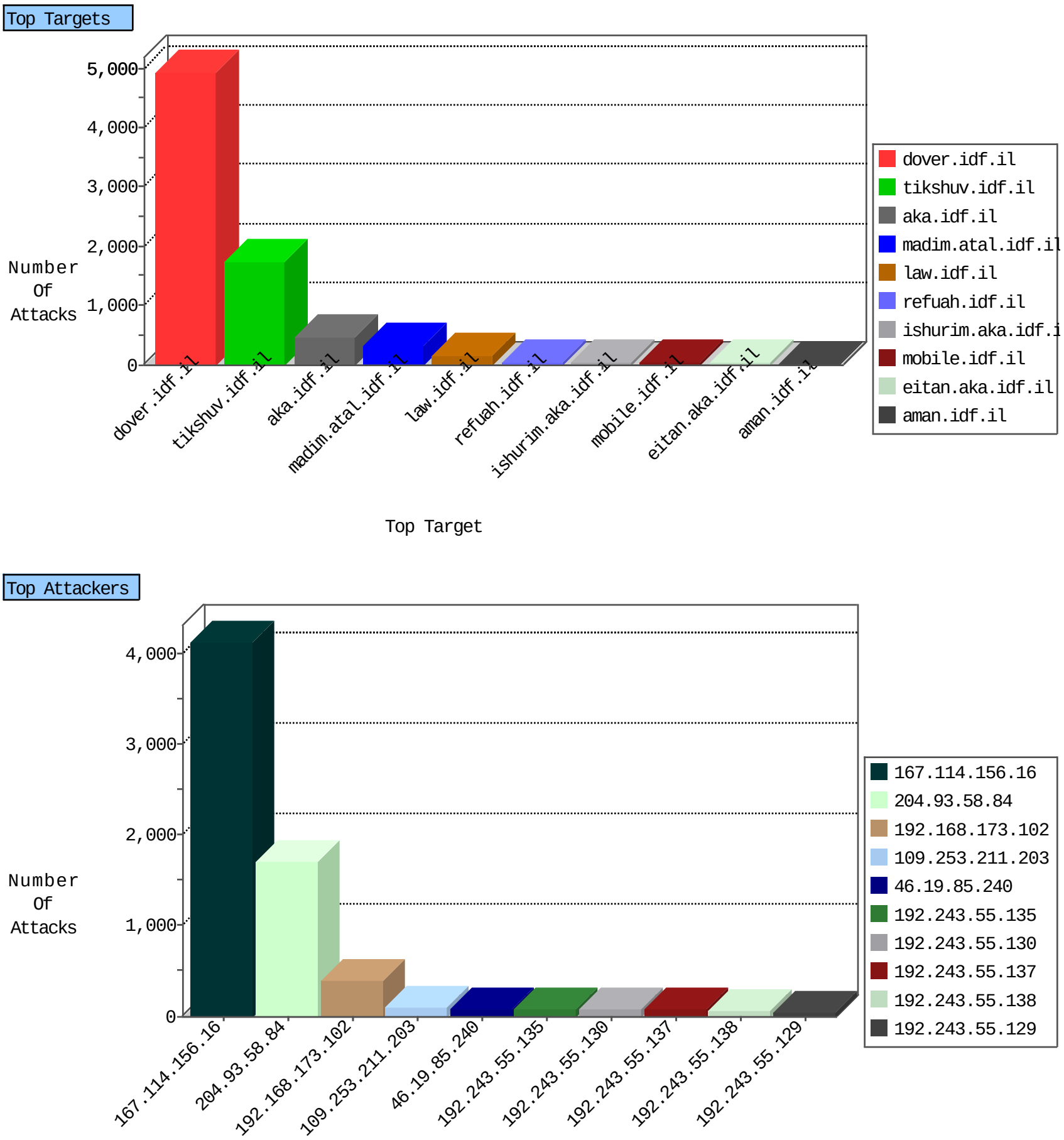
04-11-2016-09:04:01 to 04-11-2016-10:04:01

IDF Under Attack Daily Report



04-11-2016-09:04:01 to 04-11-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4141
80.178.189.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	325
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	192
94.159.130.204	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	131
82.166.137.19	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.121.138.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
192.118.64.29	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
37.26.148.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
91.227.165.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
84.94.180.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
2.54.144.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
192.243.55.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.3.146.200	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
2.53.41.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
179.43.144.50	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
221.2.208.18	China	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.247.243	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.118	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
221.2.208.18	China	147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	1
62.219.190.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.114	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.125	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
192.243.55.134	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.122	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
195.16.162.218	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.118	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
219.74.148.111	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.166.137.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.247.239	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-09:04:01 to 04-11-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.22.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
199.207.253.101	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
88.198.230.79	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
88.198.230.79	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
88.198.230.79	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
2.109.204.29	Denmark	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
88.198.230.79	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-09:04:01 to 04-11-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.116.3.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.77.212	Korea, Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
31.210.187.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.141.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.25.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
156.207.7.229	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.180.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.75.136	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
46.121.97.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.77.212	Korea, Republic of	e.dover.idf.il	ET SCAN NMAP -f -sS	1
5.28.145.31	147.237.72.166	Israel	aka.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
185.130.5.208	147.237.76.38	Lithuania	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1
109.253.218.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.188.158.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.187.157.79	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.219.154.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-09:04:01 to 04-11-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
204.93.58.84	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1708
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	263
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	131
37.26.148.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.124	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
37.26.146.203	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.80.62.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
155.254.239.121	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
84.229.32.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.138	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.114	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.118.12.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.120.126.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.146.176	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.206.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.216.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.209.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.216.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.134.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.15	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.45.255.84	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.106.54.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

04-11-2016-09:04:01 to 04-11-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.211.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.220.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.55.56.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.53.41.252	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	19
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
31.168.126.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	15
109.253.199.124	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	5
80.246.136.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	3
2.53.41.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
94.230.93.134	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.41.252	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.41.252	Block	2
85.65.25.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
207.46.13.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.10.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.100.81	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/2811.pdf	Block	1
192.241.234.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.70.94.230	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1236-he/refuah.aspx	Block	1
94.230.93.198	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.71.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/71513	Block	1
156.207.7.229	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.37.174	Israel	147.237.76.42	refuah.idf.il	Multiple _vti_ from 79.182.37.174	Block	1
46.19.86.223	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.230.93.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/general.aspx	Block	1
174.129.237.157	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
109.253.206.197	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
94.230.93.201	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.136.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
176.228.61.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.227.144.220	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
46.120.248.122	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
94.230.93.252	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.110.117.31	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper	Block	1
175.43.95.77	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/+navmenu.qc+	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
94.230.93.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
23.81.90.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

04-11-2016-09:04:01 to 04-11-2016-10:04:01