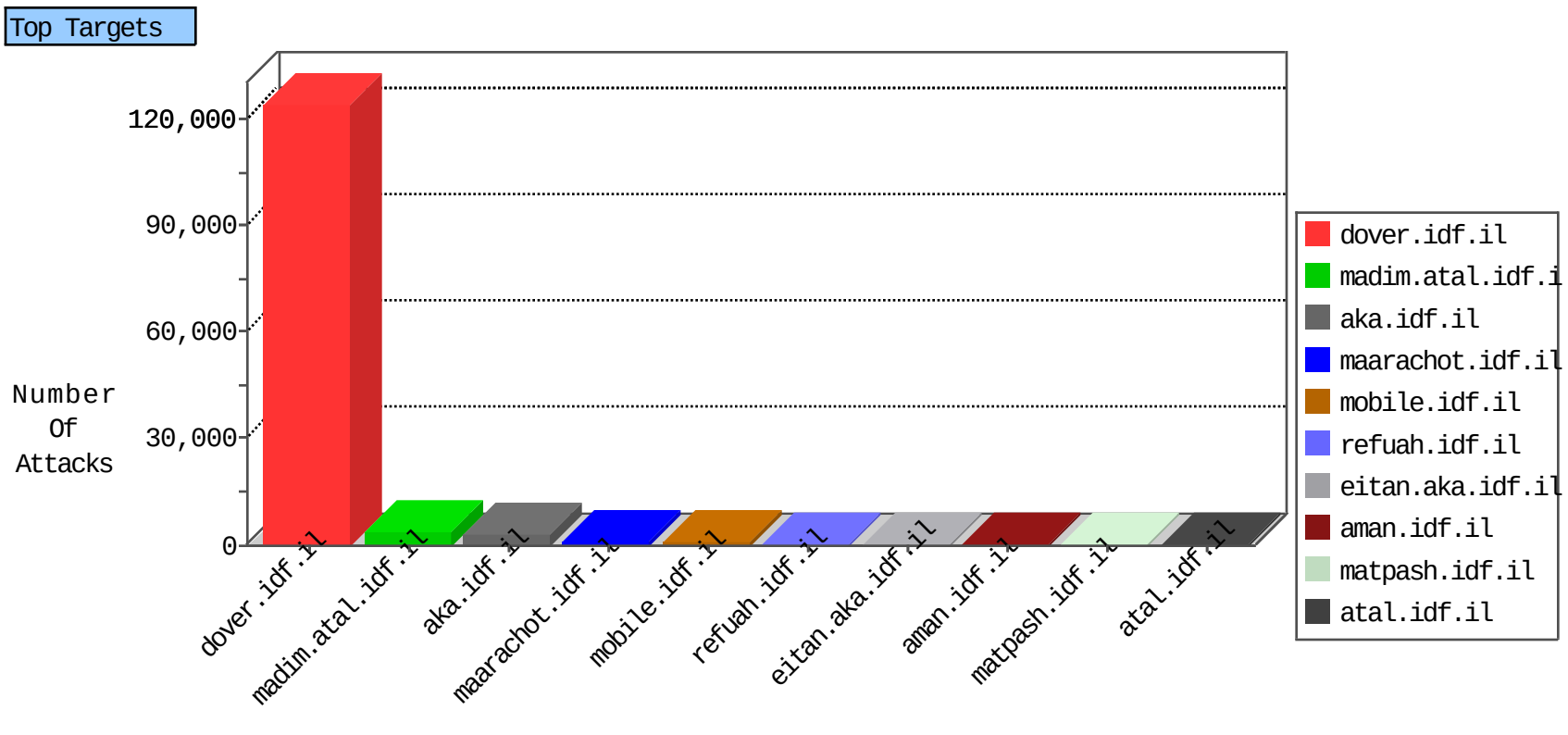
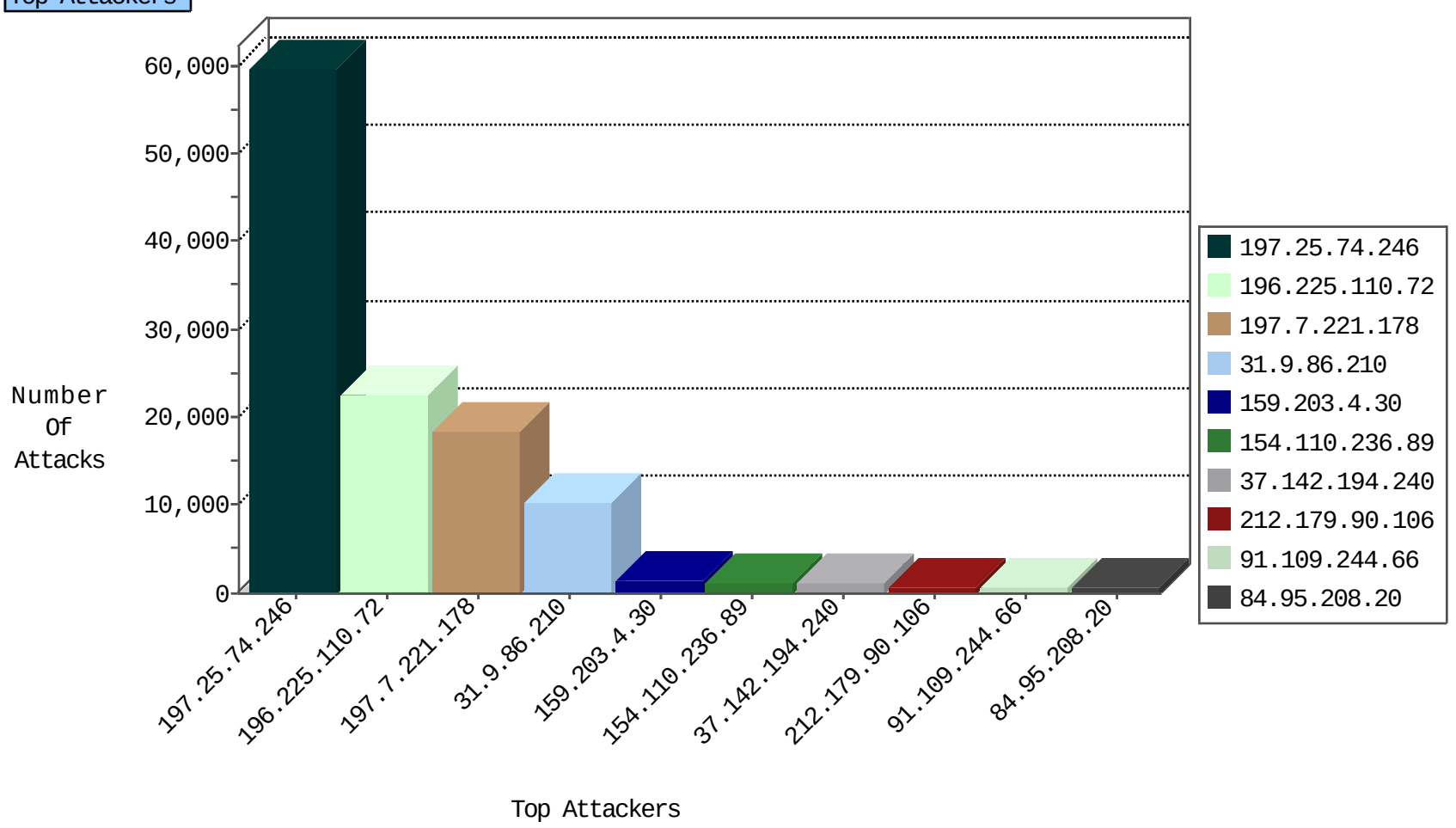
09-17-2016 to 09-18-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-17-2016 to 09-18-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	338751
197.7.221.178	Tunisia	147.237.77.216	dover.idf.i	DOS-HTTP-torshammer	forward	8379
197.7.221.178	Tunisia	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	6208
197.7.221.178	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	648
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	60
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	55
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	55
109.226.10.107	Israel	147.237.77.216	dover.idf.i	Black List	drop	52
213.219.200.147	Russian Federation	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	50
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	49
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	45
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	42
187.60.34.102	Brazil	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	39
185.23.175.81	Israel	147.237.77.216	dover.idf.i	Black List	drop	38
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	37
197.25.74.246	Tunisia	147.237.77.216	dover.idf.i	Invalid TCP Flags	drop	37
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	33
85.114.105.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Black List	drop	30
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	30
195.66.156.6	Ukraine	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	29
85.114.107.226	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Black List	drop	27
4.53.161.218	United States	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	27
197.25.74.246	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	26
192.116.105.65	Israel	147.237.77.216	dover.idf.i	Black List	drop	24
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	24
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	24
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	24
112.211.251.105	Philippines	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	23
213.175.157.60	United Kingdom	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	23
177.67.200.30	Brazil	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	22
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	21
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	21
80.179.119.22	Israel	147.237.77.216	dover.idf.i	Black List	drop	20
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	20
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	19
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
80.90.83.17	Albania	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	16
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	16
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	15
85.114.105.161	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Black List	drop	15
200.240.240.74	Brazil	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	15
62.128.42.1	Israel	147.237.77.216	dover.idf.i	Black List	drop	15
212.199.221.116	Israel	147.237.77.216	dover.idf.i	Black List	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	14
193.0.240.58	Ukraine	147.237.77.216	dover.idf.i	network flood IPv4 ICMP	drop	14

09-17-2016 to 09-18-2016

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	91
69.30.221.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	49
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	45
69.30.221.250	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	34
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	28
69.30.213.82	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	19
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	17
106.38.241.105	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	13
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	11
91.200.12.47	Ukraine	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	8
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Permit	8
178.32.203.32	Poland	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
106.38.241.105	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	6
46.119.115.28	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	5
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	4
88.198.230.79	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.4.116.197	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
211.157.151.57	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	2
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
88.198.230.79	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.250	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
78.46.50.246	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
212.47.229.189	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.230.79	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.230.79	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.234.159.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.250	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
87.68.16.75	Israel	147.237.72.156	aman.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2
69.30.213.82	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
111.255.177.208	Taiwan	147.237.77.216	dover.idf.il	13118: ICMP: Windows DirectAccess Server IPv6 Invalid Header Denial-of-Service Vulnerability	Block	2
88.198.230.79	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.12.75	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.250	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.103	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
185.26.92.74	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
123.126.68.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
95.10.179.158	Turkey	147.237.0.15	kosher-kravi.idf.i	C1000016: HTTP: administrator in URI	Permit	1
188.120.154.105	Israel	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-17-2016 to 09-18-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.17.147	147.237.77.216	Canada	dover.idf.il	Tehila - Perl LWP with fake user agent	81
80.246.130.84	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
87.68.16.75	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	8
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	7
79.179.151.172	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	7
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	6
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	6
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	5
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	5
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	5
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	4
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	3
197.7.221.178	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	3
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	3
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.233	Netherlands	atal.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
120.33.120.73	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.212	Netherlands	e.dover.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	3
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
66.249.69.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
218.24.171.223	147.237.76.31	China	nakchal.idf.il	GPL SCAN nmap TCP	2
202.155.58.28	147.237.72.217	Indonesia	e.idf.il	ET SCAN NMAP -sS window 1024	2
59.46.193.114	147.237.76.31	China	nakchal.idf.il	GPL SCAN nmap TCP	2
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	2
202.155.58.28	147.237.8.46	Indonesia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
202.155.58.28	147.237.0.15	Indonesia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
91.224.161.69	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
109.60.153.178	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	2

09-17-2016 to 09-18-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41257
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18252
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12942
31.9.86.210	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10194
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	5011
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3677
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		monitor	3645
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop		drop	1375
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1301
159.203.4.30	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1174
154.110.236.89	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	986
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	807
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	769
91.109.244.66	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	766
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	583
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	576
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	drop		drop	540
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Response out of state	monitor	520
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	484
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	412
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	367
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	306
2.53.148.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	300
178.62.54.14	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	257
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	156
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	145
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	140
89.237.119.248	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	104
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	101
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
168.235.207.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	85
87.70.18.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
167.114.17.147	Canada	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	81
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
62.16.72.250	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	70
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
159.203.4.30	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	64
82.145.220.37	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
87.69.79.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
84.111.25.48	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	55

09-17-2016 to 09-18-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	556
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	548
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	548
196.225.110.72	Tunisia	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	548
5.29.84.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	547
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	490
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.25.74.246	Block	432
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.25.74.246	Block	432
109.253.131.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	362
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	247
84.109.115.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	230
176.13.239.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	221
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	193
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	136
87.68.16.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.16.75	Block	123
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	123
197.25.74.246	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	123
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
109.253.195.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
176.13.13.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.53.29.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.53.172.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	90
109.253.133.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
109.65.120.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
87.70.59.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.53.141.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.53.140.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
154.110.236.89	Tunisia	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	55
154.110.236.89	Tunisia	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	55
154.110.236.89	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	55
176.13.18.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.223.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.53.132.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
2.53.52.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
141.226.145.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.26.149.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 37.142.194.240	Block	29
109.253.135.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
2.55.20.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
87.71.112.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
87.70.10.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	16

09-17-2016 to 09-18-2016