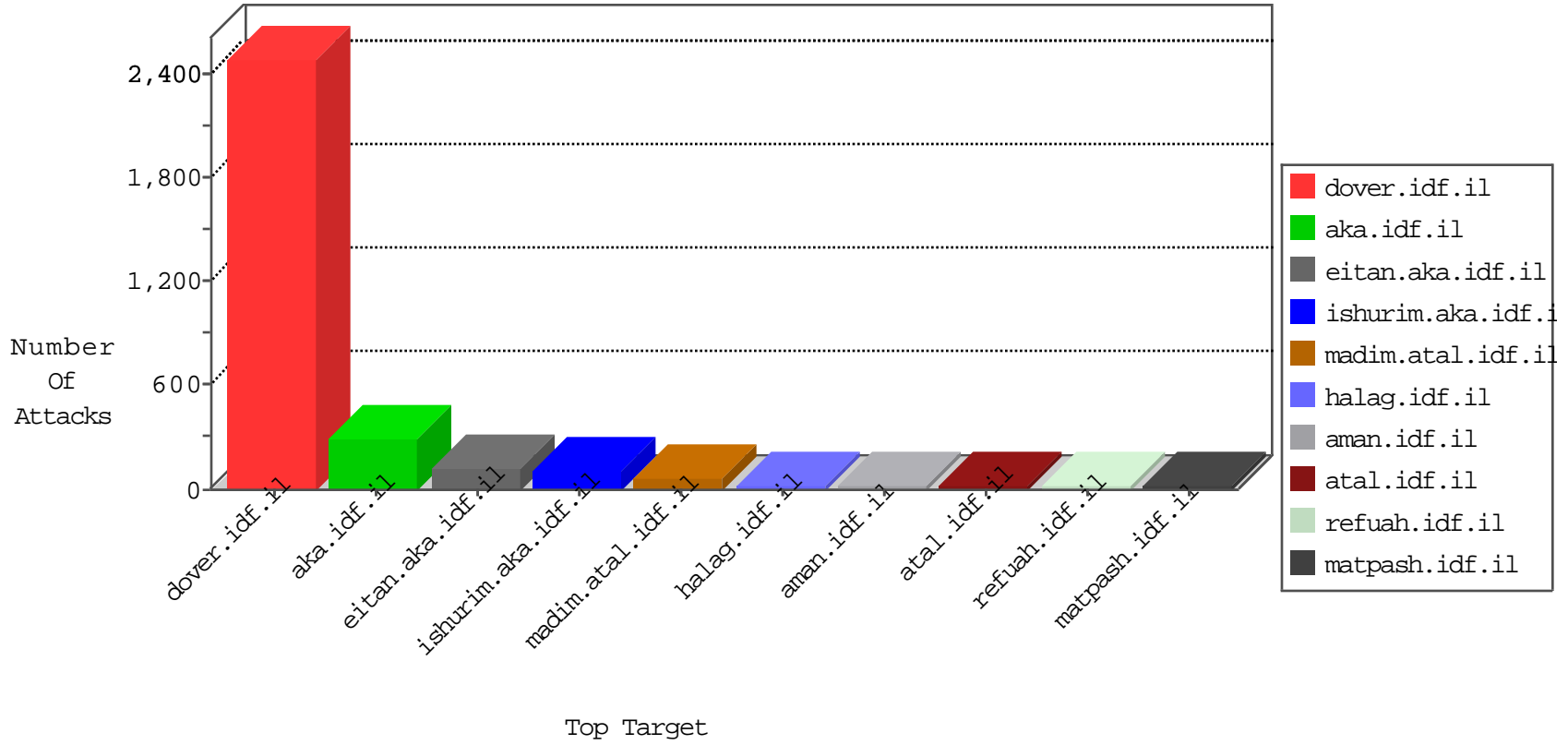


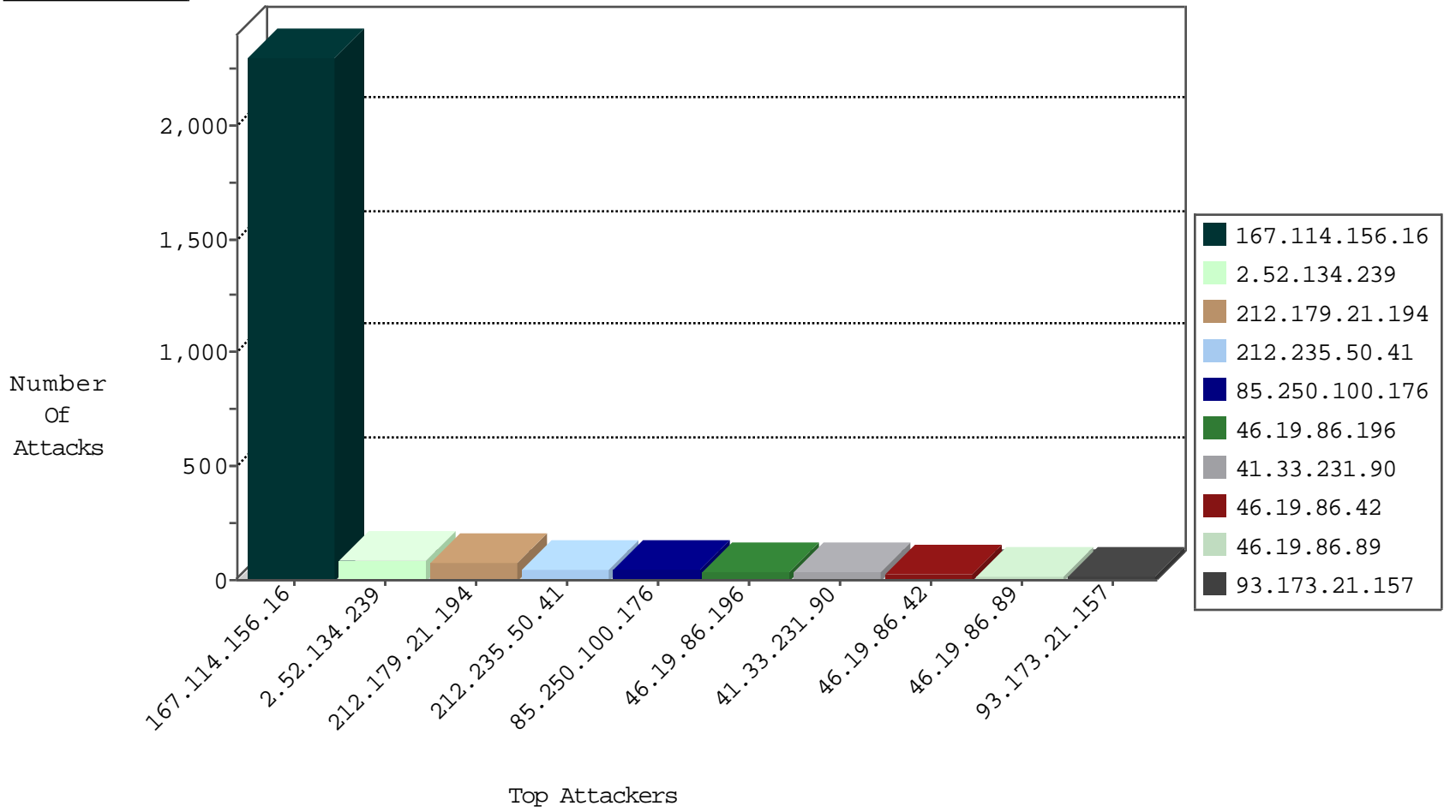
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3459
66.249.64.55	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2682
222.186.21.181	China	147.237.76.198	e.yohanan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
167.88.7.246	United States	147.237.0.19	madim.atal.idf.il	block-sp-trafl	drop	1
146.185.239.100	Russian Federation	147.237.0.19	madim.atal.idf.il	block-sp-trafl	drop	1
167.88.7.230	United States	147.237.76.86	navy.idf.il	block-sp-trafl	drop	1

12-07-2015-08:04:06 to 12-07-2015-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.183	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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
62.0.67.133	147.237.8.46	Israel	e.chimuch.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.181	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.199.71.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.226.22.74	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.1.5.171	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.139	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.90.201.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.25.16.234	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.181	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.172.234.8	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.181	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.143.147.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
168.1.5.171	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
63.142.161.17	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.25.16.234	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

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	34
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
85.250.100.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.42	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
2.52.134.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.52.134.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.52.134.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
79.182.24.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.134.239	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	14
85.250.100.176	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.134.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
62.0.197.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.54.170.76	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.134.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.21.157	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
188.161.150.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.62.24	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.20	Israel	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	6
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.93.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.134.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.62.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
174.67.122.2	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.134.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.220	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.235.50.41	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
180.175.191.116	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
118.69.224.118	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.220	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.166.239	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.89	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
193.16.147.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.54.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.183.142.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.2.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.130.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.32.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.147.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.54.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.54.110	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.50.41	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.13.17.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.37.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	8
37.26.148.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	4
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	4
176.13.16.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.142.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.175.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.112	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.112	Block	2
2.54.145.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.43.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.38.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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	2
66.249.64.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
46.19.85.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.27.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
136.243.36.96	Germany	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.143.147.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/m/	Block	1
192.116.149.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/payslips/payslipslist.asp	Block	1
46.19.86.105	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.18.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.16.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/flash/recruitlane/recruitlane.swf	Block	1
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.27.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
149.88.38.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.150.155.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/home	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/mobile/	Block	1
195.62.53.168	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /css/css	Block	1
157.55.39.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.166.186.212	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.164.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.176.124	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.64.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1