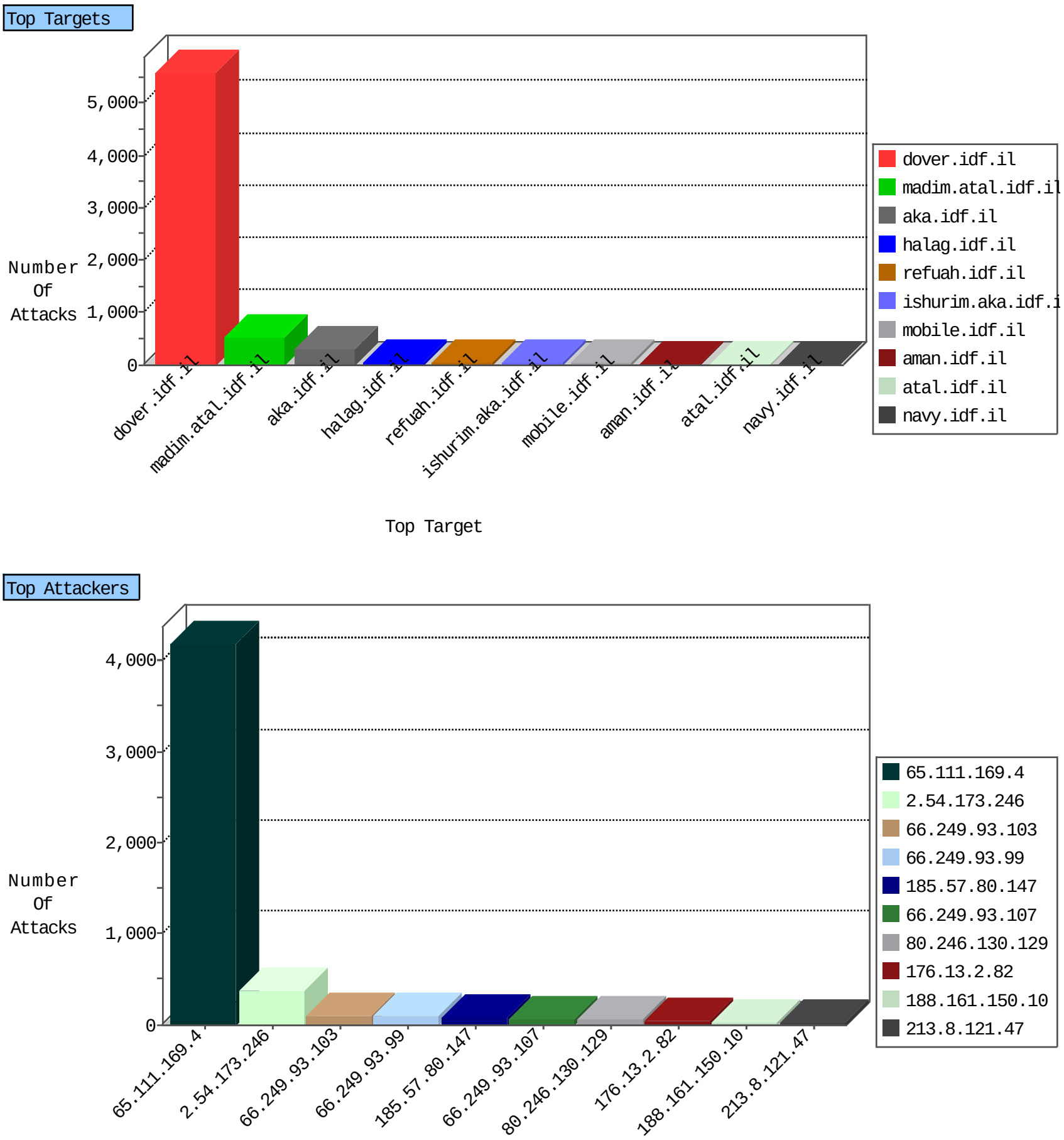
02-17-2016-13:04:08 to 02-17-2016-14:04:08

IDF Under Attack
Daily Report



02-17-2016-13:04:08 to 02-17-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.111.169.4	United States	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	26257
65.111.169.4	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	280
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
65.111.169.4	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	105
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	96
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	94
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	67
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	63
188.161.150.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
82.208.136.157	Romania	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
37.26.146.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
176.67.111.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
66.249.91.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
207.46.13.181	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	13
37.26.148.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
188.247.72.57	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
37.26.146.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
176.67.111.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
37.26.148.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
37.26.148.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
185.57.80.147	Romania	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
37.202.92.200	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	7
207.46.13.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
52.68.136.185	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.208.136.157	Romania	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
60.242.133.181	Australia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.71.161.22	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
162.243.57.54	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
199.16.156.125	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.29.198.26	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
37.26.148.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
85.115.52.201	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.26.146.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.67.111.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
107.170.142.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
66.220.146.30	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3

02-17-2016-13:04:08 to 02-17-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-13:04:08 to 02-17-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.117.2.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.159.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.50.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.253.132.89	147.237.77.216	Argentina	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.127.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.130	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.69.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.47.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.84.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.242.218.25	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
84.228.141.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.118.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-17-2016-13:04:08 to 02-17-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
65.111.169.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2502
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	64
80.246.130.129	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
213.8.121.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.54.143.204	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.8.184.30	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.155.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.8.142.84	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.136.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
41.144.89.31	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.33.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.12.176	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.221.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
130.193.50.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.221.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.107.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.76.107.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.69	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
147.236.38.135	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.64.223.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.215.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.132.229.1	United States	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop		drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.29.117.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.148.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.178.50.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.102.49.78	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
46.19.85.101	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
62.219.161.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.158.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.102.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.102.49.78	Netherlands	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3
149.88.15.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-17-2016-13:04:08 to 02-17-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.173.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	189
2.54.173.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	150
176.13.2.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.52.32.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
2.54.173.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	30
2.54.136.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
84.228.141.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.141.62	Block	15
2.54.13.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
2.54.5.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
2.54.10.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
84.228.141.62	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
80.246.136.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.192.0	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8516-he/himush.aspxâ€?â€Ž	Block	3
46.118.114.111	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.96	Block	3
185.32.179.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.133.85	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
2.54.155.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	2
176.13.0.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 217.194.198.104	Block	1
212.117.132.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.227	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
95.106.183.88	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
80.246.130.129	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
62.219.123.105	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
149.88.111.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.142.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 217.194.198.104	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
46.19.86.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
176.13.6.29	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
5.29.117.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
207.46.13.128	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
64.79.85.205	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.188	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 217.194.198.104	Block	1
84.228.141.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
2.52.161.21	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.215.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

02-17-2016-13:04:08 to 02-17-2016-14:04:08