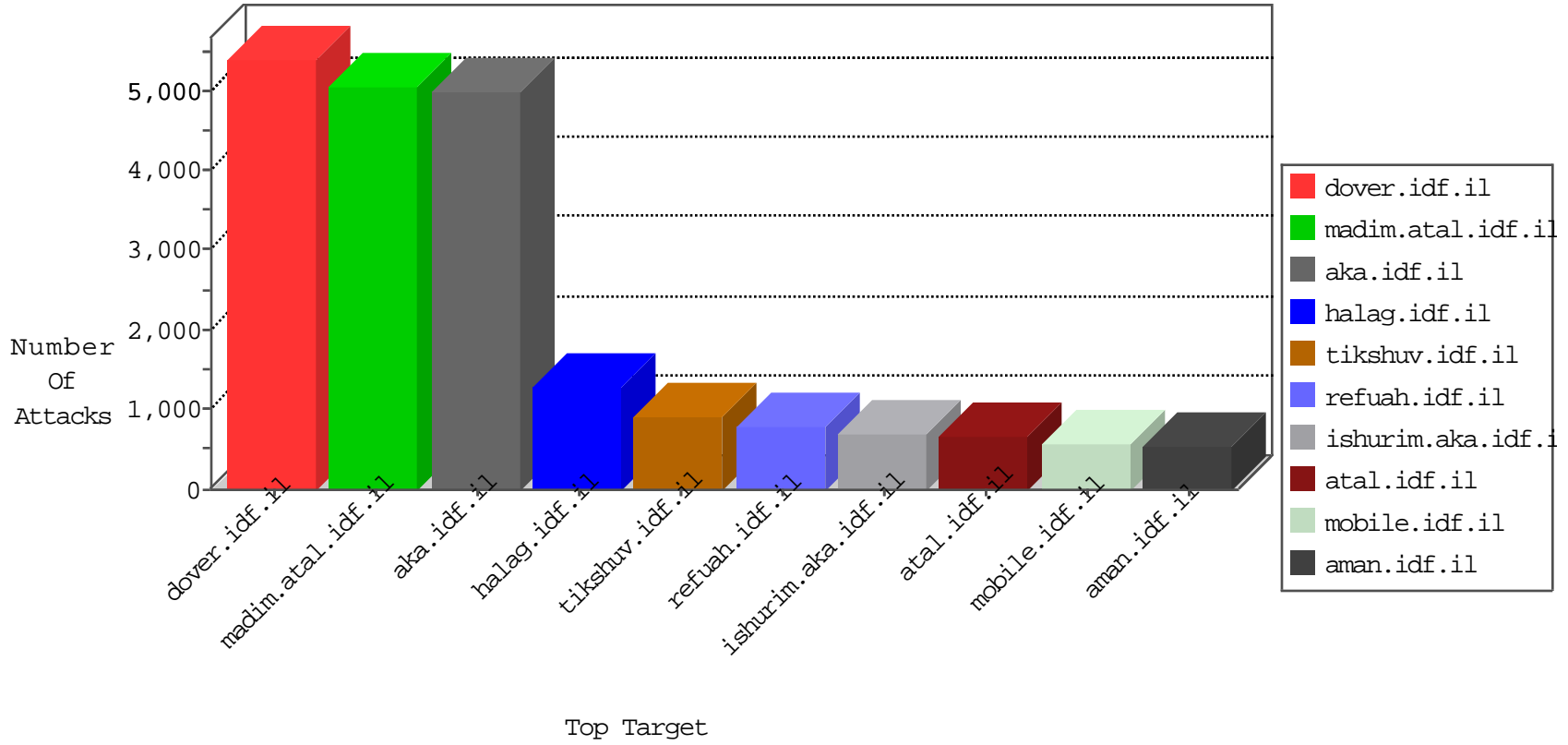


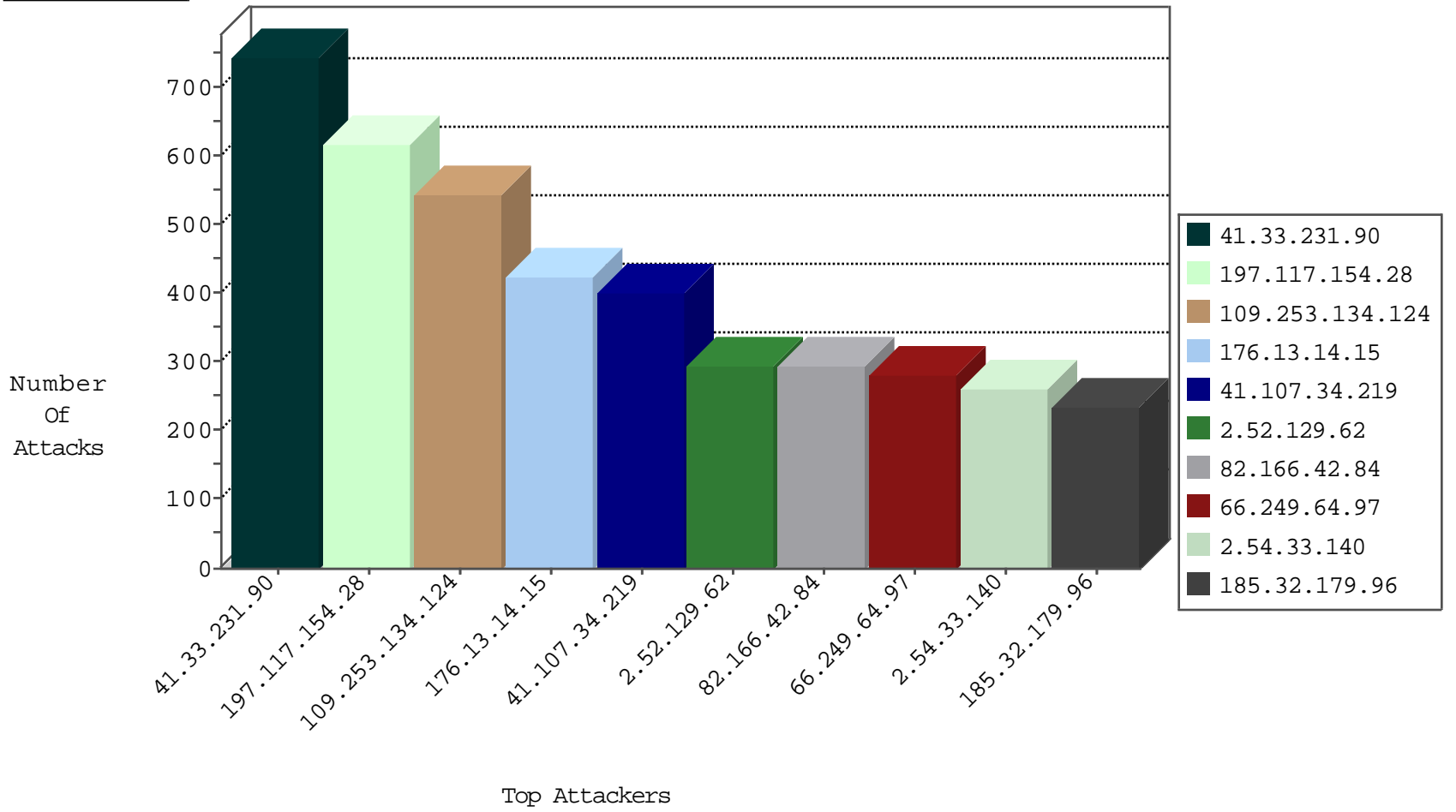
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	897
197.117.154.28	Algeria	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	617
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	603
41.107.34.219	Algeria	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	327
82.145.222.65	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	37
54.72.182.187	Ireland	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	34
82.145.211.122	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	21
200.9.67.2		147.237.77.216	doover.idf.il	TCP handshake violation, first packet not syn	drop	17
79.180.120.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	15
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	I4 Source or Dest Port Zero	drop	10
217.26.171.188	Moldova, Republic of	147.237.76.176	test.noore.idf.il	I4 Source or Dest Port Zero	drop	8
176.13.4.248	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	8
212.199.182.150	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	6
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
79.183.171.153	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.65.188.38	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.47	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	5
185.40.4.95		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	5
82.145.220.162	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	5
185.40.4.95		147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	5
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	drop	4
82.145.209.95	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	4
82.145.216.188	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	3
82.81.12.22	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
79.183.175.80	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
109.66.25.80	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
197.211.44.107	Nigeria	147.237.8.28	e.mobile-ks.idf.il	I4 Source or Dest Port Zero	drop	3
109.65.49.86	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
37.26.146.217	Israel	147.237.77.216	doover.idf.il	Invalid TCP Flags	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
185.103.252.5		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
119.41.216.161	China	147.237.76.176	test.noore.idf.il	Invalid TCP Flags	drop	2
79.183.175.80	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
109.66.25.80	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
222.74.220.18	China	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	2
119.41.216.161	China	147.237.76.177	noore.idf.il	Invalid TCP Flags	drop	2
61.178.192.220	China	147.237.77.235	sviva.idf.il	Invalid TCP Flags	drop	2
222.74.220.18	China	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	2
118.213.224.138	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	2
185.94.111.1		147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	2
185.40.4.95		147.237.0.16	ny-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
202.133.60.114	India	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	2
123.130.244.18	China	147.237.76.148	ggcenter.aka.idf.il	Invalid TCP Flags	drop	2
113.240.42.26	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
184.105.139.124	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	90
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	60
61.135.189.122	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
79.181.201.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
79.180.149.131	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
5.29.88.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
176.228.166.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
10.0.0.11		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
149.78.36.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
149.78.87.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.182.219.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
188.120.148.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
85.250.204.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
188.120.148.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
81.218.241.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.179.149.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
77.125.143.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
89.138.13.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.182.25.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.88.188.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
80.179.114.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.102.229.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	9
46.117.252.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.67.172.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	8
46.116.80.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
217.132.13.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.163.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.64.2.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
95.86.112.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.163.60	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.121.137.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
217.132.16.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.176.7.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.80.56.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.71.5.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
51.254.141.46	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
213.8.10.14	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.194.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
62.219.137.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	280
66.249.93.15	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	100
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	69
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
185.99.32.3	147.237.77.233		atal.idf.il	ET SCAN NMAP -sA (2)	6
185.32.179.133	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
62.90.154.230	147.237.72.166	Israel	aka.idf.il	Tehila - Perl LWP with fake user agent	5
109.253.221.90	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
80.246.133.154	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
120.55.90.163	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	2
218.24.171.223	147.237.76.177	China	noore.idf.il	GPL SCAN nmap TCP	2
66.249.93.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.84.166	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.99.32.3	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sA (2)	2
31.168.203.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
80.246.133.96	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
45.32.80.167	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
84.110.145.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.93.121	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
217.194.197.154	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
188.120.148.133	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
59.46.193.114	147.237.76.177	China	noore.idf.il	GPL SCAN nmap TCP	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
100.116.148.180	147.237.77.216		dover.idf.il	GPL SCAN nmap TCP	2
94.102.48.193	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.1.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.118.11.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.51.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.61.228.113	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.126.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.215.19.235	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
62.232.207.210	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.0.35	Indonesia	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.178	India	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
40.113.118.99	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
95.211.239.230	147.237.72.156	Netherlands	aman.idf.il	OS-OTHER Cisco IOS HTTP configuration attempt	1
80.179.16.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.10.64.39	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.172.21.120	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.82	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 2048	1
91.231.192.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.56	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	717
82.166.42.84	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	295
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
2.54.39.191	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
82.166.248.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	131
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
77.125.142.5	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	118
2.52.15.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	94
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	92
79.183.193.249	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	83
69.31.51.245	Anonymous Proxy	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	80
204.93.58.62	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	76
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
41.107.34.219	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	71
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
212.179.226.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
80.246.130.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
46.117.16.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	57
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
103.50.11.142		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
91.121.101.78	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	55
109.253.193.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	49
173.208.136.170	United States	147.237.0.15	kosher-kravi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	48
46.117.67.124	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
176.13.20.254	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
80.246.130.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
79.176.198.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
80.100.6.253	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
62.128.48.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
79.176.220.113	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
80.246.133.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
80.246.130.250	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
86.90.164.108	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.15.231	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.133.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
100.118.147.236		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
109.65.242.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	34
79.178.129.7	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
94.159.177.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
109.65.218.90	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	31
185.120.125.56		147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.134.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	546
176.13.14.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	424
2.52.129.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	292
2.54.33.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	262
2.54.144.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	225
185.32.179.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	220
185.32.179.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	172
2.52.162.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	172
37.142.238.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
109.253.144.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
109.253.147.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
213.57.182.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
176.13.17.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
109.253.201.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
176.13.7.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.199.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.54.44.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
37.26.146.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.176.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.16.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
37.26.148.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.139.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.156.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.147.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.21.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.147.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
5.102.198.193	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	32
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
93.172.249.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
5.28.168.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.155.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.196.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.6.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.15.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.220.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
188.225.182.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	23
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
77.125.241.82	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	20
109.253.138.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.203.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18