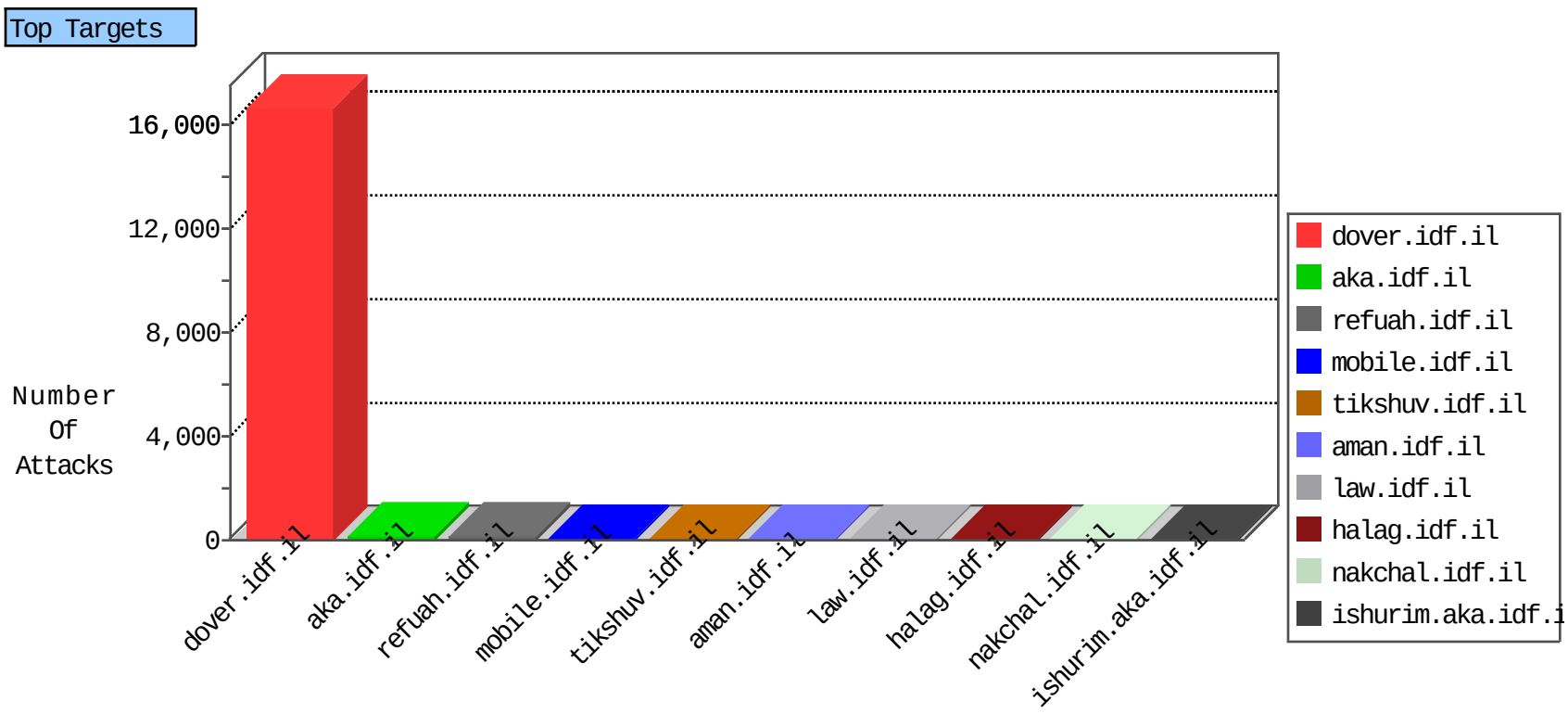
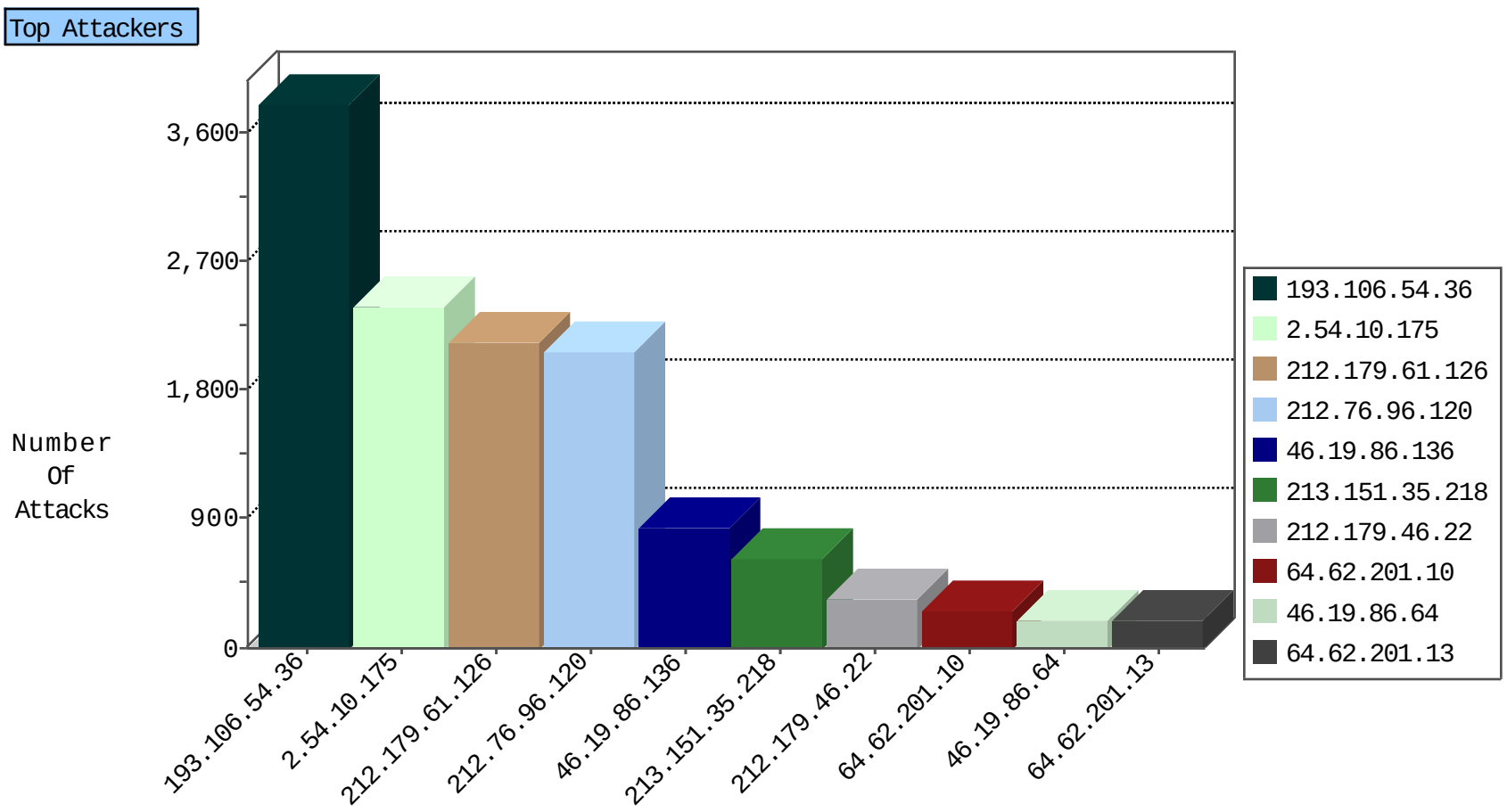
04-30-2015-16:03:04 to 04-30-2015-17:03:04

IDF Under Attack
04-30-2015-16:03:04

Top Targets



Top Attackers



04-30-2015-16:03:04 to 04-30-2015-17:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.85.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2595
66.249.67.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.183.70.121	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
46.19.85.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
69.25.27.108	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
69.25.27.112	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
2.54.185.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.66.24.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
195.37.190.86	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
79.177.33.26	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
82.102.141.248	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
140.242.64.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
64.62.201.13	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.110.214.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.91.60.10	Europe	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.82.78.10	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
69.25.27.118	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-30-2015-16:03:04 to 04-30-2015-17:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.114.23.18	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.160.164	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
109.66.61.254	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
158.112.85.164	Norway	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
187.50.185.181	Brazil	147.237.0.15	kosher-kravi.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.i	DVRep_B-N_60_100	Block	1
46.19.85.163	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1

04-30-2015-16:03:04 to 04-30-2015-17:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.121.86.180	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.62.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.233.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.29.28.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.135.111.75	Israel	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.250.97.225	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.63.124	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.0.33	idf.il	ET SCAN NMAP -sS window 3072	1
194.90.198.201	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
41.159.136.195	Gabon	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
182.92.163.19	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
182.92.163.19	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.108	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.106.54.36	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
41.159.136.195	Gabon	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -f -sS	1
182.92.163.19	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
176.58.68.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-30-2015-16:03:04 to 04-30-2015-17:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
193.106.54.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3795
2.54.10.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2389
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2136
212.76.96.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2065
46.19.86.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	842
213.151.35.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	629
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	336
64.62.201.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
46.19.86.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
64.62.201.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	178
198.144.105.20	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	119
41.130.48.217	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
138.246.2.179	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
110.174.114.182	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
93.173.145.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
46.19.85.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.66.61.254	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	48
79.179.166.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
212.150.214.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
176.58.68.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
2.54.47.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
140.194.40.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
94.159.170.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
37.142.244.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
107.72.164.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
212.150.195.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
207.46.13.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
212.29.225.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
84.228.241.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
158.112.85.164	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
66.87.116.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
88.90.22.196	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.163.234.5	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
87.69.89.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
195.110.41.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.120.140.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
188.120.140.47	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 188.120.140.47	Block	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
109.67.138.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
81.218.33.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	3
178.137.166.68	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
37.142.152.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
37.26.147.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.57.204.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.156.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.148.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
185.32.178.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.166.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
132.71.84.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
80.246.133.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.138.17.205	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/2609011010.aspx	Block	1
177.134.197.225	Brazil	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/skira/default.asp	None	1
109.65.163.198	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
87.68.68.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
50.188.118.174	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
2.54.151.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
185.53.44.65		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
79.178.26.217	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
140.250.56.7	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.67.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
93.173.61.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.76.125.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19798-he/idfgdover.aspx	Block	1
66.249.64.68	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
89.248.248.149	Czech Republic	147.237.77.74	law.idf.il	PHP Attempt	Block	1
185.53.44.178		147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/chinuch/kurs/	None	1
79.179.166.213	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	1
149.78.133.126	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.136	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
94.159.152.234	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
84.228.237.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.28.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.52.168.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
180.76.4.245	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
77.237.154.221	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1