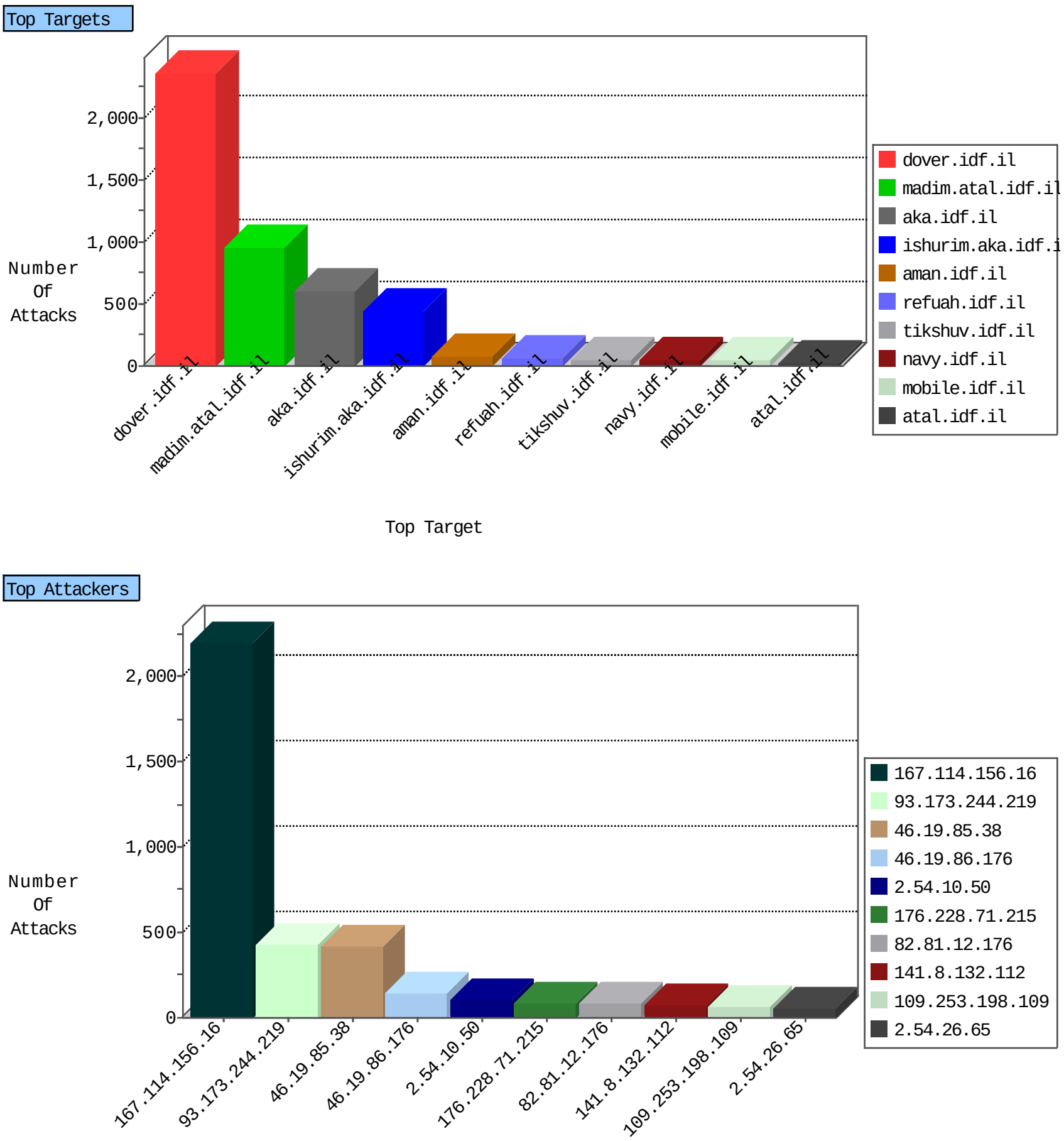
01-24-2016-13:04:06 to 01-24-2016-14:04:06

IDF Under Attack Daily Report



01-24-2016-13:04:06 to 01-24-2016-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3030
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	81
79.182.220.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

01-24-2016-13:04:06 to 01-24-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.63.71.182		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-24-2016-13:04:06 to 01-24-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.177.209.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

01-24-2016-13:04:06 to 01-24-2016-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.244.219	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	408
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
2.54.10.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.219.193.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
93.173.244.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.179.208.184	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.248	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
109.64.106.246	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
2.54.10.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
2.54.10.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.54.10.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
149.62.201.196	Bulgaria	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
185.3.147.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.10.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
176.106.46.74	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
109.64.106.246	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.130.222.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.180.125.210	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.10.50	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	9
85.130.222.182	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.219.44	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
85.130.222.182	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
2.54.40.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.219.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.253.201.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.77.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.120.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.14.96	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.130.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.200.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.220.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.14.96	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.22.135.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.2.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.47.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
85.130.222.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.40.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	234
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	146
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
176.228.71.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
109.253.198.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
2.54.26.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
37.26.147.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.38	Block	37
176.13.19.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
185.120.126.74		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
80.178.203.76	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
79.179.134.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.1.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.178.222.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
176.13.17.157	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.120.233.241	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.233.241	Block	9
37.26.147.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.134.212	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	6
185.120.126.74		147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	6
80.179.192.126	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
109.253.196.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.158.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.209.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.171.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.130.219.44	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
37.26.147.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	3
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
109.253.197.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.230.97	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.182.96.48	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
81.218.50.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sacahr	Block	2
79.182.96.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.5.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.193.165	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method Â¬UÂ±:SÂªNÃ…Â«buX[[#17]]wÃˆ	Block	1
37.59.62.43	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.59.62.43	Block	1
85.64.28.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.35.253.161	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1361-he/dover.aspx	Block	1
5.29.176.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.61.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1