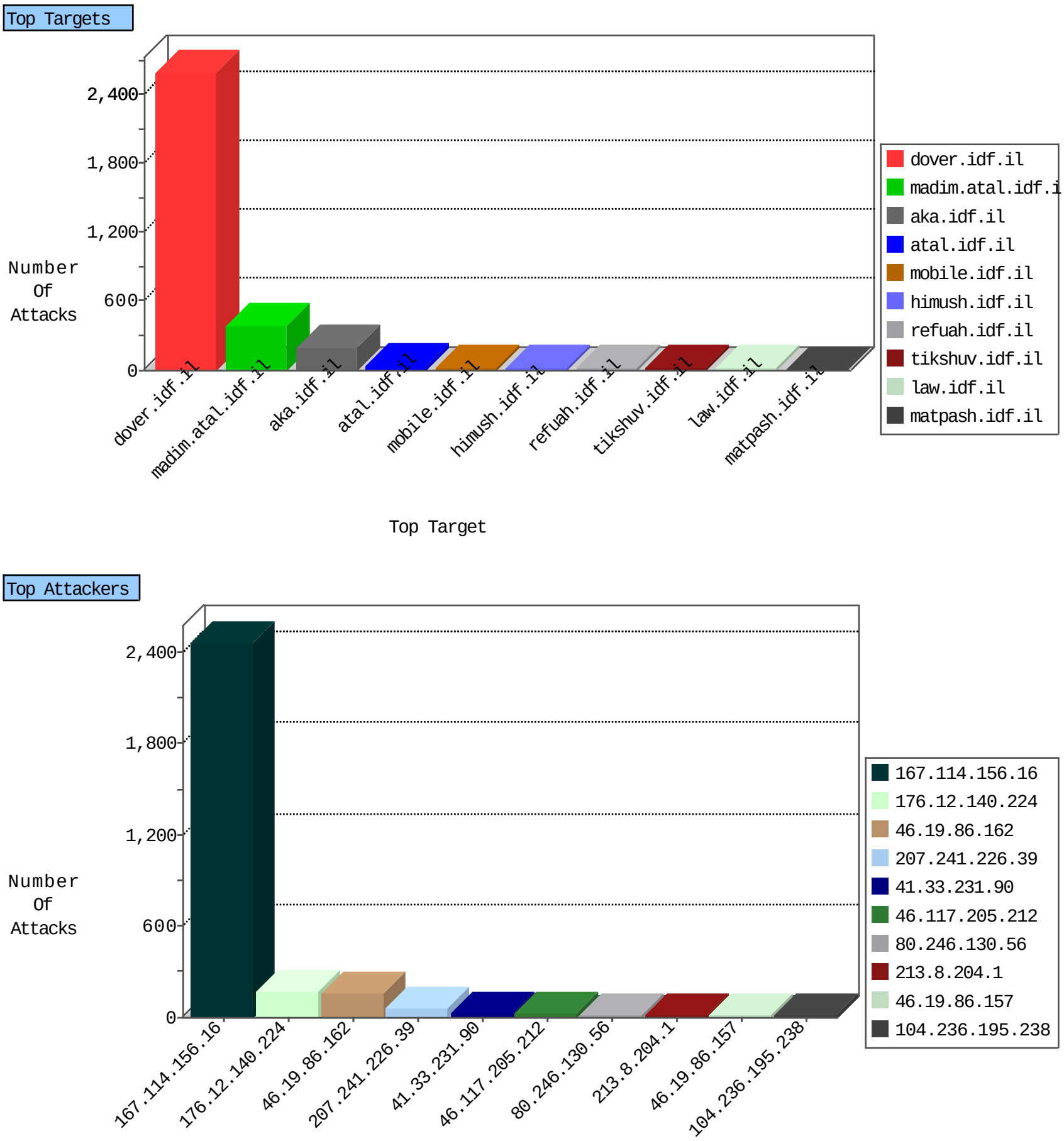
12-11-2015-09:04:03 to 12-11-2015-10:04:03

IDF Under Attack
Daily Report



12-11-2015-09:04:03 to 12-11-2015-10:04:03

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	3413
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	67
188.138.33.34	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.210	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.50	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
94.102.49.210	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.50	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
94.102.49.210	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
188.138.33.34	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
107.150.55.53	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
94.102.49.210	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.50	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

12-11-2015-09:04:03 to 12-11-2015-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-11-2015-09:04:03 to 12-11-2015-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.56	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
125.39.180.115	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.193.2.8	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
179.155.84.106	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.33.224.238	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.193.2.8	147.237.76.198	France	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.92.214.215	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-11-2015-09:04:03 to 12-11-2015-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.117.205.212	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
104.236.195.238		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.182.60.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.56	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
179.87.225.18	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.149.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.35.205.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
179.87.225.18	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.148.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.186	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
212.0.130.192	Sudan	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	5
176.12.149.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.226.41	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
5.102.254.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.130.56	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.35	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.186.20.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.155.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.246.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.35	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.186.20.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.127.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.52.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.9.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.129.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.95.2.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.161.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.69.246.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.128.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.162.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.67.108.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
169.229.3.90	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.12.149.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

12-11-2015-09:04:03 to 12-11-2015-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.140.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
207.241.226.39	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	61
176.12.140.224	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.224	Block	53
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
207.46.13.30	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
46.19.86.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.205.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.9.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.191.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.70.142	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
79.205.117.249	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
2.54.8.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.14.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
109.67.150.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
80.246.136.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.125	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/1133-22638-he/dover.aspx.	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
46.19.86.204	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
128.232.110.29	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
37.26.148.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.172.158.186	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.199.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
109.64.189.31	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
213.8.204.2	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.28.183.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
173.252.114.116	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.117.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.191.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.241.226.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/best/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.29.46.213	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.64.215.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.215.25	Block	1
207.46.13.71	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
46.117.34.210	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
37.142.196.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.228.217.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
109.67.170.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.145.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-11-2015-09:04:03 to 12-11-2015-10:04:03