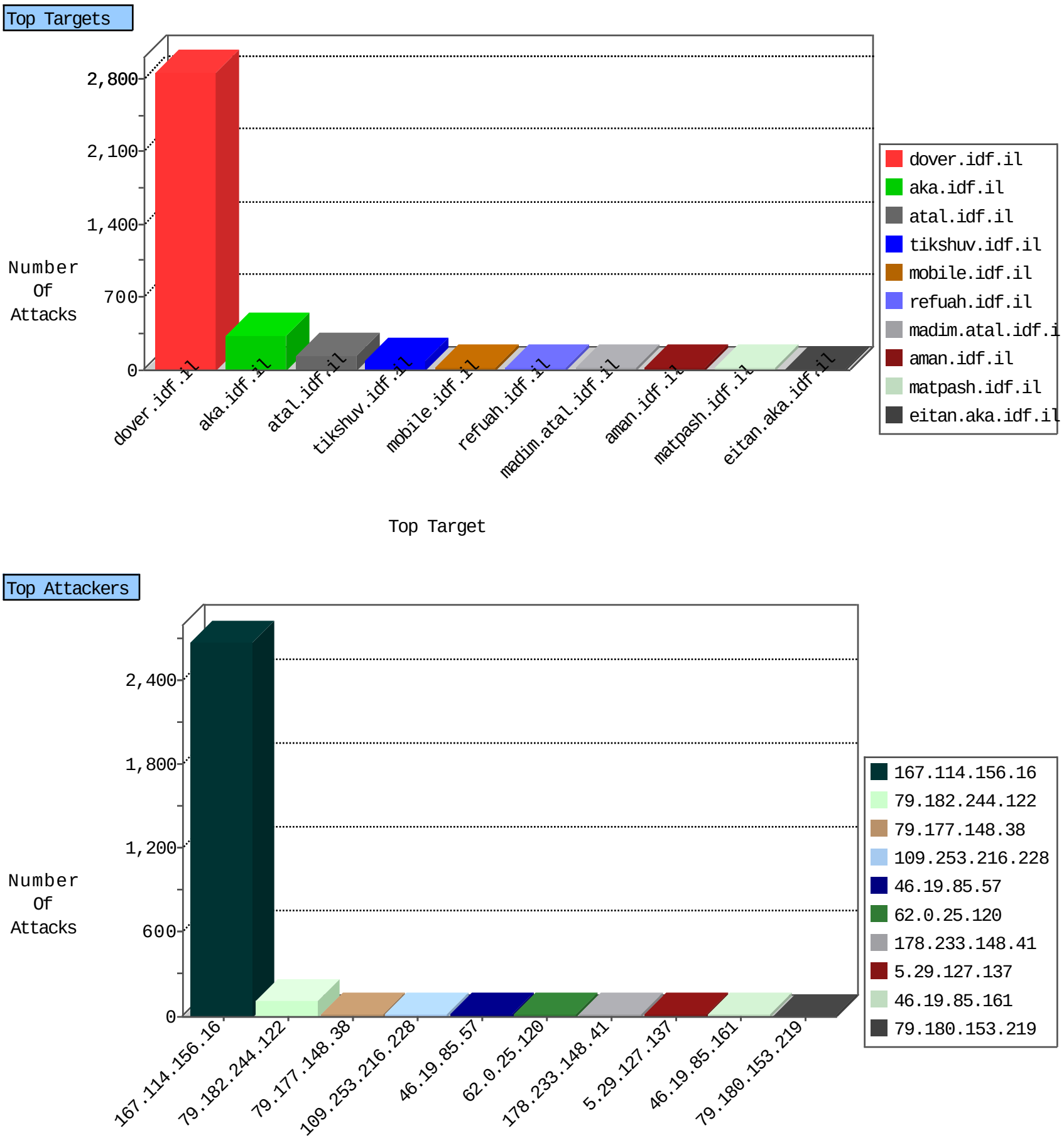
03-13-2016-18:04:03 to 03-13-2016-19:04:03

IDF Under Attack
Daily Report



03-13-2016-18:04:03 to 03-13-2016-19:04:03

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	DOS-Tool-SwitchbladG	dest-reset	3951
109.65.112.218	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
213.57.91.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.112.218	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
170.210.203.68	Argentina	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.56.28.67	Netherlands	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

03-13-2016-18:04:03 to 03-13-2016-19:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
84.108.31.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.120.53.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
2.52.182.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.69.96.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.9.87.111	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.40.95.70	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
62.90.179.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.88.188.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.117.62.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.235.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
164.132.161.7	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.20	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.29	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.80	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.195	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.122	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-13-2016-18:04:03 to 03-13-2016-19:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
84.108.103.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.176	Cote D'Ivoire	test.ncore.idf.i	ET SCAN NMAP -sS window 2048	1
82.166.75.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.109.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.97	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.199.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
184.80.10.136	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.19.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.24.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.11.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.154.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.115.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.176	Cote D'Ivoire	test.ncore.idf.i	ET SCAN NMAP -f -sS	1
79.182.219.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.110.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.25.105.249	147.237.77.216	United Arab Emirates	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
37.142.183.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
184.80.10.136	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
149.88.186.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.8.24	Austria	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
85.65.6.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-13-2016-18:04:03 to 03-13-2016-19:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.244.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	66
79.177.148.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
62.0.25.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	15
178.233.148.41	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.216.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.57	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
120.63.153.32	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.168.93.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.81.36.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.177.143	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.117.101.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.223.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.173.174.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.130.77	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.144.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.168.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.57	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.253.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.170.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.221.251	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.153.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.53.31.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.180.153.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.22.130.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.182.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
31.154.160.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.52.5.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.2.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.30.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.203.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.88.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.94.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
79.180.207.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.57.97	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
2.54.145.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
174.129.237.157	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 174.129.237.157	Block	4
109.253.216.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
174.129.237.157	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
149.88.157.62	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
109.253.216.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.113.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
99.237.79.37	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 99.237.79.37	Block	3
80.246.130.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.205.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
174.129.237.157	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 174.129.237.157	Block	2
149.78.113.170	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
99.237.79.37	Canada	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
213.57.91.199	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.86.213	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
31.168.31.178	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
87.70.71.145	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/slider.js	Block	1
2.53.31.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.118.11.120	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.120.68.255	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
39.59.18.23	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
220.181.108.142	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
79.179.4.202	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
8.29.198.35	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/feed/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/drushim/misrot.aspx	Block	1
149.78.65.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
37.26.148.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.45.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/2685.jpg	Block	1
195.154.207.160	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 195.154.207.160	Block	1
157.55.39.122	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
46.120.68.255	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
41.193.211.221	South Africa	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
8.29.198.37	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/feed/	Block	1
79.182.244.122	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
46.116.30.75	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
37.26.148.180	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3394.jpg	Block	1
5.29.34.216	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
195.154.207.160	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/shared/usercontrols/headerupper/	Block	1
157.55.39.122	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
46.120.68.255	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1