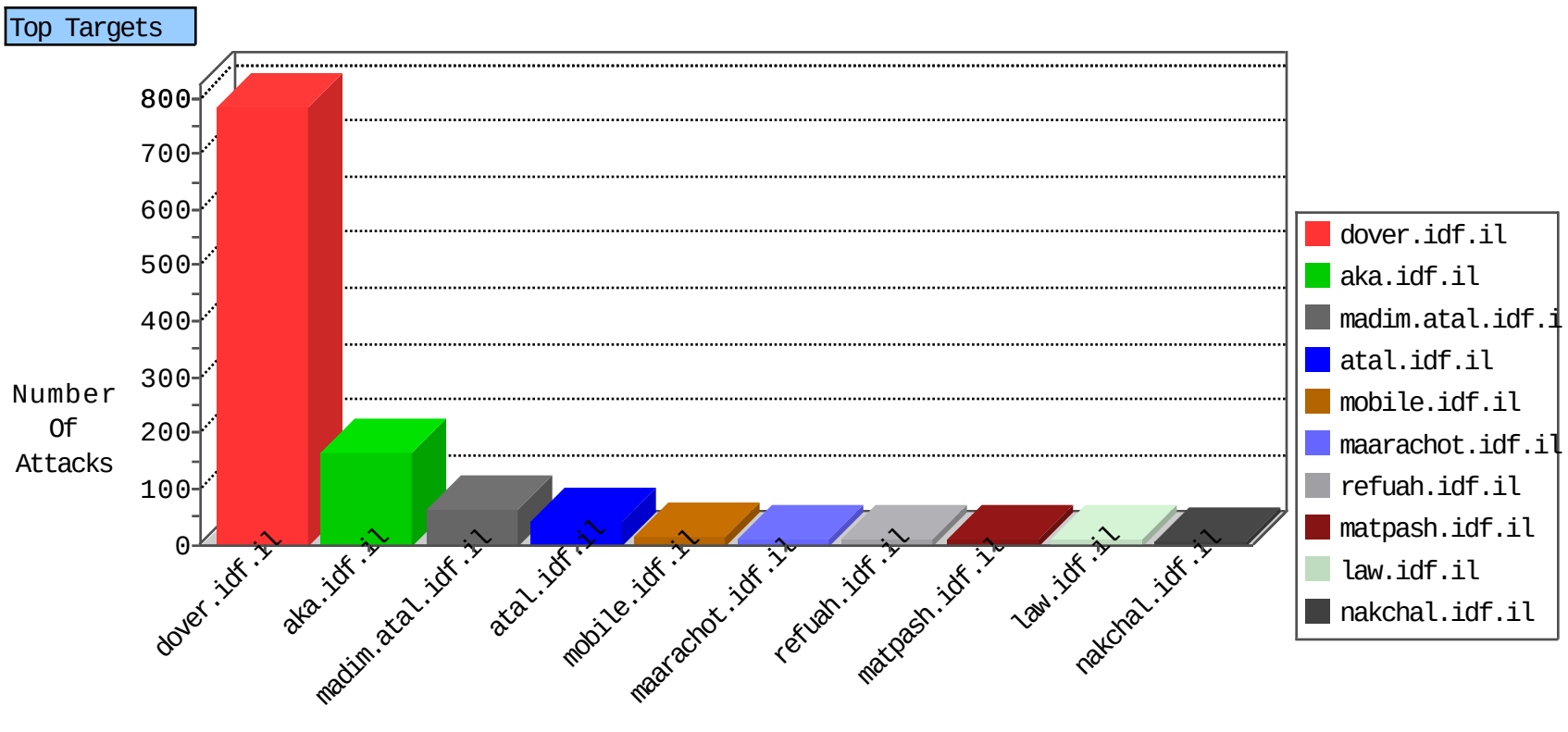
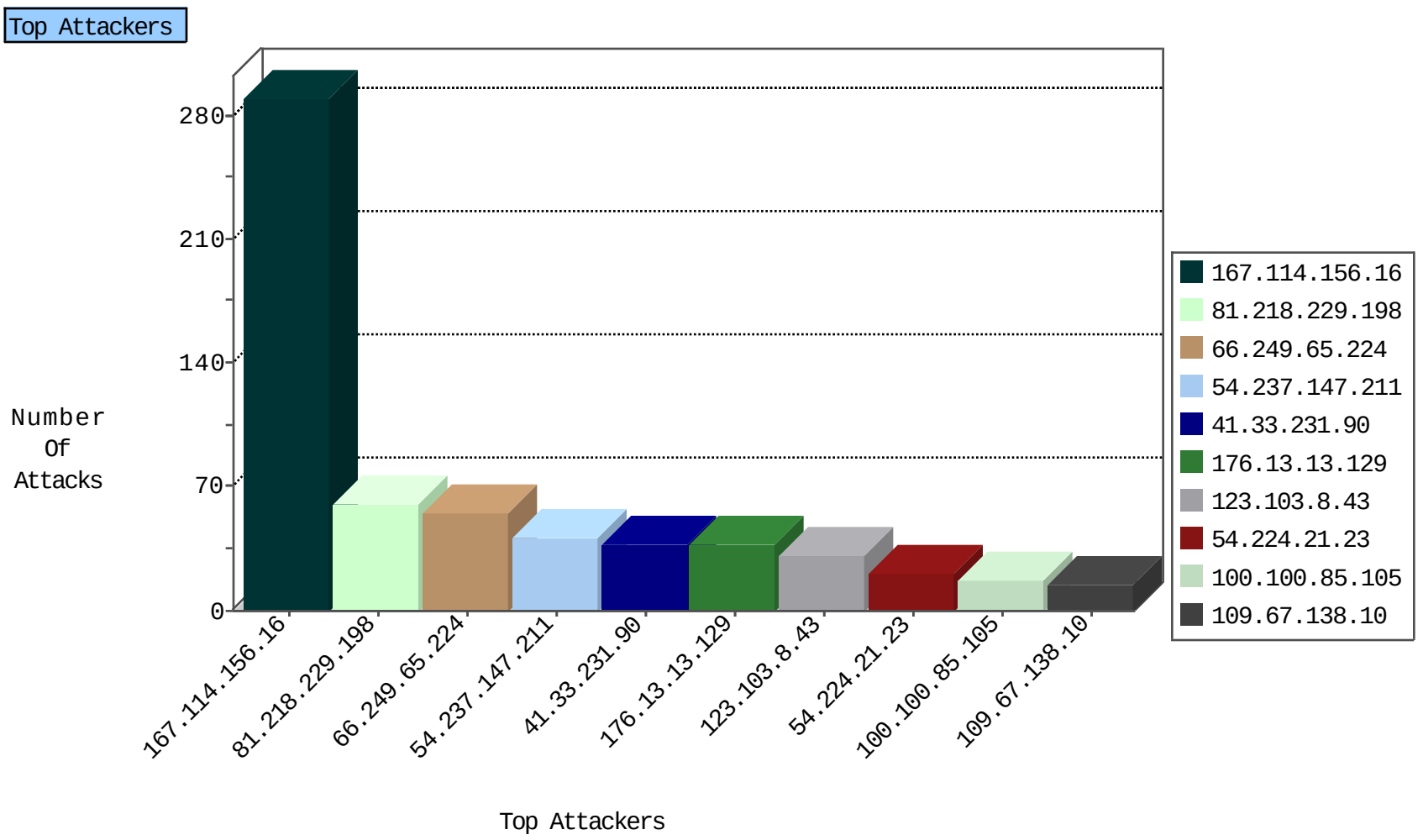
11-21-2015-10:04:04 to 11-21-2015-11:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-21-2015-10:04:04 to 11-21-2015-11:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	17156
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	191
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	33
176.12.138.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
77.127.224.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
5.28.164.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
31.154.161.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
89.139.168.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-21-2015-10:04:04 to 11-21-2015-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.243.192	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-21-2015-10:04:04 to 11-21-2015-11:04:04

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	4
66.249.66.72	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
121.40.195.144	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
31.6.71.154	147.237.77.205	Poland	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
219.153.65.239	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
219.153.65.239	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
219.153.65.239	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
186.83.66.138	147.237.72.166	Colombia	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.249.106.23	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
31.6.71.154	147.237.77.234	Poland	halag.idf.il	ET SCAN NMAP -sS window 1024	1
219.153.65.239	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
219.153.65.239	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
219.153.65.239	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.5.201.246	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
188.214.128.12	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

11-21-2015-10:04:04 to 11-21-2015-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
54.237.147.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
81.218.229.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
123.103.8.43	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.85.105		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
179.43.144.48	Switzerland	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
62.219.163.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.57.47		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
84.94.109.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.239.136.124	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
100.100.89.7		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.29.244.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.138.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.138.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.161.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
65.55.210.123	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.70.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.179.25.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.25.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
62.128.45.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.47.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.252.115.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.13.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.252.115.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
100.100.89.7		147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	4
176.12.143.132	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.185.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
136.243.253.138	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
100.100.118.251		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.40	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.165.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.178.145	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
79.176.183.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.226.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.116.46.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.102.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.120.148.239	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.159.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
81.218.229.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	17
2.54.181.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.182.165.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.229.198	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	4
89.139.168.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.14.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.91.149	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (403) in Session from 31.154.91.149	Block	3
81.218.229.198	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.48.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.120.126.1		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.243.192	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.121.198.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.154.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
27.34.110.71	Nepal	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.78.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/mobile/	Block	1
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	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1398294938000	Block	1
37.26.148.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.45	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/~~Ã–â€™~~ Ã–â„¢Ã–Å“Ã–â„¢Ã–â€¢Ã–Â Ã–â€¢Ã–ª	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
141.212.122.160	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
62.102.148.67	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
107.150.55.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on /	Block	1
84.110.210.29	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
31.154.91.149	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per Session	Block	1
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	1
180.76.15.27	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.65.136.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19815-he/idfgdover.aspx	Block	1
40.77.167.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.22.131.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
81.218.229.198	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
149.78.94.32	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3199.pdf	Block	1
84.228.24.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.243.192	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 213.57.243.192	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.67.138.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/×©×§×• ×¤×™×ª 2	Block	1
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.150.43.202	United States	147.237.77.235	sviva.idf.il	Distributed Unauthorized URL Access on /	Block	1
5.29.244.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1