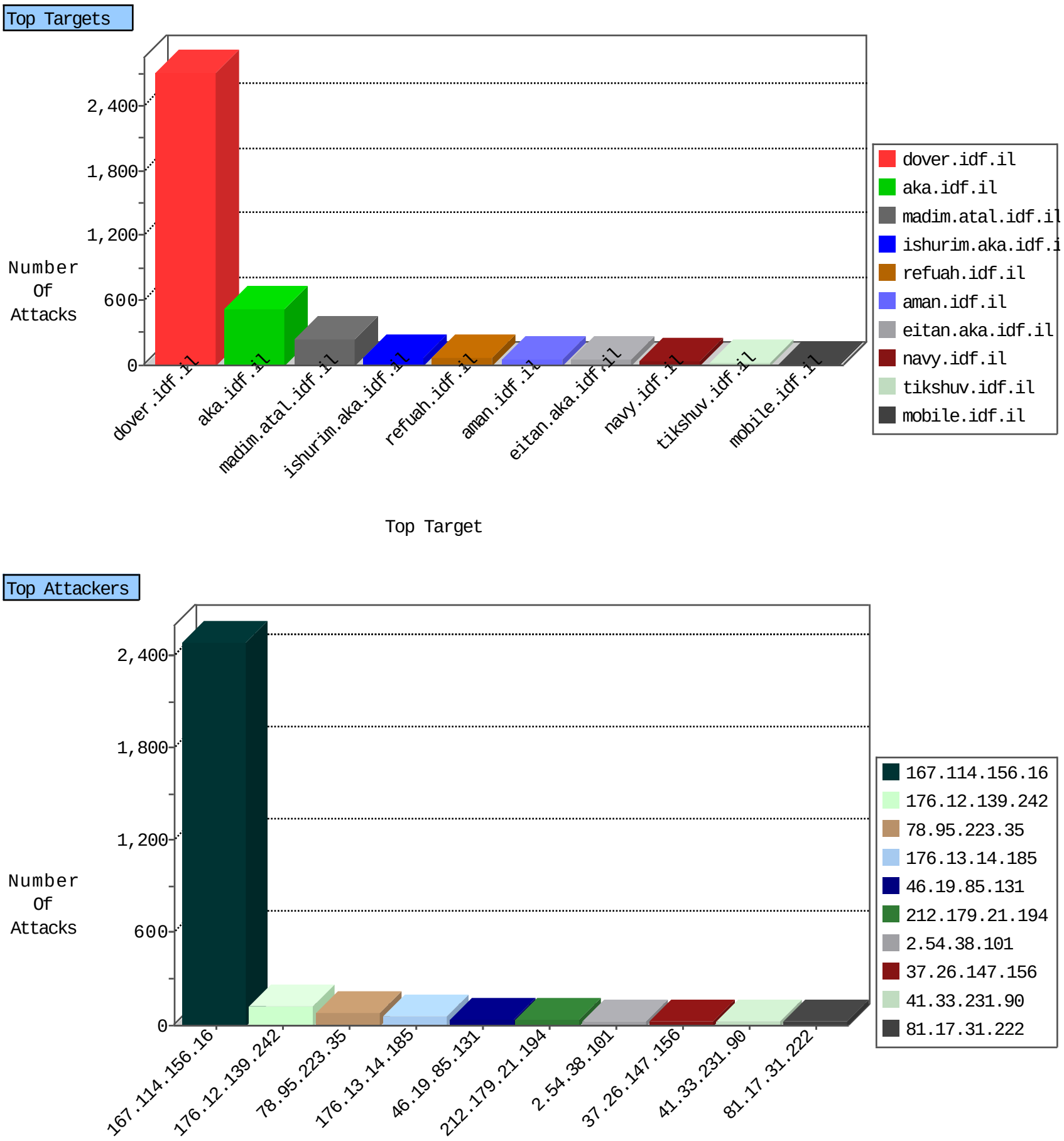
12-07-2015-11:04:03 to 12-07-2015-12:04:03

IDF Under Attack Daily Report



12-07-2015-11:04:03 to 12-07-2015-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.142	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8797
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3632
66.249.65.37	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	80
80.246.140.139	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
167.88.7.243	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
219.145.32.137	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.254	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
219.145.32.137	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
106.120.48.128	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
223.68.193.163	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.231	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
185.35.62.49	Switzerland	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

12-07-2015-11:04:03 to 12-07-2015-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.132	Italy	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-07-2015-11:04:03 to 12-07-2015-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.140.139	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
213.236.42.134	147.237.77.176	Saudi Arabia	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.114	147.237.76.196	Ukraine	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.166.147	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.166.131.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.207.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.60.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.246.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.153.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.236.42.134	147.237.77.176	Saudi Arabia	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.166.147	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
85.65.140.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.23.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.11.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-07-2015-11:04:03 to 12-07-2015-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.131	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
78.95.223.35	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
78.95.223.35	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
81.218.196.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
78.95.223.35	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
79.179.54.94	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
78.95.223.35	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	13
37.26.147.156	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.38.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
80.246.136.160	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.156	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
2.54.33.134	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.207	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.17.31.222	Switzerland	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.156	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
78.95.223.35	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.140.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.66.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.8	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.66.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.38.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.17.31.222	Switzerland	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.112.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
132.64.8.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.181.112.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.112	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.56.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.130.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
37.26.147.196	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.28.157.11	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.100.45	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
78.95.223.35	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.194.207.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.102	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.28.157.11	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.10.150	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

12-07-2015-11:04:03 to 12-07-2015-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.139.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
176.13.14.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	30
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.11.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.250.192.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.250.192.12	Block	7
37.26.148.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.64.160.30	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.160.30	Block	5
176.13.13.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.64.160.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	4
109.186.59.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
81.17.31.222	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.145.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.234.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.255.19	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 93.173.255.19	Block	3
5.29.110.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
92.61.237.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.160.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	2
77.127.25.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.18.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.117.60.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
84.95.247.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	2
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	2
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.17	Block	2
2.52.37.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.104.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
176.13.11.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.162.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.205.198.47	United Arab Emirates	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
46.116.66.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.255.19	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 93.173.255.19	Block	1
93.173.255.19	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name RÂ³Â?Ã“ `Â´]}[[#17]]G0{=ÂµÂµ[[#2]]Ãª[[#28]][[#15]]Ã“	Block	1
212.143.137.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl10.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.182.6.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/elramklali.aspx	Block	1
46.19.85.58	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
5.29.242.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.192.12	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
207.46.13.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1

12-07-2015-11:04:03 to 12-07-2015-12:04:03