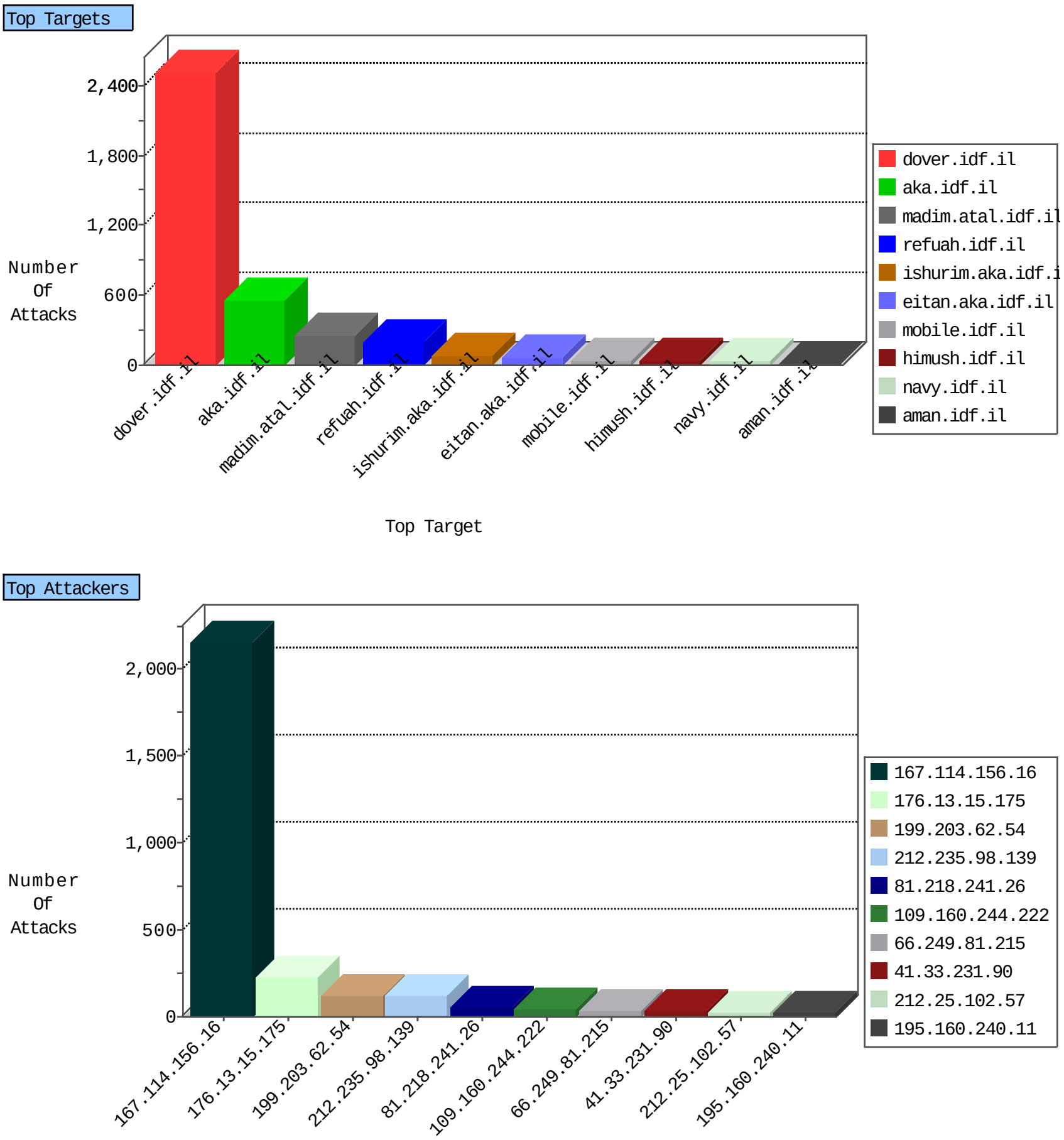
12-16-2015-10:04:04 to 12-16-2015-11:04:04

IDF Under Attack
Daily Report



12-16-2015-10:04:04 to 12-16-2015-11:04:04

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	3435
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
92.85.50.249	Romania	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.179.177.148	Israel	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
178.155.30.39	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
199.115.117.117	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Https	drop	1

12-16-2015-10:04:04 to 12-16-2015-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.203.196.253	Israel	147.237.72.166	aka.idf.il	14062: HTTP: SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)	Block	2
162.210.196.130	United States	147.237.77.216	dover.idf.i	C1000106: HTTP: majestic bot	Block	1

12-16-2015-10:04:04 to 12-16-2015-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.253.193.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.166.169.97	147.237.77.74	Lithuania	law.idf.il	Tehila - Perl LWP with fake user agent	1
94.102.48.195	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.219	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.219	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.219	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.174.93.219	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.116.236.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.24.186.193	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.7.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.74.208.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
2.54.156.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.219	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.219	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.219	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
93.174.93.219	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.219	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
188.13.52.162	147.237.8.27	Italy	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
81.218.56.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-16-2015-10:04:04 to 12-16-2015-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.203.62.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	119
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	86
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
46.19.85.111	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	21
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
212.199.50.254	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	12
2.52.38.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
62.0.197.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
213.57.134.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
132.66.40.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.176.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.184.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.164.218	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	8
37.26.146.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.250.7.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
193.104.77.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.13.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.229.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.159.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.244.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.111.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.185.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.218.231	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	6
109.67.38.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.25.69.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.52.160.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.15.175	Block	69
109.160.244.222	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.244.222	Block	38
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	16
2.54.20.32	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.20.32	Block	10
2.54.139.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.24.207.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.24.207.12	Block	8
212.179.46.16	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.72	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.72	Block	6
212.25.102.57	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
2.52.188.229	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.166.169.97	Lithuania	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.166.169.97	Block	3
176.13.22.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
212.76.110.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
84.228.102.46	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
176.12.136.24	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
2.54.11.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.13.3.52	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	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
2.54.16.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.76.110.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.110.11	Block	2
46.19.85.72	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.16.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.1.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
2.54.20.32	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
92.85.50.249	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 92.85.50.249	Block	1
46.166.169.97	Lithuania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/fckeditor/	Block	1
176.13.3.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 82.80.196.44 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.19.86.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
199.203.53.3	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/main	Block	1
2.54.29.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.79.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx&sa=u&ved=0ahukewjxypfy-9_jahvmwbokhd1aa0oqfggwmau&usg=afqjcnepjiaix3qorrzujiwlvwkx6xrmsw	Block	1
46.35.253.161	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation sCh in www.idf.il/	Block	1