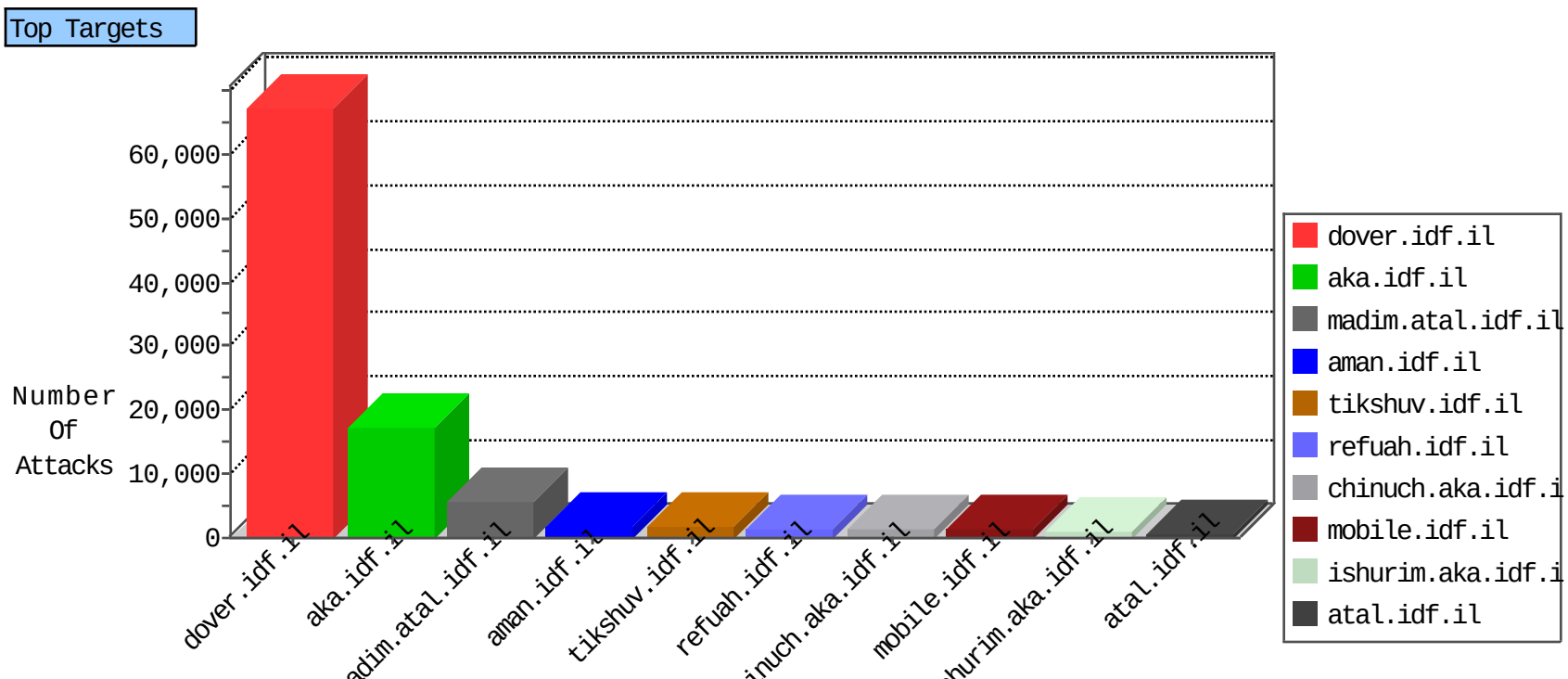
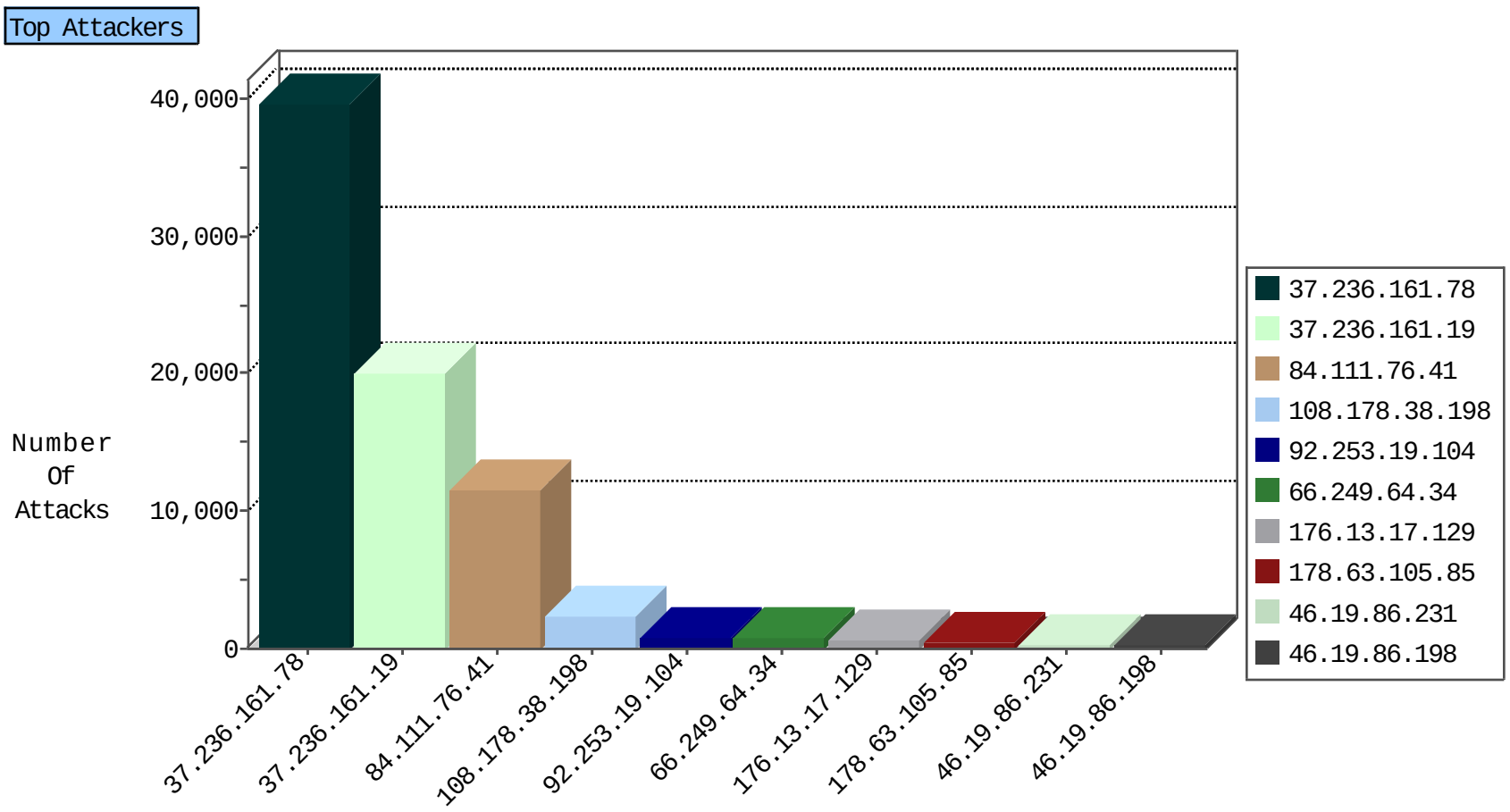
03-07-2016 to 03-08-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-07-2016 to 03-08-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1699
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	832
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	501
92.253.19.104	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	460
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
82.145.218.138	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	136
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	87
82.145.220.152	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	69
82.145.219.110	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
82.145.216.106	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	30
134.191.232.68	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	29
82.145.223.54	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	20
82.145.208.23	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
82.145.219.13	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
46.19.86.128	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
82.145.216.44	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
82.145.209.99	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
46.19.85.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
109.64.224.141	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
2.54.135.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.52.58.242	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
80.179.5.67	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.177.116.56	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
188.165.235.21	France	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.217.18	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
79.177.116.56	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
79.177.105.174	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	5
82.145.218.34	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
79.181.135.147	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.86.116	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
79.183.207.48	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.103.252.5		147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
185.103.252.5		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
77.125.84.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.103.252.5		147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	4
79.176.203.109	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.218.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.177.11.64	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3

03-07-2016 to 03-08-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.180.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	78
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	48
217.132.110.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	27
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	21
5.29.231.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
79.178.145.212	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
192.117.101.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	16
79.177.120.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
31.168.113.160	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
84.110.145.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
213.8.204.22	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
2.52.20.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
85.250.183.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
192.115.177.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
217.132.140.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
87.70.64.124	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
81.218.135.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.108.61.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
185.120.126.162		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.229.208.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.142.156.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	9
84.109.0.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
192.115.64.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
84.110.192.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.34.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.151.45.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.148.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.64.202.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.69.197.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
217.132.82.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.34.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.236.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.136.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.150.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
109.67.152.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.70.23.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.189.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6

03-07-2016 to 03-08-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	696
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	67
200.59.205.238	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	24
46.19.86.89	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	20
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	12
197.242.159.42	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	12
213.204.105.29	147.237.77.233	Lebanon	atal.idf.il	ET SCAN NMAP -sA (2)	10
59.125.130.154	147.237.0.19	Taiwan	madim.atal.idf.il	SERVER-WEBAPP apache directory disclosure attempt	8
59.125.130.154	147.237.0.19	Taiwan	madim.atal.idf.il	GPL WEB_SERVER apache directory disclosure attempt	8
50.97.138.113	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	6
84.245.33.104	147.237.76.42	Netherlands	refuah.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
94.102.153.58	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	3
108.178.38.198	147.237.72.156	United States	aman.idf.il	portscan: TCP Distributed Portscan	2
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
79.183.29.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
64.233.172.169	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
2.54.55.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
217.66.232.187	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	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
192.117.188.57	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.46.193.114	147.237.8.46	China	e.chinuch.idf.il	GPL SCAN nmap TCP	2
66.102.9.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
140.242.217.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
62.128.41.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
209.126.116.147	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.73.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.244.49.137	147.237.76.196	Hong Kong	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
46.19.85.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.23.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.94.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.124.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.245	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
132.66.42.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.103.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.140.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sS window 3072	1
213.8.159.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.110.158.12	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.117.7.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-07-2016 to 03-08-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38074
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17747
84.111.76.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1320
108.178.38.198	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1174
108.178.38.198	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1173
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1064
92.253.19.104	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	358
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	312
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	272
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop		drop	200
176.12.135.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
176.13.3.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	136
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	135
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	130
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
212.143.222.47	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
87.69.37.129	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
212.179.226.141	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.86.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	77
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	76
77.127.134.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	75
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	74
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	74
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	71
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
2.54.188.227	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
93.158.152.68	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	67
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	67
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	64
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
192.115.30.42	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
37.26.149.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.253.135.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	54
80.246.136.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	53
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	52
79.182.13.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	49
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	48
79.182.36.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	47

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.76.41	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 84.111.76.41	Block	6531
84.111.76.41	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning V1	Block	3668
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	292
2.54.63.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	253
132.70.66.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	235
176.13.6.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	228
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	226
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.236.161.19	Block	193
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	162
176.13.5.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
2.54.144.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
37.26.146.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
109.253.206.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
79.176.99.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
176.13.15.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.54.158.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.21.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.52.153.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
2.54.23.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.52.21.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
79.176.110.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	73
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.54.184.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.54.12.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.236.161.78	Block	56
2.52.50.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.132.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.54.173.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
37.26.149.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.136.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
37.26.146.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
185.32.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.13.14.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.147.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.120.186.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.131.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
212.199.57.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
176.13.7.78	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	35
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.52.180.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32

03-07-2016 to 03-08-2016