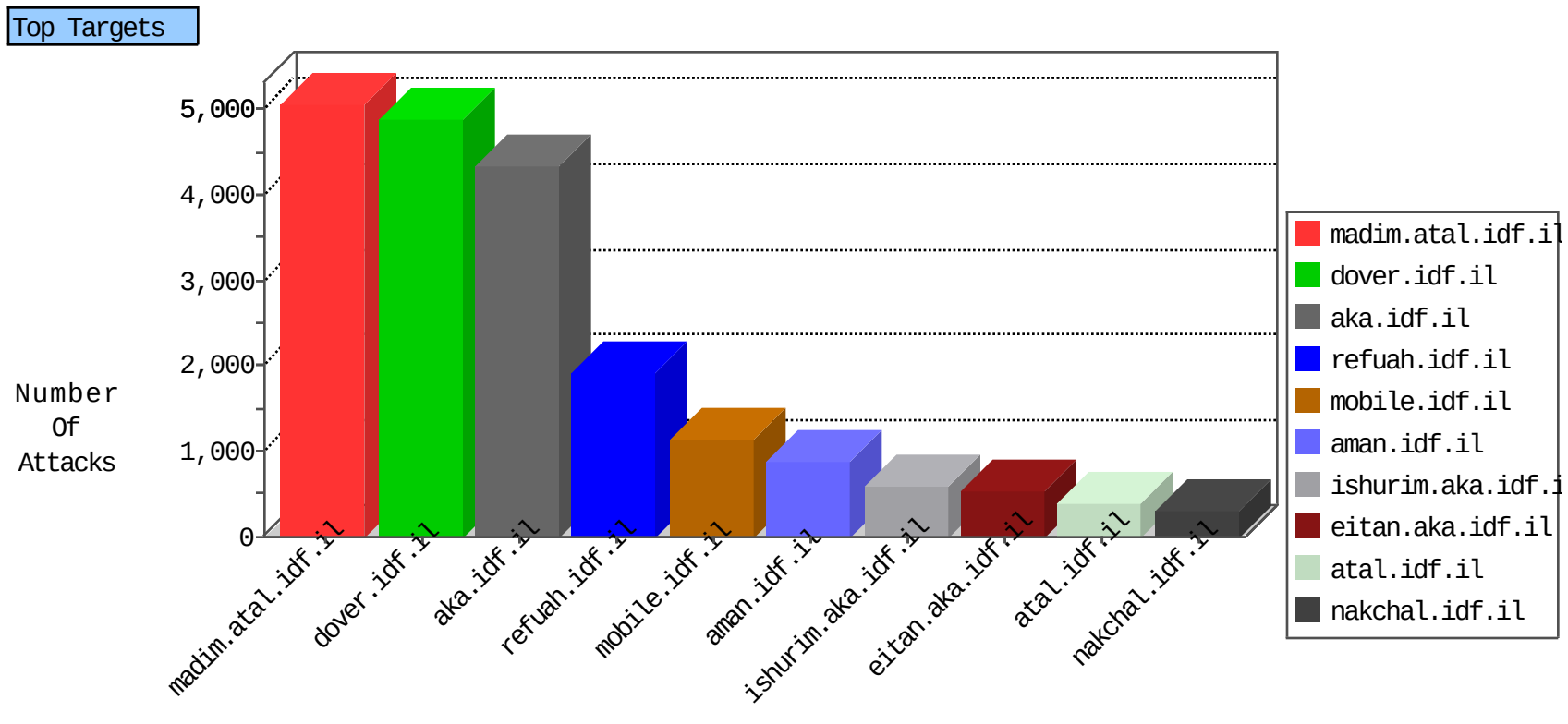
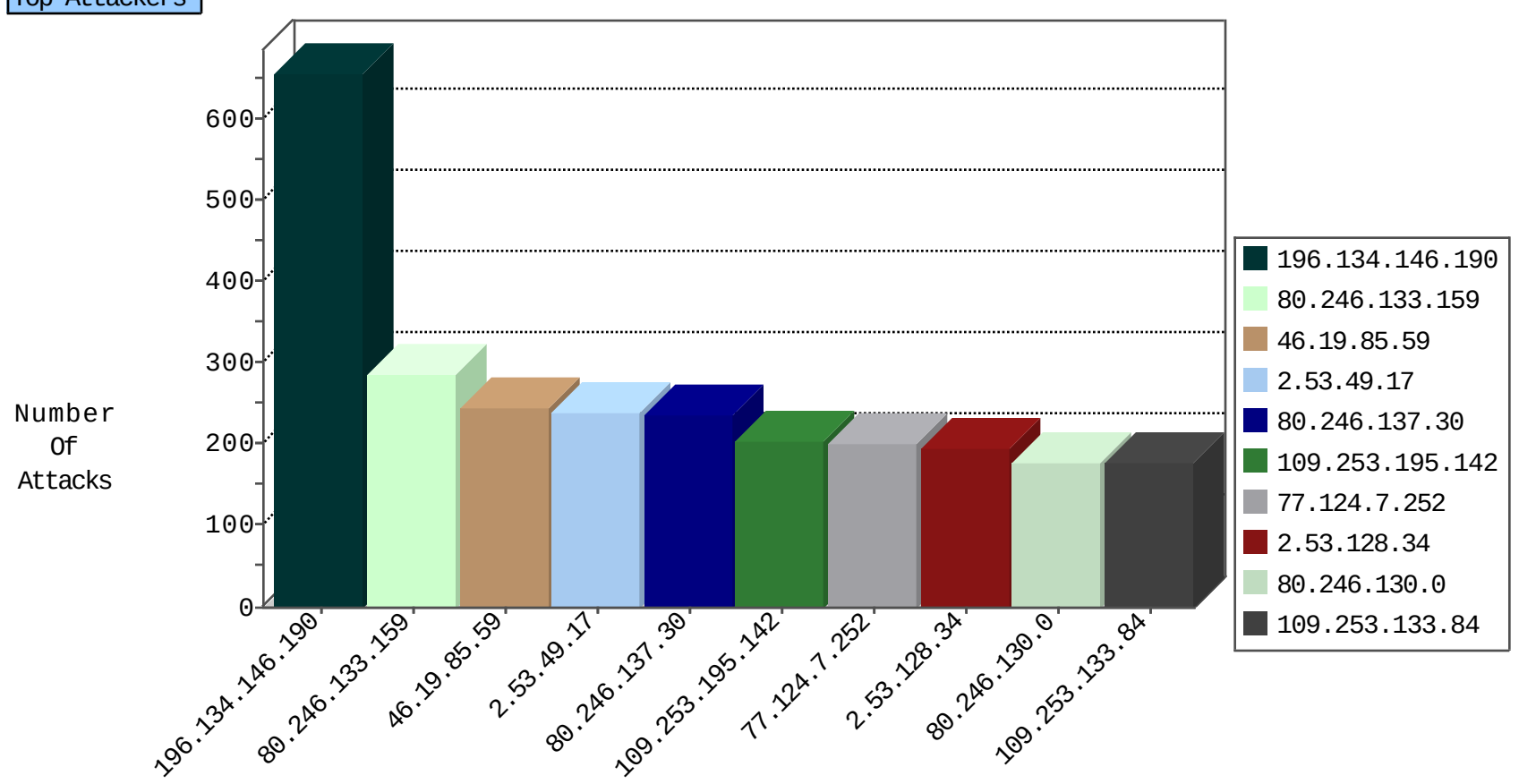
09-15-2016 to 09-16-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-15-2016 to 09-16-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	20507
77.124.7.252	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	8270
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	Anomaly-IP-bad-frag-bits	drop	2365
77.124.7.252	Israel	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1798
109.64.45.90	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	497
62.0.105.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	463
79.173.226.205	Jordan	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	244
79.183.41.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	143
145.132.236.165	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	32
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	26
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	25
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	24
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	21
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	ICMP-fragmented	drop	21
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	21
95.86.121.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	20
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	19
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	19
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	15
2.55.184.96	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	14
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
5.102.254.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10

09-15-2016 to 09-16-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	59
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	52
69.30.221.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	43
5.9.89.170	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	35
138.201.127.112	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	32
89.163.148.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	27
106.38.241.105	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	25
138.201.127.112	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	21
193.111.140.153	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	20
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	19
89.163.148.22	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	16
106.38.241.105	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	16
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
89.163.148.22	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	11
5.9.89.170	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	11
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	10
69.30.221.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	10
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	9
193.111.140.153	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	9
193.111.140.153	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
138.201.127.112	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	8
69.30.221.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	7
69.30.221.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	5
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
89.163.148.22	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
5.9.89.170	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.221.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
89.163.148.22	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.90.118	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
138.201.127.112	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.178	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
138.201.127.112	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.210.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
178.63.86.11	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
220.181.124.113	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
185.81.158.124	France	147.237.77.216	dover.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
94.102.49.190	Netherlands	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.155	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.17	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.159	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.99	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
5.9.89.170	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
118.200.203.78	Singapore	147.237.77.74	law.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

09-15-2016 to 09-16-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.96	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	46
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	15
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	14
176.13.246.0	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	10
212.199.57.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	5
31.168.0.253	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
109.64.55.1	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	5
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	4
49.14.91.173	147.237.76.31	India	nakchal.idf.il	GPL SCAN nmap TCP	4
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	3
80.246.130.195	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	3
175.207.77.148	147.237.77.74	Korea, Republic of	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
46.227.67.158	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	2
141.226.217.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	2
31.168.144.253	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential SSH Scan	2
151.80.40.87	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
82.81.76.144	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2

09-15-2016 to 09-16-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	286
2.53.128.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	195
80.246.130.0	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	173
79.177.153.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	146
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	132
185.69.4.253	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
2.53.60.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	119
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
84.110.55.248	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	99
89.139.113.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	98
37.26.147.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
77.125.82.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
80.246.140.86	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
141.0.14.217	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
31.154.23.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	56
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
77.125.22.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.117.101.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
192.116.94.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
141.0.14.74	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
82.145.220.145	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	43
82.145.219.190	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	43
2.55.141.55	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
80.178.150.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	41
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.6	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
37.26.147.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
62.0.210.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
194.90.178.37	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	34
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
185.3.147.174	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
217.132.51.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
62.0.221.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
80.246.130.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
46.19.85.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
77.127.240.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
141.226.218.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	29
87.69.52.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
192.118.78.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
2.53.49.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	240
80.246.137.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	235
109.253.195.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	202
109.253.133.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	169
176.13.2.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
2.53.50.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
109.253.202.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
37.26.149.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	140
176.13.245.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
109.253.158.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
2.53.167.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
2.53.22.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
109.253.209.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
176.13.7.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
185.32.179.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.219.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
37.26.149.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.240.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.53.19.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
46.19.85.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.23.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
37.26.148.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.53.48.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
185.32.179.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
213.57.178.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
176.13.15.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
77.139.166.156	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.55.189.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
80.246.136.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
176.13.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.53.10.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
141.226.218.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.149.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
79.181.116.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.128.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
185.69.4.253	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 185.69.4.253	Block	35
109.253.196.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.148.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.65.31.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
80.246.139.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.13.231.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.86.207	Block	24

09-15-2016 to 09-16-2016