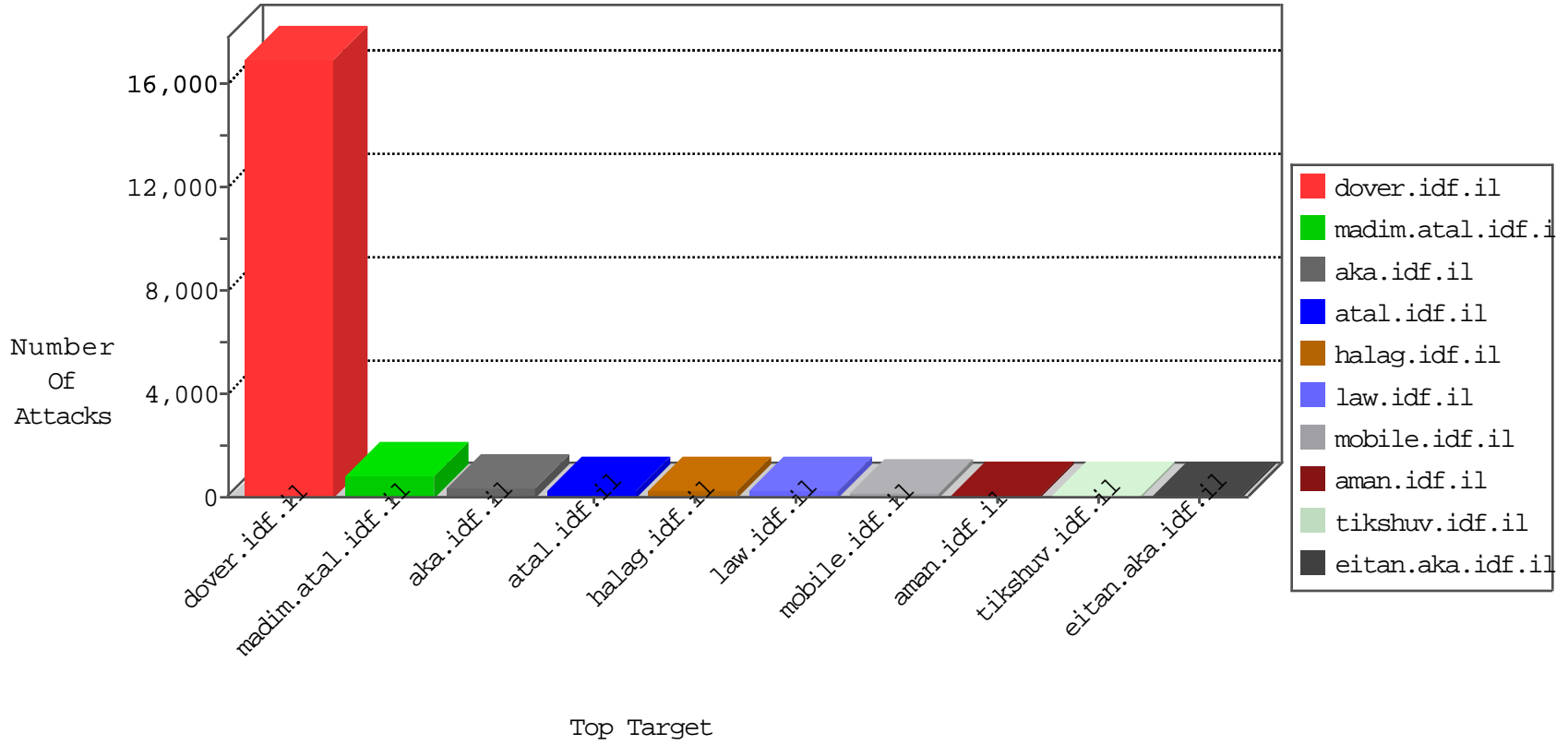


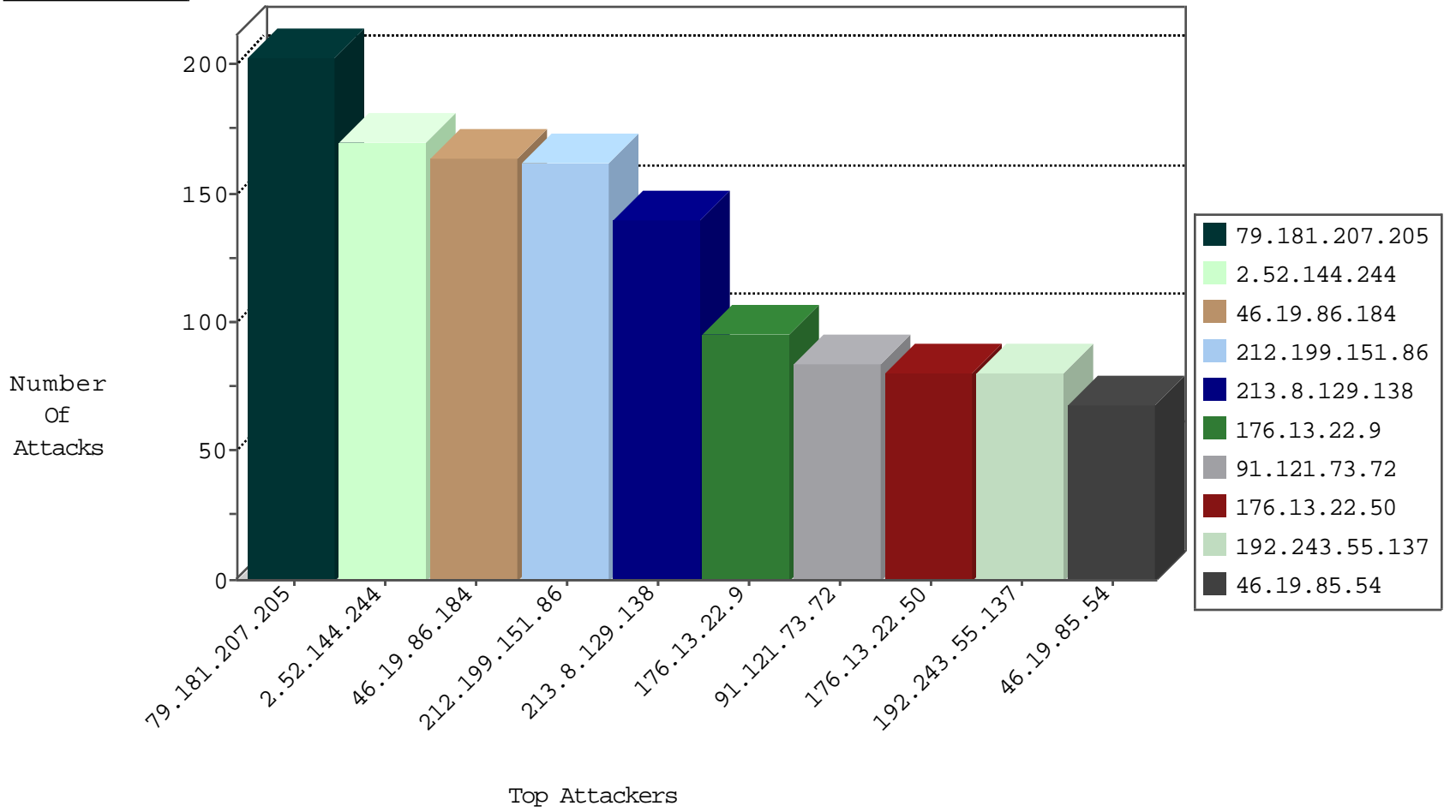
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
247.245.0.129		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35637
67.228.197.144	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34709
53.112.78.3	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34499
62.121.106.1	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34481
70.158.115.121	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34431
183.136.192.39	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34275
143.179.246.229	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34226
235.160.48.137		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34051
81.253.158.72	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34003
40.235.148.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33991
213.47.43.83	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33944
128.72.14.215	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33931
119.91.255.205	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33929
41.189.107.65	Cote D'Ivoire	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33819
110.229.47.48	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33792
78.248.155.57	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33729
126.129.58.140	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33665
185.97.171.49		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33632
234.50.138.170		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33597
174.94.38.245	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33594
152.5.171.203	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33548
123.185.202.128	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33538
129.184.14.229	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33512
40.56.236.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33509
198.62.94.25	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33485
117.239.154.30	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33450
44.160.227.123	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33440
77.100.85.151	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33277
189.146.197.55	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33274
245.75.245.112		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33218
250.4.89.191		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33181
116.97.148.204	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33173
96.177.88.85	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33108
253.63.65.129		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33107
207.40.246.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33093
118.171.230.101	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33045
89.65.161.183	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33023
29.120.175.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32966
2.2.134.106	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32964
55.172.74.96	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32940
159.92.3.121	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32936
34.221.164.123	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32912
172.11.70.222	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32876
47.24.76.70	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32848
8.41.143.114	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32815
144.105.3.108	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32611
188.142.137.118	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32587
101.196.214.190	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32530
150.27.252.113	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32519
46.149.102.201	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32487

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.78.161.110	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
192.116.55.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
37.26.147.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.119.127.64	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.108.170.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.64.86.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.64.175.211	Russian Federation	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
240.0.4.146		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.111.206		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.149.89		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.182.158		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.230.0		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.78.63		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.115.239		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.47.15		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.124.159		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.141.154		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.165.142		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.177.223		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.19.76		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.104.129		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.160.99		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.210.152		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.250.195		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.114.37		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.169.77		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.206.219		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.255.204		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.31.192		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.108.128		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.113.70		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.128.240		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.135.114		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.136.131		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.246.111		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.6.15.115		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.6.22.254		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.6.68.5		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.6.179.159		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.6.219.0		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.7.3.65		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.7.100.231		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.7.132.120		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.180.8.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.120.125.27	147.237.72.166		aka.idf.il	ET SCAN NMAP -sA (2)	2
109.200.30.168	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.148	India	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
77.126.164.57	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
109.65.188.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.64.252.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
93.113.125.11	147.237.0.200	Romania	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
194.90.131.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.155.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.161.187.91	147.237.72.217	Mexico	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.94.164.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
159.122.254.212	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.13.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.148	India	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
79.176.202.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.18.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.67.237.220	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.65.128.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
194.90.198.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
192.243.55.137	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.156.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.42.39.126	147.237.77.74	Brazil	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.167.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.96.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.148	India	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
79.179.110.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.207.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	197
80.246.133.224	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
176.13.22.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
91.121.73.72	France	147.237.72.156	aman.idf.il	drop	SAM rule	drop	42
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	42
80.246.133.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
79.182.21.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
85.250.209.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
94.159.208.240	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
176.13.22.9	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
109.67.173.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
176.13.22.9	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
185.130.5.193		147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
176.13.22.50	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
213.57.154.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
81.199.122.188	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.111.197.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
85.130.239.243	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
85.130.239.243	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.168.93.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
85.130.239.243	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.149.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.22.50	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
177.208.52.28	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
89.139.155.213	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
2.54.62.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.144.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
212.199.151.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
213.8.129.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
176.13.22.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
93.172.156.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	7
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
109.186.191.80	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.191.80	Block	4
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
5.29.71.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
80.230.17.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.8.204.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.147.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
185.112.248.32		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
94.159.208.240	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.133.73	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.146.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.203.203	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
79.178.144.251	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.154.161	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.22.134.233	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.64.252.91	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.64.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.250.0.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.161.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.183.39.170	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
2.54.35.245	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.64.252.91	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
188.162.166.150	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.mag.idf.il/templates/getfile/getfile.aspx	Block	1
109.64.252.91	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
80.246.133.224	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.147.175	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.10.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.26.230	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.154.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
109.186.191.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
109.64.252.91	Israel	147.237.72.166	aka.idf.il	Malformed URL >	Block	1
207.241.229.224	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
185.89.217.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.138.224.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1