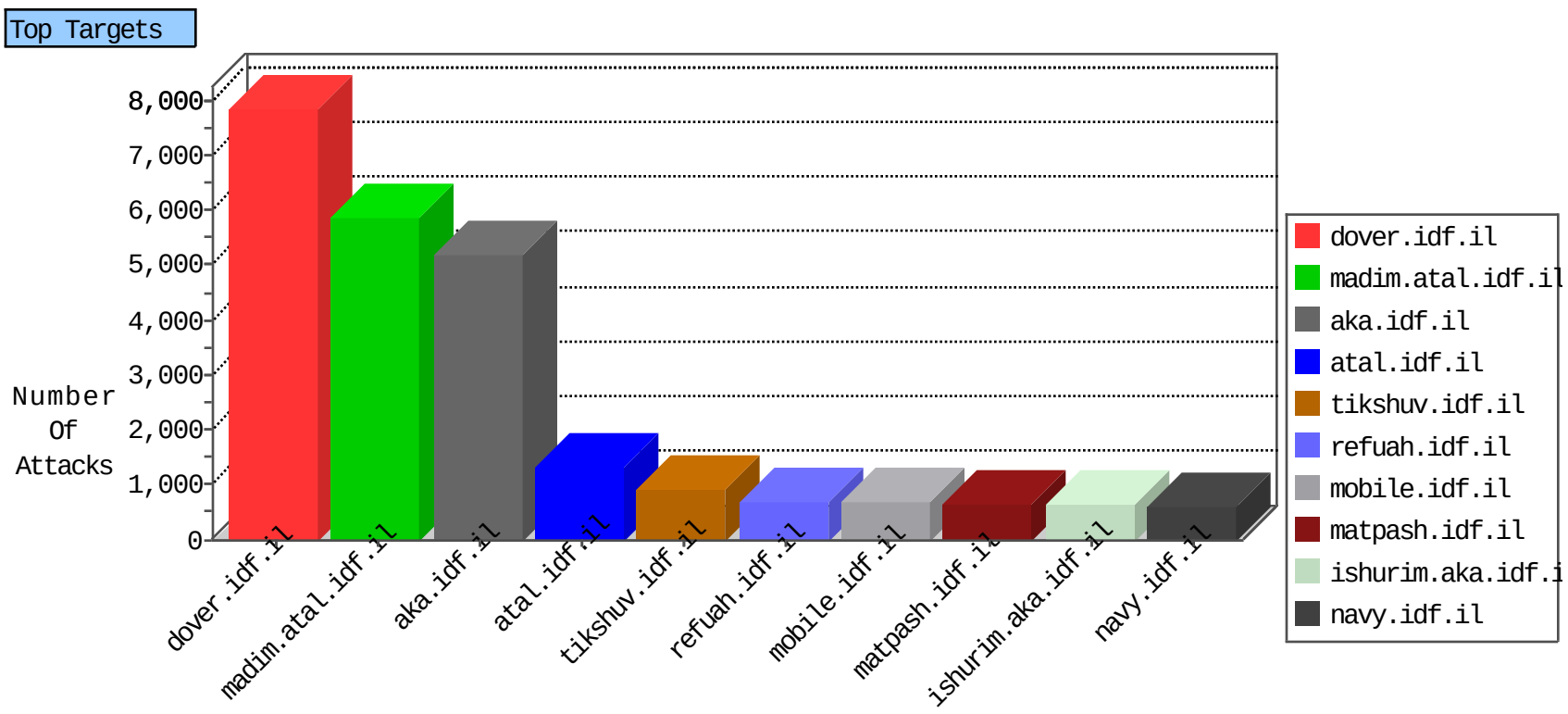
03-08-2016 to 03-09-2016

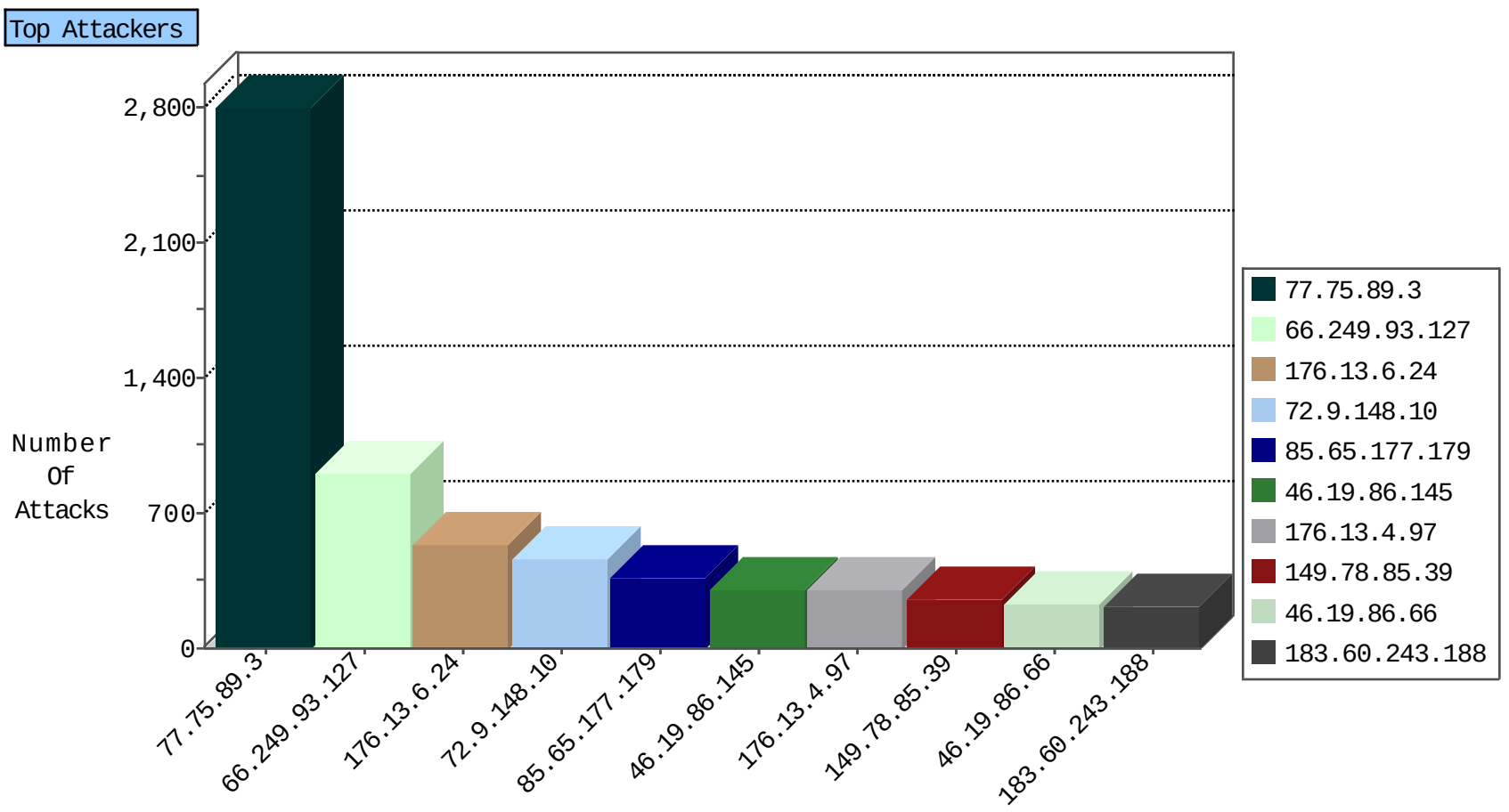
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-08-2016 to 03-09-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	704
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	508
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	354
220.99.175.82	Japan	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	244
212.150.171.253	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	133
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	72
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	69
82.145.211.173	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	35
81.45.180.180	Spain	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	35
82.145.217.167	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
2.54.176.7	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
80.179.99.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
109.253.132.219	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
82.145.222.249	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
82.145.216.114	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
109.253.147.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
2.52.34.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
82.145.211.7	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
82.145.221.66	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
31.154.41.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
80.178.158.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
193.81.79.142	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
79.176.197.214	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
199.203.84.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
79.176.197.214	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
176.13.16.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
82.145.216.114	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.253.132.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.179.31.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.221.12	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
176.13.4.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.52.191.36	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.52.28.255	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
84.94.235.30	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.218.26	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.218.152	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
82.145.210.238	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
2.54.176.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
109.253.195.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.182.162.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.136.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4

03-08-2016 to 03-09-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	51
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	30
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	29
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
93.173.37.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	15
213.57.197.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	12
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
213.8.204.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
217.132.105.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.178.11.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
5.22.130.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
31.168.99.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.45.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.52.32.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
217.132.130.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.230.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.28.135.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.142.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.67.104.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.48	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
212.199.205.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
147.235.185.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.50.97.138	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
132.64.102.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.8.204.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.140.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
64.31.44.6	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
42.101.152.49	China	147.237.77.176	matpash.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	4
2.54.55.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
93.173.244.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.210.170.165	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
87.106.179.116	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
67.228.38.74	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
85.250.88.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.29.26.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
177.185.194.138	Brazil	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
62.210.170.165	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4

03-08-2016 to 03-09-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	877
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	68
212.142.148.244	147.237.76.42	Spain	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	18
152.115.70.227	147.237.77.74	Denmark	law.idf.il	SQL Injection - Select From	12
177.185.194.138	147.237.76.86	Brazil	navy.idf.il	SQL Injection - Select From	12
176.13.6.24	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
80.246.130.207	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
64.31.44.6	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
216.185.43.135	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
67.228.38.74	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	6
87.106.179.116	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	6
2.54.183.210	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	4
66.249.93.117	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	4
173.236.255.128	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
81.45.180.180	147.237.77.19	Spain	law-forum.idf.il	ET SCAN NMAP -sS window 1024	3
80.246.130.201	147.237.76.147	Israel	chinuch.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
213.57.231.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
81.218.118.126	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
31.168.209.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
212.142.148.244	147.237.76.148	Spain	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
81.45.180.180	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.147	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.142.148.244	147.237.76.202	Spain	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.30	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
213.204.105.29	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
37.142.40.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
212.142.148.244	147.237.76.199	Spain	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
176.13.4.97	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
46.59.252.185	147.237.77.216	Germany	dover.idf.il	ET SCAN NMAP -sA (2)	2
81.45.180.180	147.237.77.234	Spain	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
212.142.148.244	147.237.76.201	Spain	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
117.5.89.36	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.198.210	147.237.76.148	Russian Federation	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
89.138.160.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.239.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.137.113	147.237.76.30	Belgium	himush.idf.il	ET SCAN NMAP -f -sS	1
61.244.49.137	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
37.139.27.231	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

03-08-2016 to 03-09-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2641
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	331
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
46.19.86.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
84.94.221.138	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	117
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
109.67.136.169	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
77.125.159.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	76
8.37.231.94	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
109.65.82.38	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
79.180.60.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
212.29.225.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
176.13.4.114	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
80.246.130.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
185.3.147.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
2.54.130.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	45
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	45
69.31.51.50	Anonymous Proxy	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	42
85.250.81.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
2.52.133.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	38
5.29.212.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	37
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	35
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
81.134.9.168	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	33
37.142.207.28	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
80.246.133.47	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
89.138.215.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
83.149.34.189	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
109.66.16.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.26.147.155	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.210.189.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.253.212.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
85.250.183.40	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
107.167.105.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
79.178.202.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	26
192.116.232.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.52.33.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	528
85.65.177.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	368
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	289
149.78.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	258
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	231
109.67.130.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	169
183.60.243.188	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.60.243.188	Block	166
109.253.136.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
37.26.149.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
176.13.12.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
176.13.11.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
109.253.221.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
5.29.60.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
213.151.35.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.253.212.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
203.186.71.4	Hong Kong	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 203.186.71.4	Block	71
2.54.178.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
2.54.40.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.196.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
109.253.144.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.215.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
109.253.199.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
109.253.131.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.3.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
185.32.179.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.9.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.22.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.212.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.128.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.193.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.142.222.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.184.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
183.60.243.188	China	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 183.60.243.188	Block	27

03-08-2016 to 03-09-2016