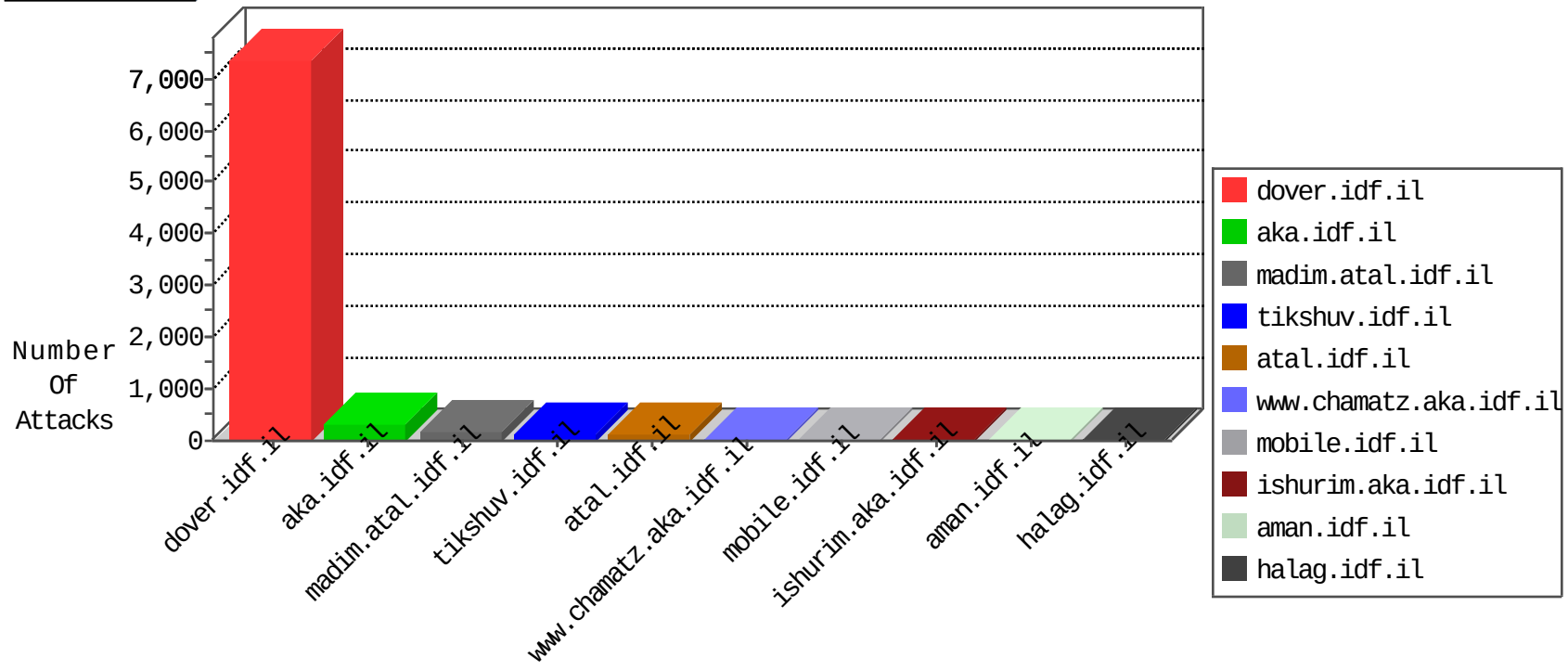
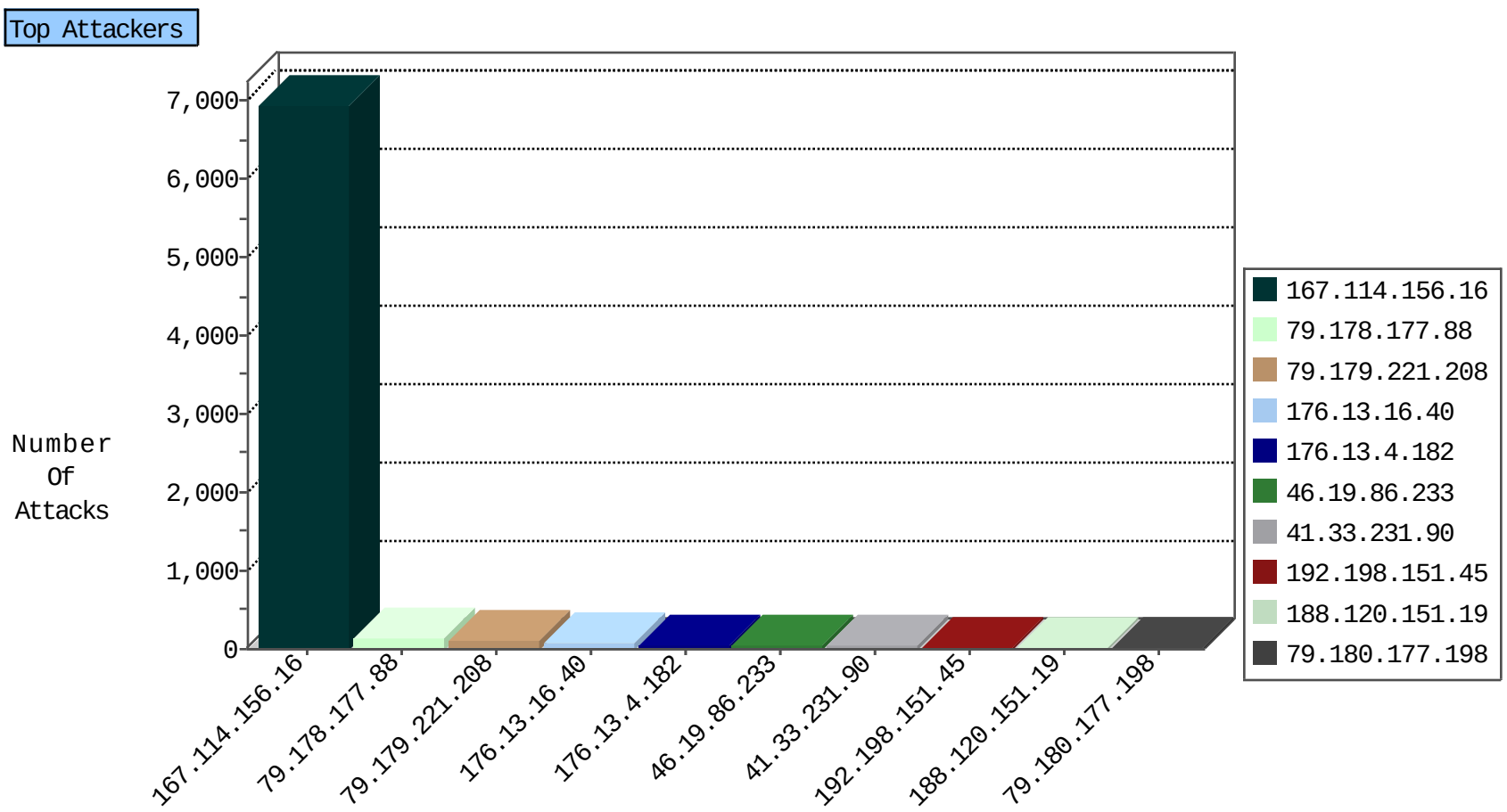
01-14-2016-21:04:00 to 01-14-2016-22:04:00

IDF Under Attack Daily Report





01-14-2016-21:04:00 to 01-14-2016-22:04:00

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	3020
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	180
128.234.108.182	Romania	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
81.129.80.116	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.205.80.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
66.249.69.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4
79.180.177.198	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.180.177.198	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.149.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
222.186.58.169	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.130.5.209		147.237.76.39	mobile.meitav.idf.i	Block_Udp_All_Nets	drop	1
1.82.41.3	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
31.13.161.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.60.5.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
173.208.137.10	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-14-2016-21:04:00 to 01-14-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-14-2016-21:04:00 to 01-14-2016-22:04:00

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	3
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
178.187.59.159	147.237.0.33	Russian Federation	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.210.67.78	147.237.76.200	Turkey	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.77.176	China	matpash.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
194.187.249.70	147.237.76.196	Europe	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.67.78	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.199	Turkey	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.44	Turkey	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-14-2016-21:04:00 to 01-14-2016-22:04:00

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	SAM rule	drop	5185
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1534
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	77
46.19.86.233	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	56
79.179.221.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	49
79.179.221.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
192.198.151.45	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.53	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
188.120.151.19	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
132.64.154.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.19.227	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
83.130.116.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
31.13.161.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.67.187.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
188.120.151.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.54.142.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.188.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.115.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.168.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
74.9.137.146	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.222.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.139	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.187.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.216.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.227	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.178.248.115	Denmark	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.2.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.164.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.84.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.180.177.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
132.64.154.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.121.199.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.8.204.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.142.250.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.204.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.95.229.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.177.88	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
176.13.16.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
176.13.4.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
176.13.4.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
83.130.104.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.81.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.150.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.148.87	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
54.197.189.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
84.108.83.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1
2.54.49.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.65.5.170	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.181.221.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.253.202.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.113	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.116.159.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.158.137.195	Europe	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
31.44.128.185	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11120-he/cogat.aspx&sa=u&ved=0ahukewikg4_ohkrkahvimg4khdgndfoqfggamag&usg=afqjcnfde_unumajve3ak9tzdsjjdolzlq	Block	1
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	1
77.127.230.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.129.94	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.43.145.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.109.101.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-23098-he/dover.asp	Block	1
217.132.144.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.129.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
176.126.252.12	Romania	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
79.182.147.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.50.124.2	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.117.42.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.58.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
84.94.42.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.99	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
176.13.11.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
66.249.64.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
84.228.33.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.135.115	Israel	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
149.88.111.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.137.206	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1