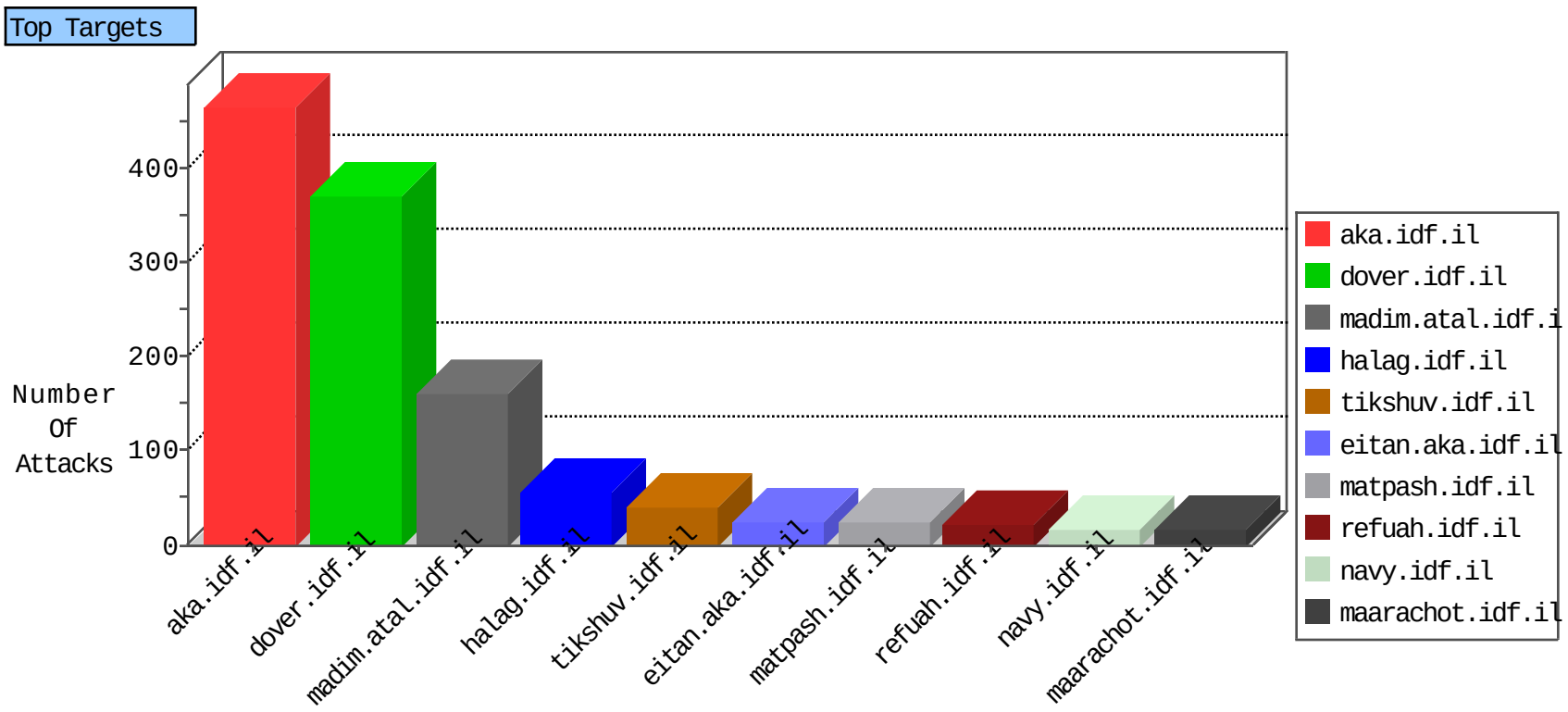
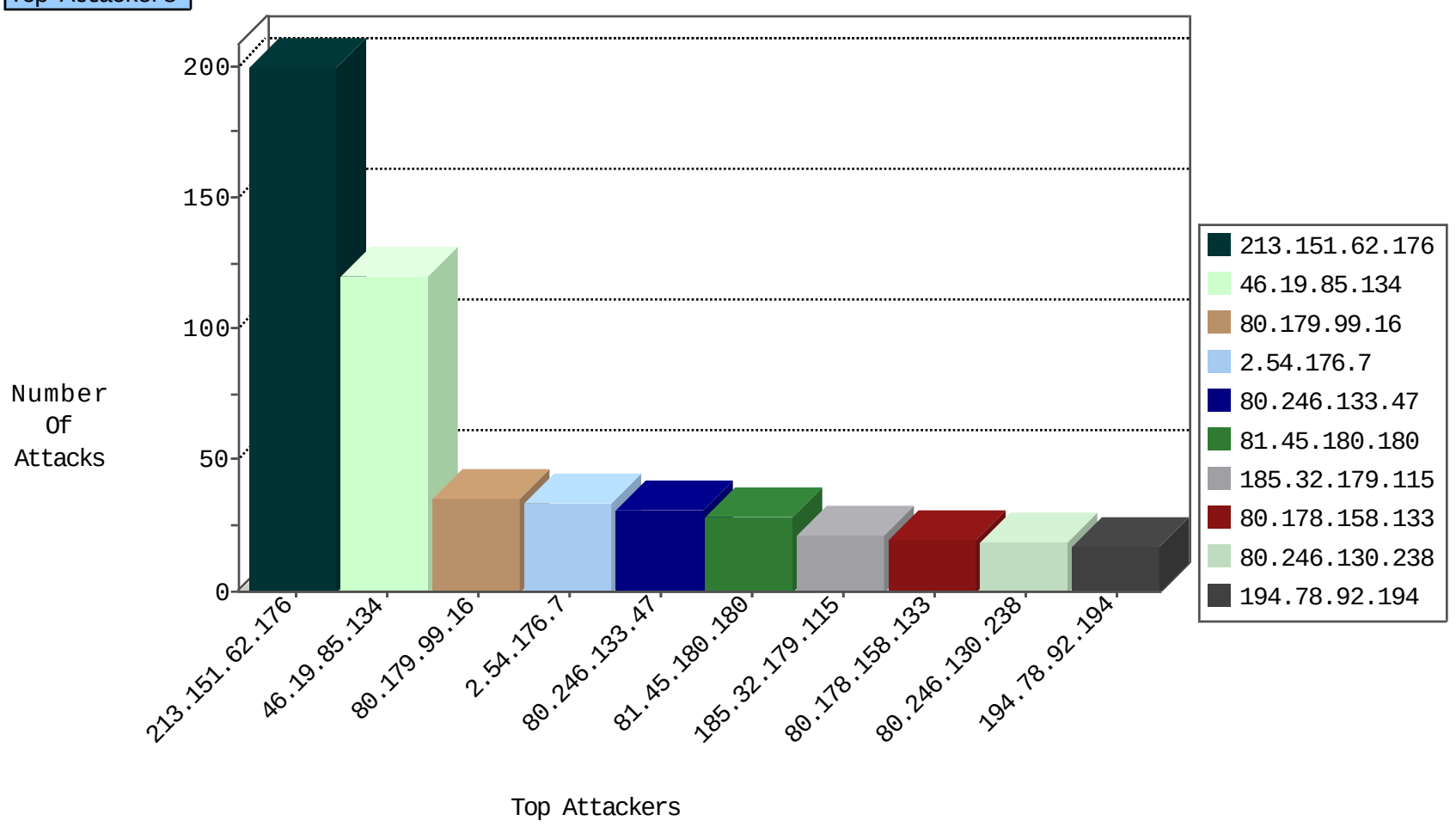
03-08-2016-15:04:06 to 03-08-2016-16:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-08-2016-15:04:06 to 03-08-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.45.180.180	Spain	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	35
2.54.176.7	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
80.179.99.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
80.178.158.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
82.145.218.152	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
80.246.136.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
94.230.93.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
94.230.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.109.9.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.94.182.156	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
64.94.179.12	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
98.27.225.40	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-15:04:06 to 03-08-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.105.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
217.132.130.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.94.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.13.1.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.13.14.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
89.138.23.252	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-15:04:06 to 03-08-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.45.180.180	147.237.77.234	Spain	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
81.45.180.180	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
79.181.134.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.235	Spain	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.166.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
37.142.210.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.212	Spain	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.151.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.174.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.157.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.176	Spain	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.136.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.35.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.170	Spain	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.139.55.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.209.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.84.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.97.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.235	Spain	sviva.idf.il	ET SCAN Potential SSH Scan	1
46.116.114.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.198.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.216	Spain	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.148.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.205	Spain	prisha.idf.il	ET SCAN Potential SSH Scan	1
5.22.131.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.133.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.178	Spain	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.88.56.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.172.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.176	Spain	matpash.idf.il	ET SCAN Potential SSH Scan	1
109.186.129.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.45.180.180	147.237.77.121	Spain	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.94.174.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-08-2016-15:04:06 to 03-08-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.47	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
80.246.130.238	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.85.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.178.150.57	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
87.71.125.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
79.180.232.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
194.78.92.194	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.32.179.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
88.253.43.30	Turkey	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	7
2.52.34.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.102.169.250	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
84.94.198.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.197.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.209.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.41.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.243.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.157	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.122.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.178.158.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.174.169	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	5
2.54.176.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.179.99.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.179.99.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.54.176.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.179.99.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.178.158.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
194.78.92.194	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
194.78.92.194	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
70.199.66.82	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.168.73.110	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.174.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.71.110.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.157.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.46.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.35.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 213.151.62.176	Block	18
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 213.151.62.176	Block	18
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 213.151.62.176	Block	18
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 213.151.62.176	Block	17
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 213.151.62.176	Block	17
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 213.151.62.176	Block	16
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 213.151.62.176	Block	15
109.253.221.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	14
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 213.151.62.176	Block	14
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 213.151.62.176	Block	14
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 213.151.62.176	Block	11
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 213.151.62.176	Block	7
5.102.227.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.53.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal URL Path Encoding from 213.151.62.176	Block	4
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Url from 213.151.62.176	Block	4
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 213.151.62.176	Block	4
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Query String from 213.151.62.176	Block	4
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.102.97.237	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	3
80.246.137.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
80.179.96.89	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
50.63.194.20	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
107.161.24.34	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
94.230.93.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.8.30.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.62.176	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding u[[#3]]1'°Ú″=[[│—λ#31[[]]#25'וx™]]lg˙™ז§;λ x[[#17]]Ž˛)˛•″v„[[#0]]q]ž°ם6]]6#[[˛<˙"—]]5#[[sr]]72#[[v¨│•[[22#]]Š‡ɔ˛‡yyת [[#29]][—[[#4]][[#22]]z¨š="[[#31]]Þ6˛ˆwבא%*Ê0cux>˛f$,·¬˛ɔqnqÊ″˛žŒדŠ{["•¿¬-˛xgu˛s[[#19]]qhע„˙ה¥ א¼y,רœmוי¦על˙[[#0]][[וו#12©k–l]]:r ɔ˙ÚŽÊ"˛{Ʊrrw»˛i	Block	1
192.243.55.129	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
150.129.238.67	India	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
98.130.0.212	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
203.127.96.196	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.110.210.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
220.255.98.120	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.170.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
50.63.197.56	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
94.230.93.21	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.37.139.95	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.69.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106007.pdf	Block	1
104.131.147.112	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
8.29.138.132	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1