Útočí se po IPv6 ?

On-line seminář nejen o IPv6, 4. 6. 2021

Tomáš Košňar, CESNET

Útočí se po IPv6 ?

- **z pohledu transportu přes páteřní síť e-infrastruktury CESNET**
- **síťové útoky, ~ „nestandardní“ chování**
- před léty „hýčkaná“ data v případě detekce nestandardního provozu
- aktuálně opakovaně/průběžně detekovaný výskyt
  - scans (tcp, udp)
    - občas i relativně agresivní
    - plošné i cílené (MS porty, „amplifikační“ porty, atd.)
  - „náznaky“ amplifikace (53, ..)
  - agresivita dotazů na resolvery (~součást amplifikačního útoku ?)

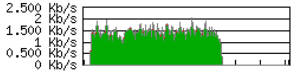
Útočí se po IPv6 ?

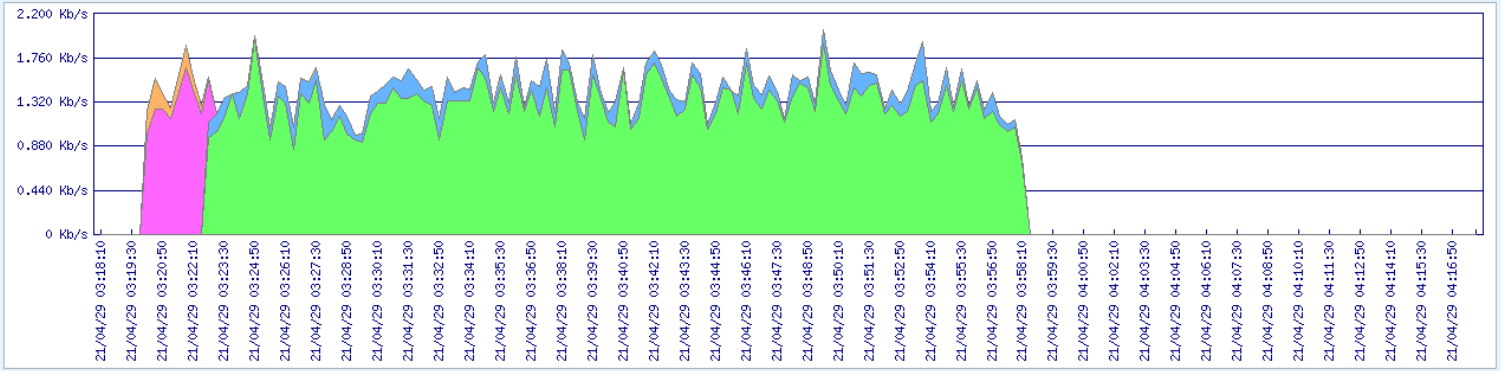
- ukázka - pomalý neagresivní TCP SYN + UDP scan + summary za delší dobu

Bytes-estimated: *rates, 21/04/29 03:18:00-21/04/29 04:18:00, value per 20 seconds, cumulative*

Summary

In graph	416.666 KB	100.00%
Rest of results	0.000 KB	0.00%
Total	416.666 KB	100.00%





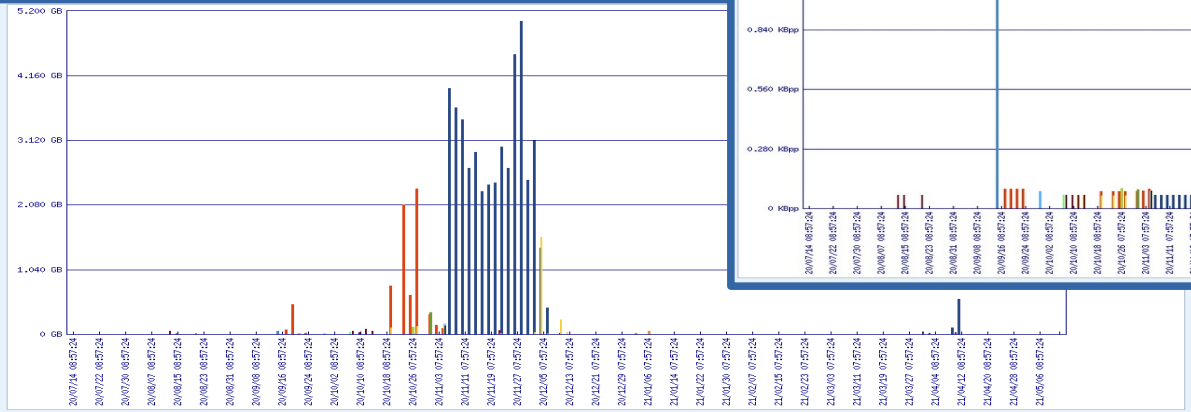
		Flow-Direction	FWD-Status	Src-IP	Protocol	TOS-flags	TCP-flags	Bytes-estimated	Pkts-estimated	Dst-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
1.	>	ingress	Drop RPF	2[redacted]1:c:0:0:0:3	tcp (6)	00000000	syn(2)	350.272 KB ~ 84.065%	5.473 Kp ~ 83.672%	5362	4786	132	64	5473 ~ 83.762%
2.	>	ingress	Drop RPF	2[redacted]1:c:0:0:0:3	udp (17)	00000000		35.934 KB ~ 8.624%	591.000 p ~ 9.035%	584	579	18	60.80	585 ~ 8.953%
3.	>	ingress	Forwarded	2[redacted]1:c:0:0:0:3	tcp (6)	00000000	syn(2)	26.880 KB ~ 6.451%	420.000 p ~ 6.421%	420	414	102	64	420 ~ 6.428%
4.	>	ingress	Forwarded	2[redacted]1:c:0:0:0:3	udp (17)	00000000		3.580 KB ~ 0.859%	57.000 p ~ 0.871%	56	55	14	62.81	56 ~ 0.857%

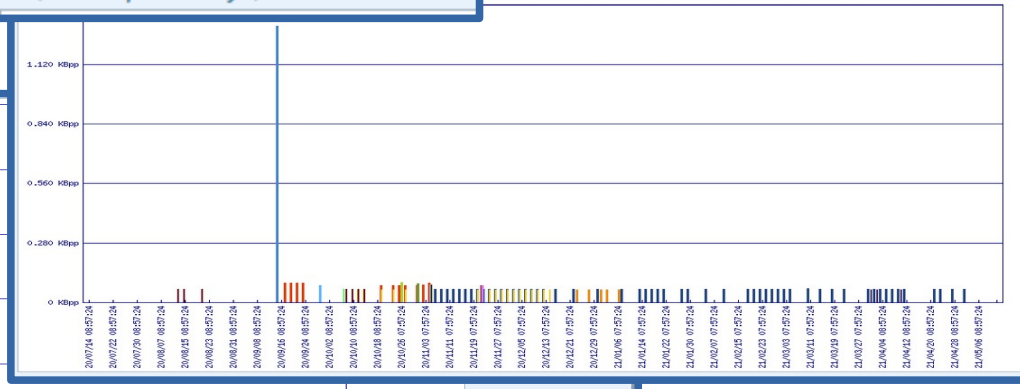
o	FWD-Status	Src-IP	Protocol	TCP-flags	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured	Dst-IP-Cnt	Flow-Cnt
1.	Drop RPF	[redacted]c:0:0:0:3	tcp (6)	syn(2)	21/04/29 03:22:47.564	21/05/12 16:28:28.810	46.632 MB ~ 79.281% → 318.760 b/s	728.629 Kp ~ 81.542% → 0.623 p/s	173035	728626 ~ 81.683% → 0.623 flows/s
2.	Drop RPF	[redacted]c:0:0:0:3	udp (17)		21/04/29 03:22:49.714	21/05/12 16:28:26.118	10.941 MB ~ 18.601% → 74.787 b/s	146.100 Kp ~ 16.350% → 0.125 p/s	92374	144629 ~ 16.214% → 0.124 flows/s
3.	Forwarded	[redacted]c:0:0:0:3	tcp (6)	syn(2)	21/04/29 03:20:01.279	21/05/12 15:22:05.348	970.176 KB ~ 1.649% → 6.653 b/s	15.159 Kp ~ 1.696% → 0.013 p/s	14389	15159 ~ 1.699% → 0.013 flows/s
4.	Forwarded	[redacted]c:0:0:0:3	udp (17)		21/04/29 03:20:06.381	21/05/12 15:22:05.873	275.531 KB ~ 0.468% → 1.890 b/s	3.670 Kp ~ 0.411% → 0.003 p/s	3555	3607 ~ 0.404% → 0.003 flows/s

Útočí se po IPv6 ?

- IPv6 – detekce, 10 měsíců, top-list

Bytes-estimated: *sums/time steps, 20/07/13 08:57:24-21/05/13 08:57:24, value per 2 days, non-cumulative*





o	>	Src-IP	Src-GeoIP	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt	Detected-Event-Cnt	Detector-Type	Detector-Name
1.	>	[redacted]:c:0:0:0:3		47.148 GB ~ 81.602%	736.673 Mp ~ 83.997%	64.00	8216369 ~ 83.710%	114560 ~ 94.657%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
2.	>	[redacted]:1:0:0:0:3a		6.999 GB ~ 12.114%	85.669 Mp ~ 9.768%	81.70	989637 ~ 10.083%	638 ~ 0.527%	Src-IP	Possible attacks to DNS resolvers, to port 53, sources
3.	>	[redacted]:0:2700:30:1270:f9c2:7897		2.118 GB ~ 3.666%	35.303 Mp ~ 4.025%	60.00	305854 ~ 3.116%	4431 ~ 3.661%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
4.	>	[redacted]:1:0:0:0:58		348.876 MB ~ 0.604%	3.965 Mp ~ 0.452%	87.98	2740 ~ 0.028%	65 ~ 0.054%	Src-IP	Possible attacks to DNS resolvers, to port 53, sources
5.	>	[redacted]:-0:89:185:233:204		301.353 MB ~ 0.522%	4.709 Mp ~ 0.537%	64	58858 ~ 0.600%	581 ~ 0.480%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
6.	>	[redacted]:f:c16c:4420:4bc7:1d8f		175.864 MB ~ 0.304%	2.093 Mp ~ 0.239%	84.02	26085 ~ 0.266%	62 ~ 0.051%	Src-IP	Possible attacks to DNS resolvers, to port 53, sources
7.	>	[redacted]:1:0:0:0:ad		136.395 MB ~ 0.236%	1.624 Mp ~ 0.185%	84.01	20294 ~ 0.207%	81 ~ 0.067%	Src-IP	Possible attacks to DNS resolvers, to port 53, sources
8.	>	[redacted]:1:0:0:0:12		120.954 MB ~ 0.209%	1.279 Mp ~ 0.146%	94.55	15570 ~ 0.159%	53 ~ 0.044%	Src-IP	Possible attacks to DNS resolvers, to port 53, sources
9.	>	[redacted]:1d0:0:0:242:f000		89.237 MB ~ 0.154%	1.476 Mp ~ 0.168%	60.45	13139 ~ 0.134%	105 ~ 0.087%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
10.	>	[redacted]:1d0:0:0:cf:5000		73.958 MB ~ 0.128%	1.233 Mp ~ 0.141%	60	15408 ~ 0.157%	154 ~ 0.127%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
11.	>	[redacted]:901:0:1:9bfc:a8ea		64.419 MB ~ 0.111%	805.232 Kp ~ 0.092%	80	24359 ~ 0.248%	63 ~ 0.052%	Src-IP	TCP SYN from internal IP address ranges
12.	>	[redacted]:1:0:0:0:42		54.452 MB ~ 0.094%	41.850 Kp ~ 0.005%	1301.12	7 ~ 0.000%	1 ~ 0.001%	Src-IP	IPv6 UDP lower-rate amplification, reflection - targets internal
13.	>	[redacted]:0:0:0:1:10		30.561 MB ~ 0.053%	477.520 Kp ~ 0.054%	64	5969 ~ 0.061%	17 ~ 0.014%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
14.	>	[redacted]:7:23:4a4d:7eff:fea4:5c1a		29.991 MB ~ 0.052%	374.892 Kp ~ 0.043%	80	93723 ~ 0.955%	61 ~ 0.050%	Src-IP	TCP SYN against internal IP address ranges from outside, sources
15.	>	[redacted]:901:0:1:9bfc:a8ea		20.320 MB ~ 0.035%	254.000 Kp ~ 0.029%	80	3175 ~ 0.032%	36 ~ 0.030%	Src-IP	TCP SYN against internal IP address ranges from outside, sources

Útočí se po IPv6 ?

- je IPv6 svět z pohledu tranzitní sítě „klidnější a bezpečnější“ ?
  - *IPv6 detekované síťové události za 6 měsíců*

o	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt
1.	10.036 GB	158.935 Mp	63.14	1715813	1461672	22049

- vs.
  - *IPv4 detekované síťové události za 6 měsíců (stejná metodika, stejné limity detektorů)*

o	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt
1.	573.084 TB	1.424 Tp	402.51	4691670126	3428605495	8017074

- … **0.274 : 99.726** …???

Útočí se po IPv6 ?

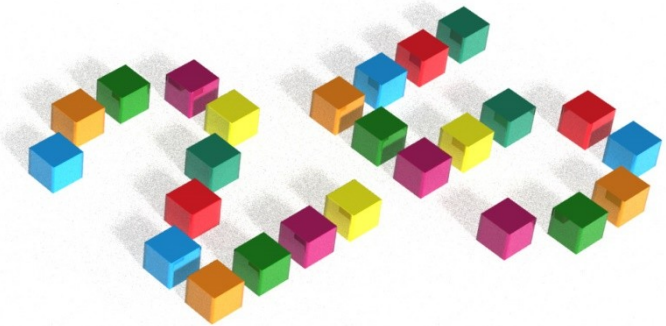
- odpovídající IPv6 : IPv4 ?
  - v tomto konkrétním případě a odpovídajících místech pozorování ~ **17 : 83**
- tak je to bezpečnější nebo ne ;-) ?

v6

o	Protocol	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt
1.	tcp (6)	87.098%	84.989%	1200.27	65.510%
2.	udp (17)	12.870%	14.861%	1036.97	32.183%
3.	ipv6-icmp (58)	0.017%	0.109%	183.64	2.254%
4.	ip-encap (4)	0.014%	0.039%	442.79	0.018%
5.	ospfigp (89)	0.000%	0.001%	80.17	0.015%
6.	ip (0)	0.000%	0.001%	183.41	0.016%
7.	esp (50)	0.000%	0.000%	224.09	0.002%
8.	pim (103)	0.000%	0.000%	108.17	0.002%
9.	ipv6-nonxt (59)	0.000%	0.000%	40	0.000%

v4

o	Protocol	Bytes-estimated	Pkts-estimated	Avr-Pkt-Length	Flow-Cnt
1.	tcp (6)	78.159%	73.798%	1119.42	75.947%
2.	udp (17)	20.464%	24.616%	789.50	22.459%
3.	esp (50)	1.175%	1.259%	845.83	0.079%
4.	gre (47)	0.127%	0.138%	978.77	0.069%
5.	icmp (1)	0.049%	0.166%	255.25	1.437%
6.	ip-encap (4)	0.019%	0.015%	1207.00	0.001%
7.	ipv6 (41)	0.006%	0.008%	703.58	0.006%
8.	ospfigp (89)	0.000%	0.000%	81.52	0.001%
9.	pim (103)	0.000%	0.000%	48.06	0.001%
10.	etherip (97)	0.000%	0.000%	68	0.000%
11.	vrrp (112)	0.000%	0.000%	56	0.000%
12.	igmp (2)	0.000%	0.000%	29.38	0.000%



Děkuji za pozornost!

Útočí se po IPv6 ?