesDay
47.4K Tweets

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Botnet spreading methods

- Random address scanning
- Hit-list scanning
- Topological scanning (search for URLs on infected machine and use them)
- Subnet scanning (devices on the same subnet as infected bot – behind firewalls)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DDoS tools

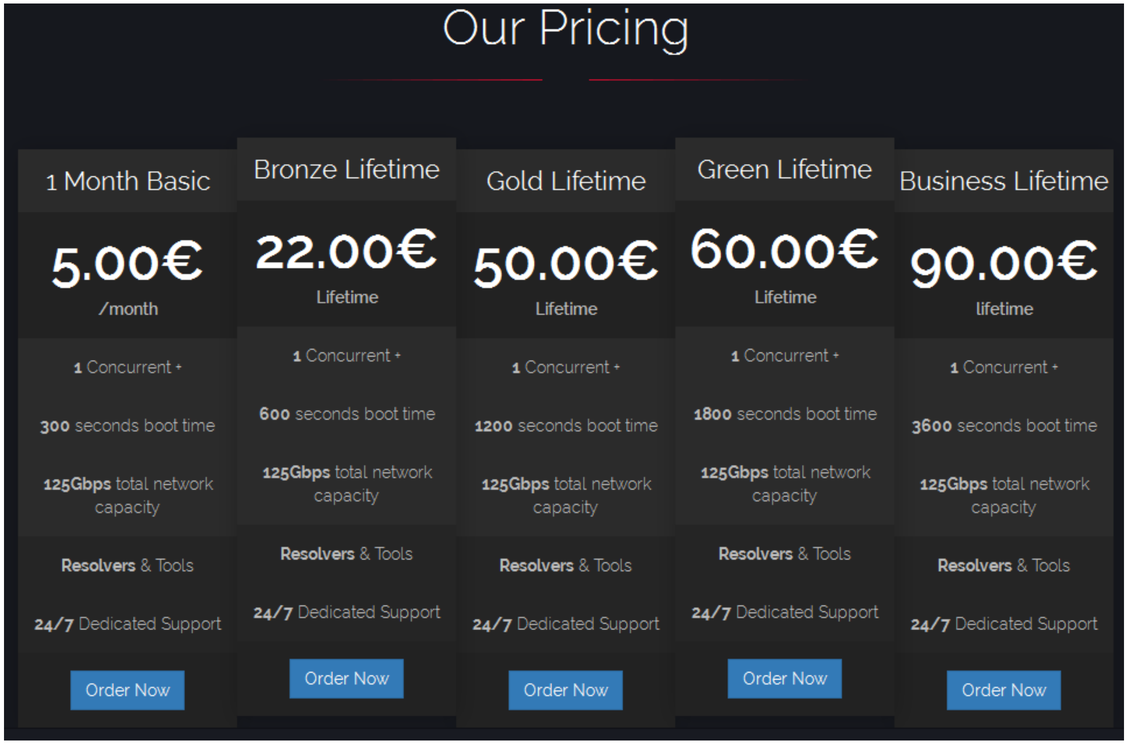
- **Trinoo** - uses UDP flooding. It can attack single or multiple IPs.
- **LOIC** Low Orbit Ion Cannon (LOIC) has become popular because of its easy one-button operation. Some people suspect that groups such as Anonymous, which uses DDoS attacks as its primary weapon, use LOIC as their main tool.
- **TFN2K** - based on TFN (Tribe Flood Network) and can perform UDP, SYN, and UDP flood attacks.
- **Stacheldraht** - similar attack capabilities as TFN2K. Attacks can be configured to run for a specified duration and to specific ports.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Botnets can be rented

- It is cheap to perform a DDoS attack (2019: 9$/hour, 67$/day)



Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

MITIGATING DOS ATTACKS

Mitigation methods

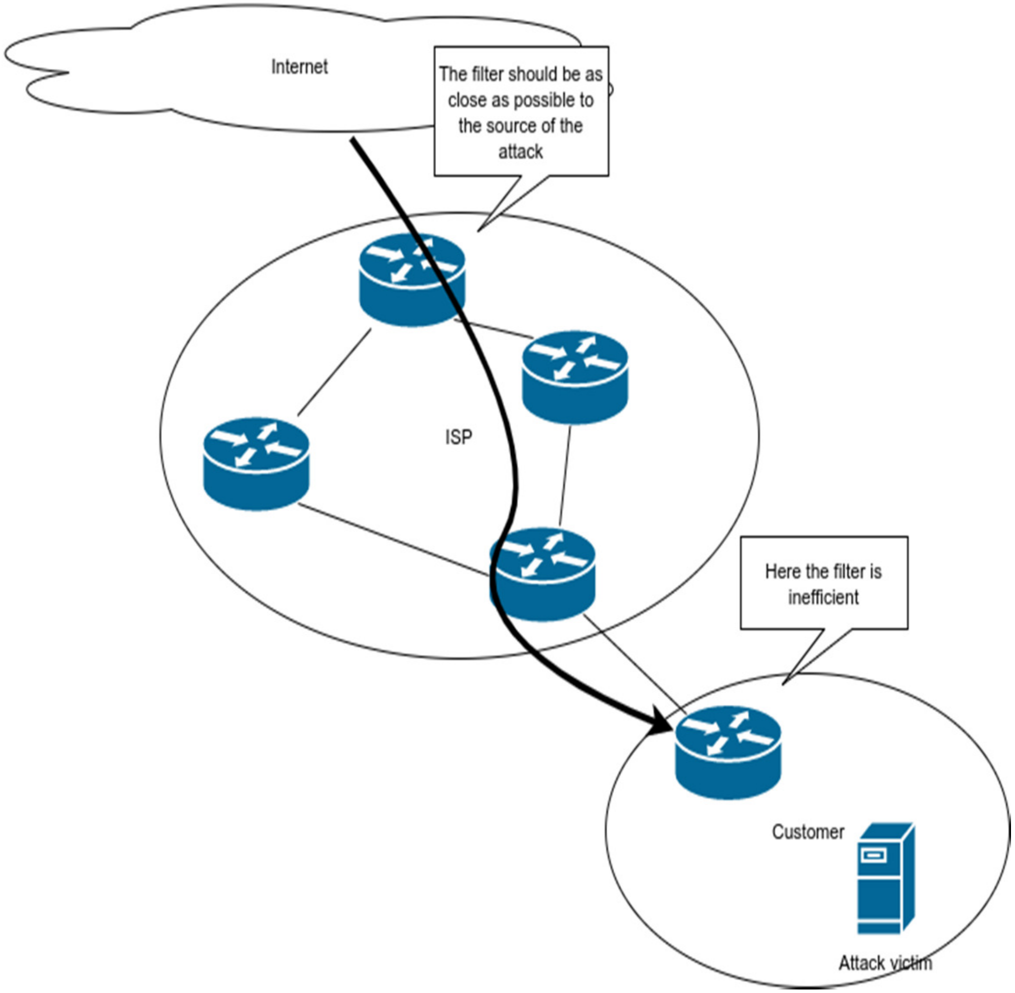
- RFC 3704/8704 filtering (unicast RPF)
- IPS/IDS (anomaly based)
- Reputation filtering
- TCP intercept (for TCP exhaustion attacks)
- Detect C&C
- Detect malware

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Mitigation strategy

- Effective mitigation has to be done upstream of the victim as close as possible to the attack source.
- Once the traffic reaches the victim, it has succeeded
- Filtering per-source address is not practical (e.g. 50K filter rules for 50K size botnet)
- ISPs offer DDoS protection as a service


Internet
The filter should be as close as possible to the source of the attack
ISP
Here the filter is inefficient
Customer
Attack victim

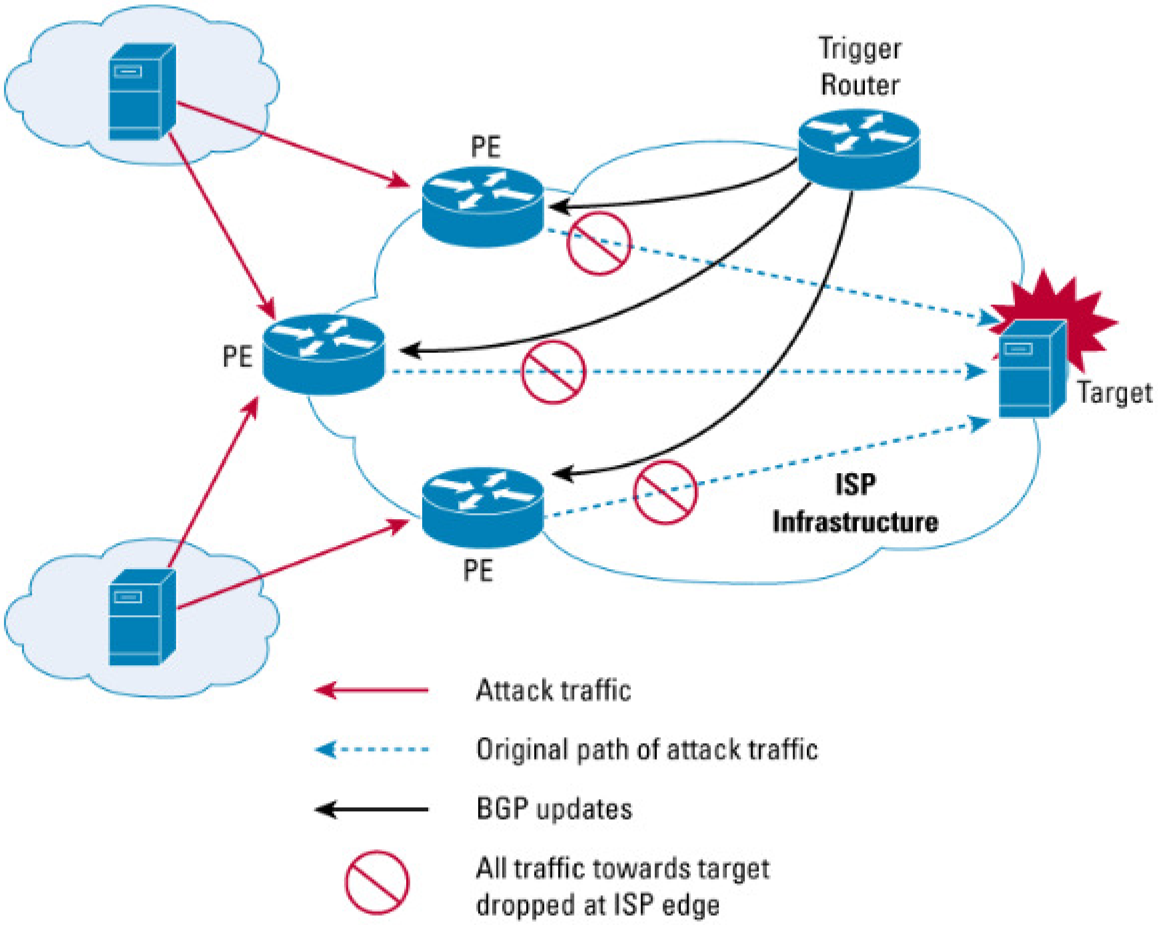
BGP RTBH

- RTBH – Remotely Triggered Black Hole filtering
- Send BGP route updates for the DoS victim to the upstream provider. The route points to the Null interface (drops packets)
- Designated trigger router sends BH updates
- Destination based RTBH – filters everything towards a victim destination
- Source based RTBH (RFC 5636) – filter based on the source address. If the source address is in the routing table, pa packet can enter

ISSES

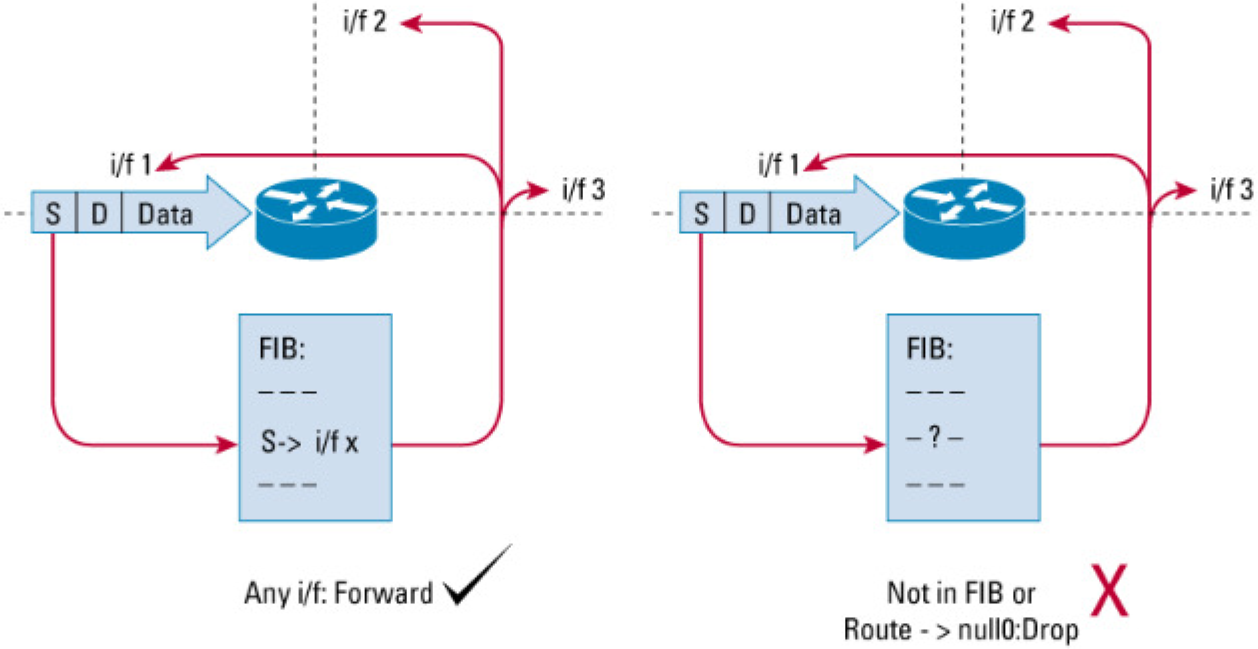
Co-funded by the
Erasmus+ Programme
of the European Union

Destination based RTBH



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

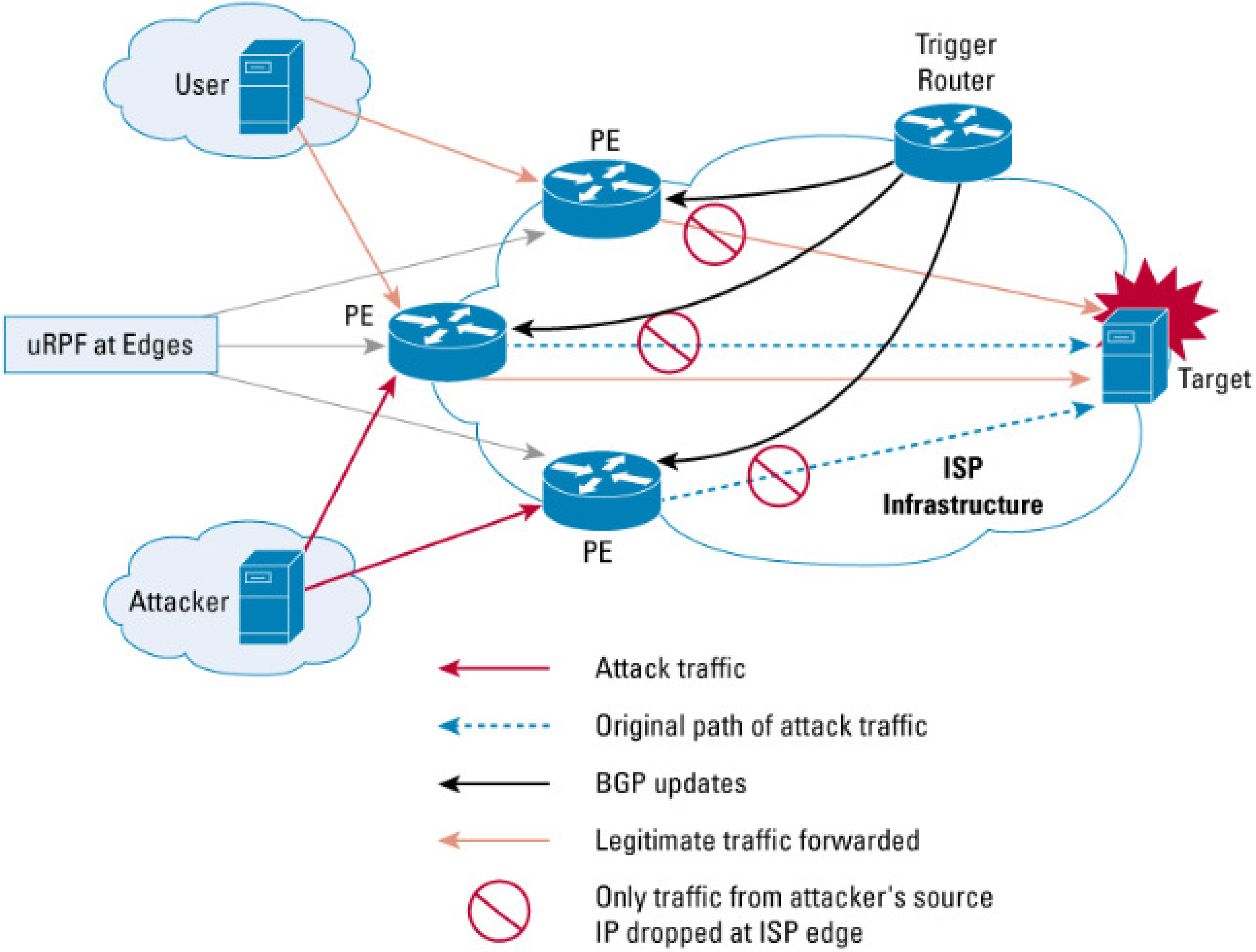
Source based RTBH



ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Source based RTBH


User
Trigger Router
PE
PE
uRPF at Edges
Target
ISP Infrastructure
PE
Attacker
Attack traffic
Original path of attack traffic
BGP updates
Legitimate traffic forwarded
Only traffic from attacker's source IP dropped at ISP edge

ISSES
Co-funded by the Erasmus+ Programme of the European Union

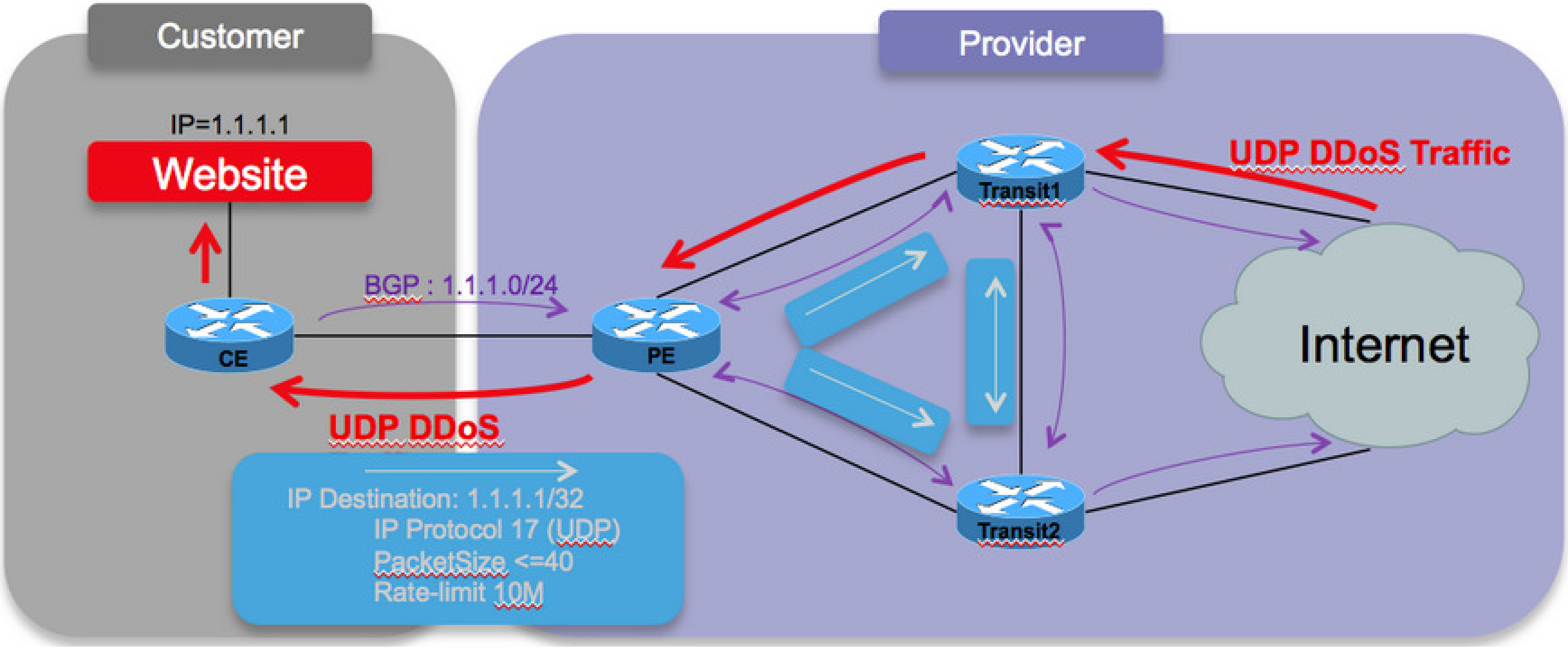
BGP Flowspec

- BGP flowspec allows for a more granular approach than RTBG
- BGP flowspec effectively construct instructions to match a particular flow with source AND destination, and L4 parameters and packet specifics such as length, fragment etc, and allow for a dynamic installation of an action at the border routers to either:
  - drop the traffic
  - inject it in a different vrf (for analysis)
  - or allow it, but police it at a specific defined rate.

ISSES Co-funded by the Erasmus+ Programme of the European Union

BGP Flowspec - example

- Customer creates a rule which defines a rate limit for a specific attack traffic



IP Destination: 1.1.1.1/32
IP Protocol 17 (UDP)
PacketSize <=40
Rate-limit 10M

ISSES
Co-funded by the Erasmus+ Programme of the European Union