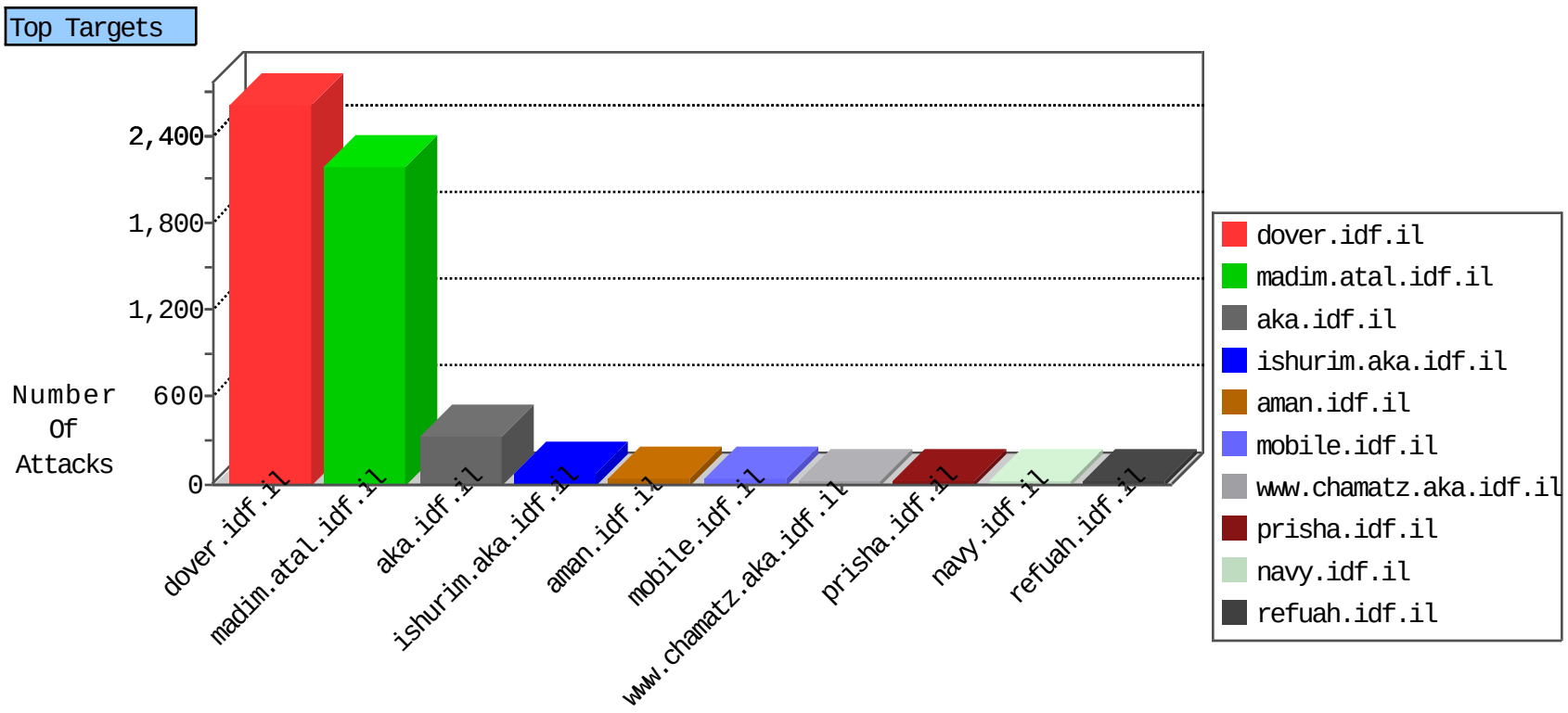
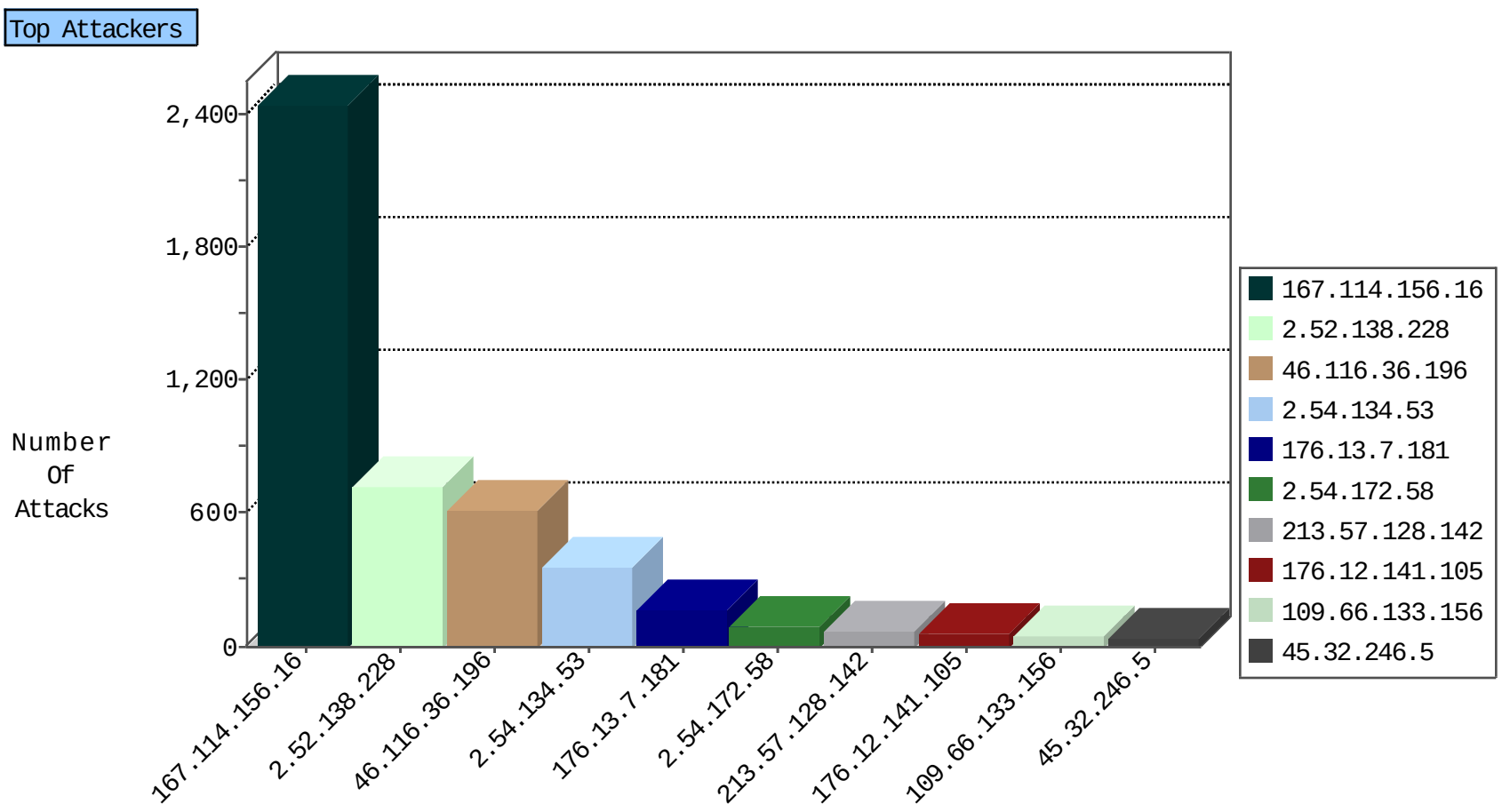
12-10-2015-10:04:01 to 12-10-2015-11:04:01

IDF Under Attack
Daily Report





12-10-2015-10:04:01 to 12-10-2015-11:04:01

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	DOS-Tool-SwitchbladG	dest-reset	3420
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	229
45.32.246.5		147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
45.32.246.5		147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	3
115.239.228.8	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.151.55.116	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
66.151.55.110	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
66.151.55.114	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.151.55.117	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

12-10-2015-10:04:01 to 12-10-2015-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-10-2015-10:04:01 to 12-10-2015-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.251.167.74	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.2.52	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.236.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.74.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
45.32.246.5	147.237.76.39		mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
12.139.41.189	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.2.52	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
87.69.195.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.247.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -f -sS	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
12.139.41.189	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.151.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-10-2015-10:04:01 to 12-10-2015-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.108	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
207.241.229.96	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	12
45.32.246.5		147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.64.160.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.89.217.225		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	9
66.249.93.106	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
176.13.18.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
45.32.246.5		147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
80.246.136.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.91.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.170	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.28	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.98.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.210	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.139.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence		monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.20.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.176.236.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.139.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	5
185.3.146.249	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.229	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.139.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Spoofed Reset		monitor	4
50.135.80.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.56.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
212.235.93.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.34	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.174.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.102.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.121.145.175	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
82.80.198.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.67.56.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.3.146.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.143.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.241.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.230.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3

12-10-2015-10:04:01 to 12-10-2015-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.36.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	387
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.138.228	Block	238
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	217
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	185
46.116.36.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	167
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	124
176.13.7.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
2.54.172.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
46.116.36.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	67
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.52.138.228	Block	66
176.13.7.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62
176.12.141.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
109.66.133.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	41
79.183.196.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
2.54.172.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
176.13.14.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	17
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	10
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.52.13.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
79.179.60.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.12.142.234	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
176.13.4.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.17.16	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.17.16	Block	3
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	2
84.111.110.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.117.21.201	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.21.201	Block	2
37.26.148.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.70	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
2.54.180.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
37.142.241.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	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
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
188.143.232.34	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.146.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.19.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.151.36.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.74.100	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/csafcsf.aspx	Block	1
82.80.198.164	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 82.80.198.164 (Open Mode)	None	1
207.46.13.186	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ajax/navbar	Block	1
46.166.139.20	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/xmlrpc.php	Block	1
132.66.222.158	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

12-10-2015-10:04:01 to 12-10-2015-11:04:01