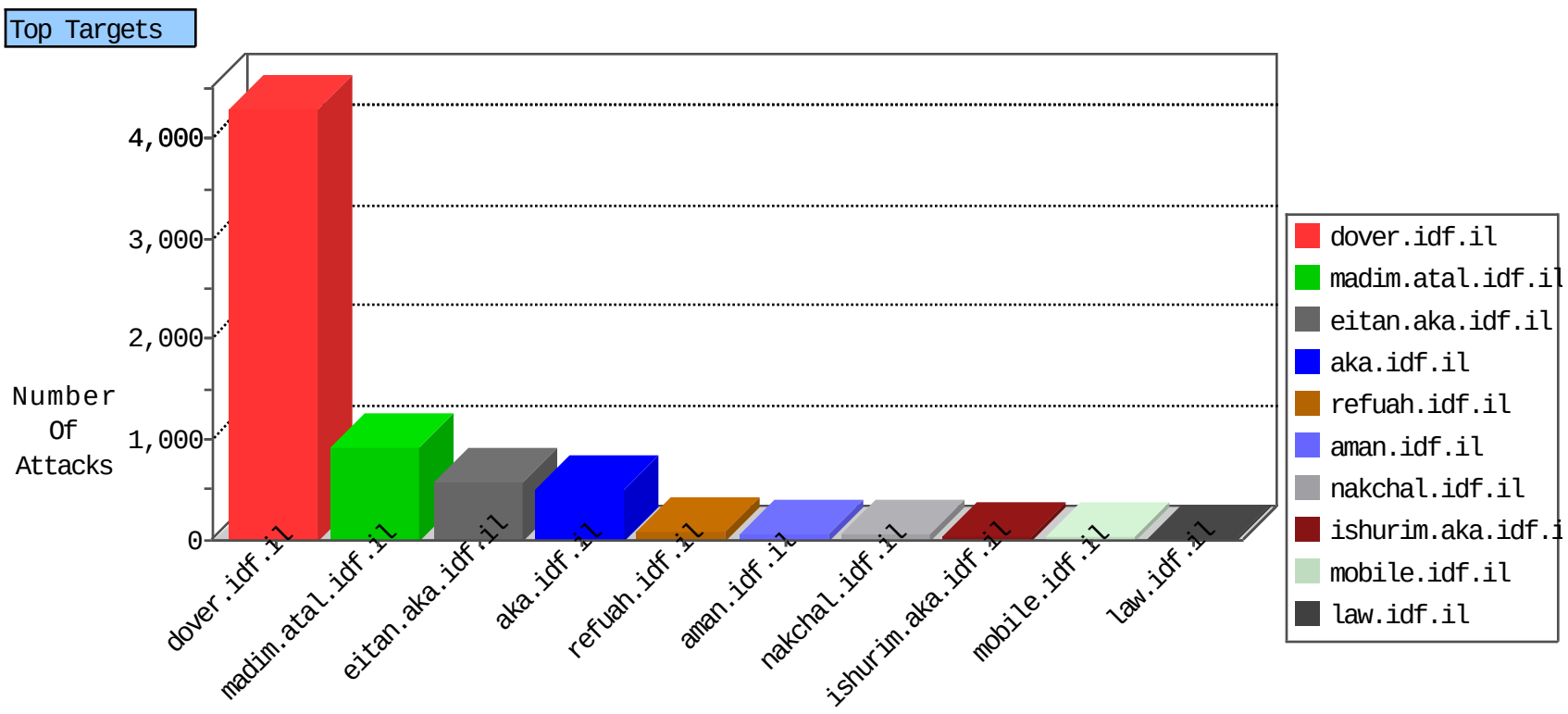
11-25-2015-12:04:07 to 11-25-2015-13:04:07

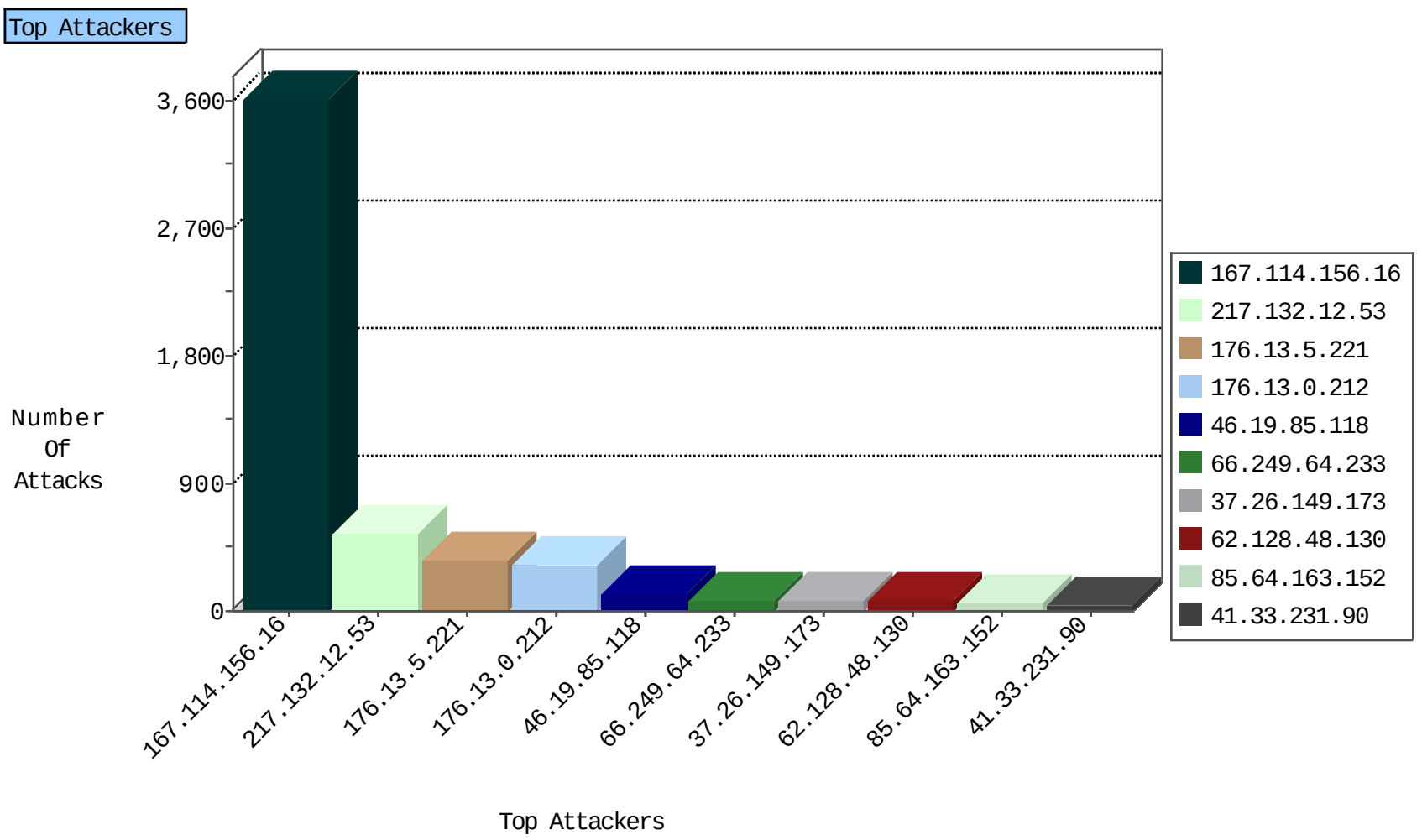
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-25-2015-12:04:07 to 11-25-2015-13:04:07

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	2943
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	243
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	21
41.142.224.114	Morocco	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	8
221.3.83.12	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
95.172.79.236	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
95.172.79.244	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

11-25-2015-12:04:07 to 11-25-2015-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.52.139	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
51.254.131.243	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
69.30.218.234	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

11-25-2015-12:04:07 to 11-25-2015-13:04:07

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	2
93.113.125.11	147.237.76.38	Romania	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.61.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.81.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.135	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
217.78.56.183	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
37.142.200.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.66.251.233	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
111.93.198.54	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
93.113.125.11	147.237.76.86	Romania	navy.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.8.24	Romania	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.146.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.135	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.195.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.82.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.6.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.66.251.233	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.76.148	Romania	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-25-2015-12:04:07 to 11-25-2015-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1432
217.132.12.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	495
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
62.128.48.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
31.135.149.251	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	40
85.64.163.152	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
85.64.163.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
37.26.148.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.13.8.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
37.26.146.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.250.244.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
213.57.138.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
100.100.99.174		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
185.120.126.19		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.178.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
109.64.219.84	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.194.202.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.54.37.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
132.71.80.48	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
149.78.38.239	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.152.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.119	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
46.19.86.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.67.113.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.24.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.142.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.32.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.28.169	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.126.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.120.56.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.30.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.126.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.56.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

11-25-2015-12:04:07 to 11-25-2015-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.5.221	Block	195
176.13.0.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
176.13.0.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	153
176.13.5.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
217.132.12.53	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 217.132.12.53	Block	56
176.13.5.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.5.221	Block	47
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
2.54.4.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
2.54.63.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
193.105.199.65	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	11
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
193.105.199.65	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 193.105.199.65	Block	8
147.161.1.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
81.218.70.243	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	6
176.13.13.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.148.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
147.161.1.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
2.54.142.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.1.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.120.126.7		147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.120.126.7	Block	3
176.13.22.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.208.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachdar/	Block	3
2.52.181.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.5.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
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	2
80.246.136.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
176.13.12.39	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.237.204.91	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
2.54.147.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.102.49.210	Netherlands	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.7.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.163.152	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
213.57.31.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
176.13.5.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
79.181.129.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl66.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
193.105.199.65	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	1
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.68.40	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.13.23.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/news.asp	Block	1

11-25-2015-12:04:07 to 11-25-2015-13:04:07