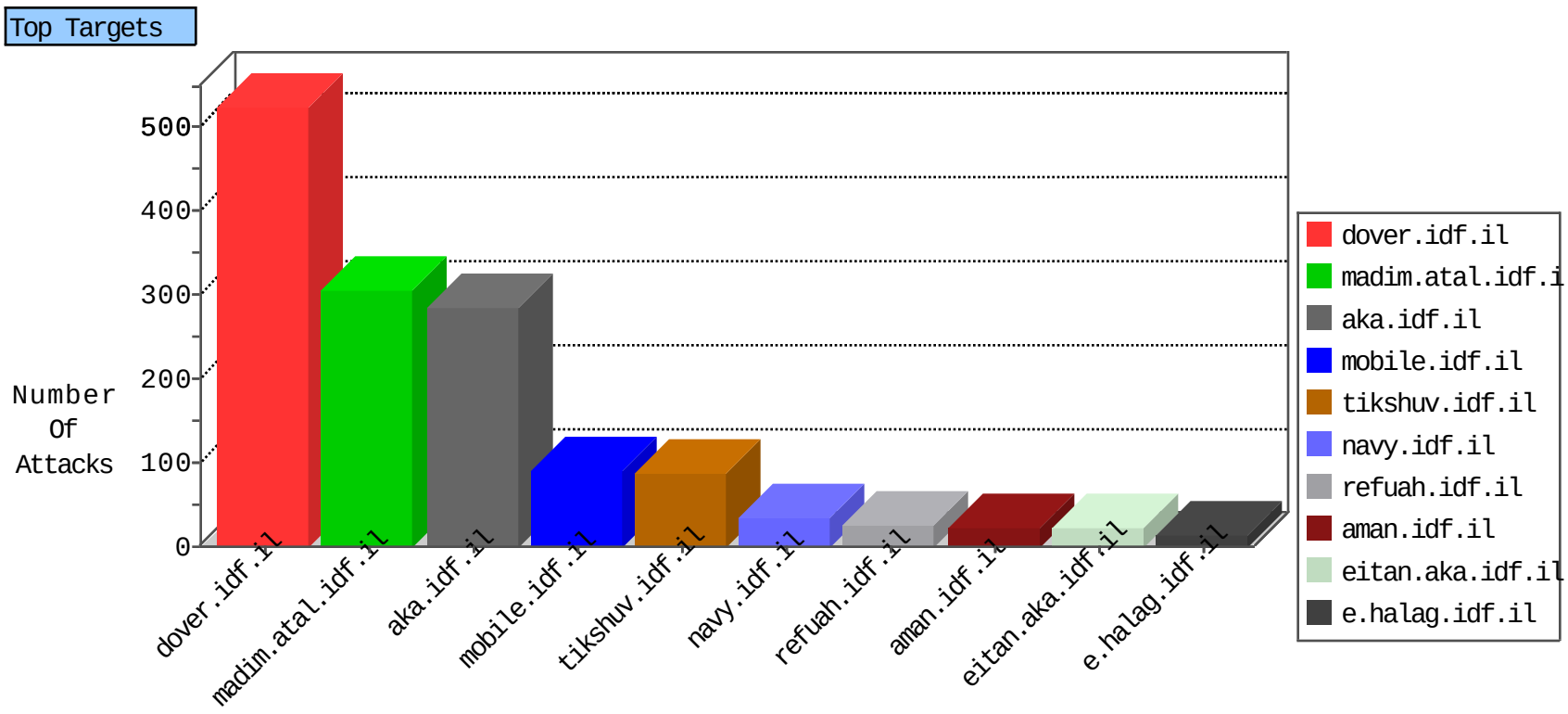
03-07-2016-16:04:05 to 03-07-2016-17:04:05

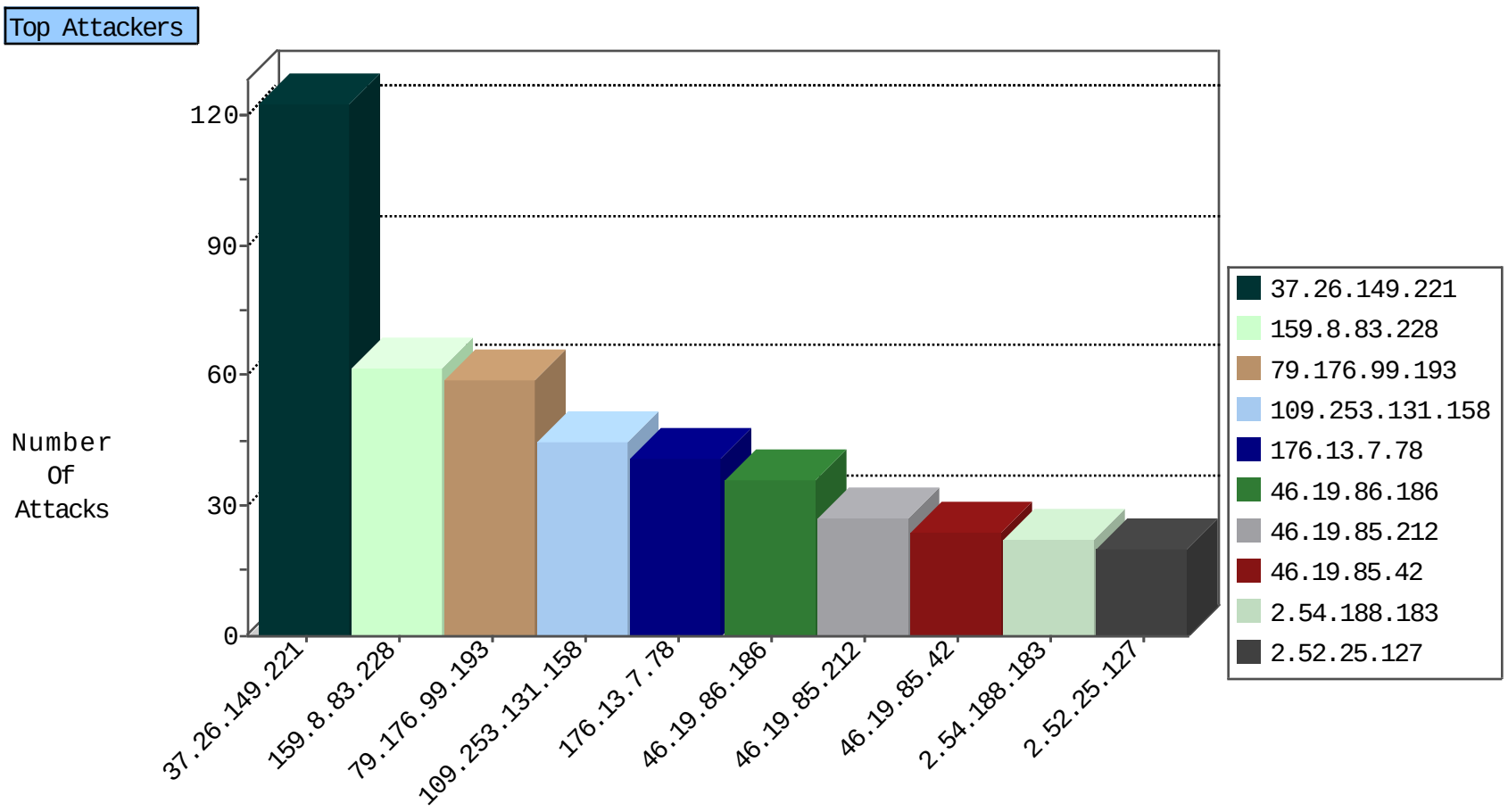
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-07-2016-16:04:05 to 03-07-2016-17:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
109.64.224.141	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
46.19.85.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.125.84.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.117.21.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
209.126.105.33	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
85.25.218.110	Germany	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
12.152.75.6	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
175.104.249.69	Japan	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-16:04:05 to 03-07-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.117.101.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
79.183.180.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
217.132.82.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.69.197.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.236.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.136.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
87.70.23.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.15.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.224.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.104.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.151.41.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
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
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
175.10.210.214	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

03-07-2016-16:04:05 to 03-07-2016-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.42.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.14.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.138.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
46.117.21.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.27.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.66.42.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.3.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.92.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.173.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.201.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.184.187	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sS window 3072	1
62.128.41.133	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
46.117.143.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.96.186.240	147.237.0.15	Brazil	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.196.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.219.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.183.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.203.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-07-2016-16:04:05 to 03-07-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.52.25.127	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
149.78.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.188.183	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.26.146.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.203.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.16.112	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
41.252.93.82	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
80.246.137.3	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.215.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.115.30.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.154.164.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.182	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.228.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.46.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.115.30.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.173.189.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.198.6	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
70.214.103.178	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.151.46.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.67.145.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.252	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.243	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.131.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
46.121.138.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.114.23.209	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
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
79.176.99.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
109.253.131.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.7.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
109.253.218.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning V1	Block	9
109.65.218.215	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.65.218.215	Block	7
65.208.151.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	6
65.208.151.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	6
37.26.146.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
62.90.58.17	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	3
176.13.7.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.131.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.89	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
2.54.173.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.89	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
45.35.105.129		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
89.138.123.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.146.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	2
17.138.56.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21229-he/idfgdover.aspx	Block	2
185.89.217.234		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.208.151.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
37.26.146.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.29.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.76.110.173	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
65.208.151.119	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.119	Block	2
65.208.151.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
147.188.244.75	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
104.236.228.120		147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/magento_version	Block	1
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
207.46.13.96	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
87.69.105.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
185.89.217.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.121.138.57	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.183.10.25	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
37.26.146.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.164.98.97	Austria	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.133.27	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.193.92.94	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.49.18	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 82.80.49.18	Block	1
62.153.147.123	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.3.147.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1
156.207.125.61		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
104.236.253.54		147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 104.236.253.54	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1