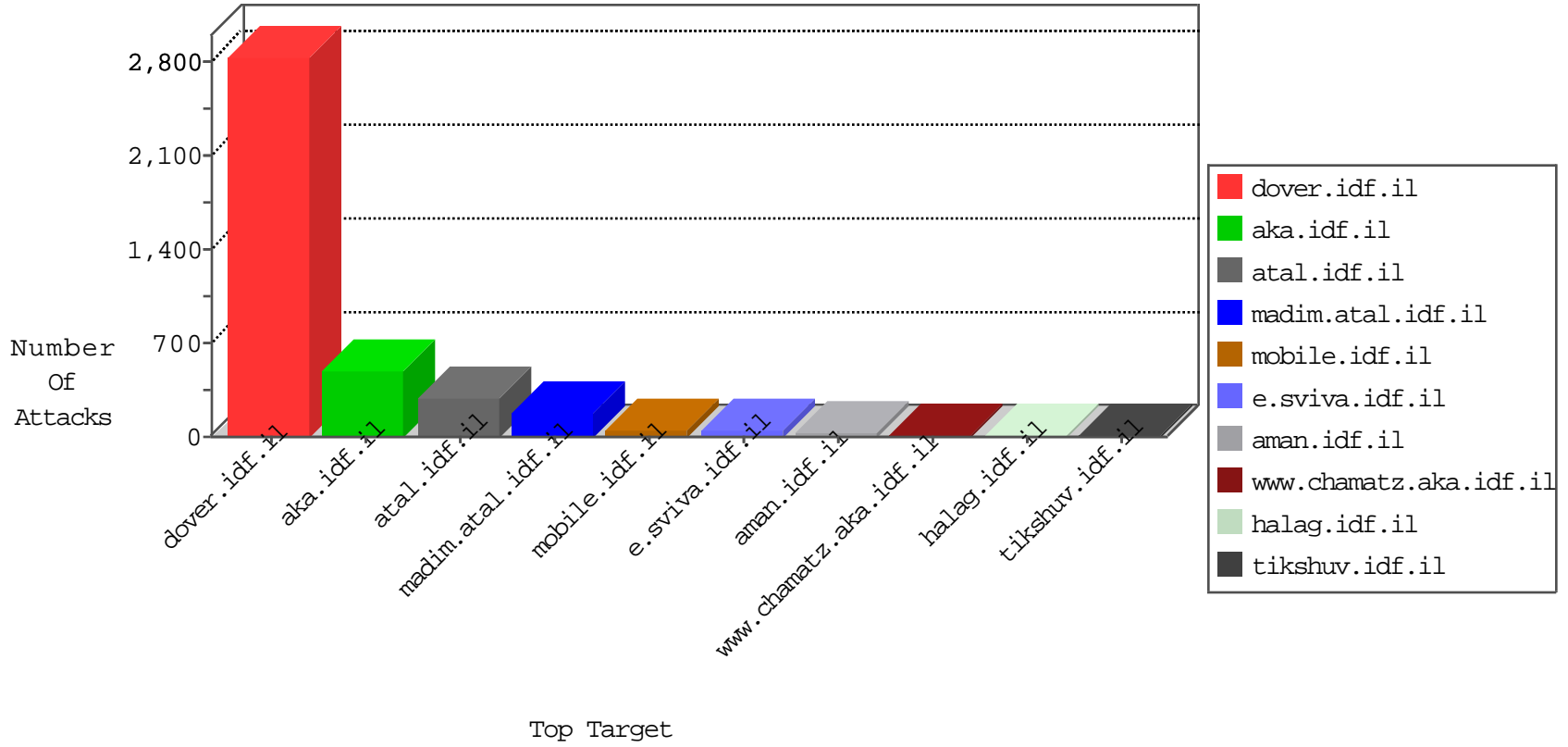


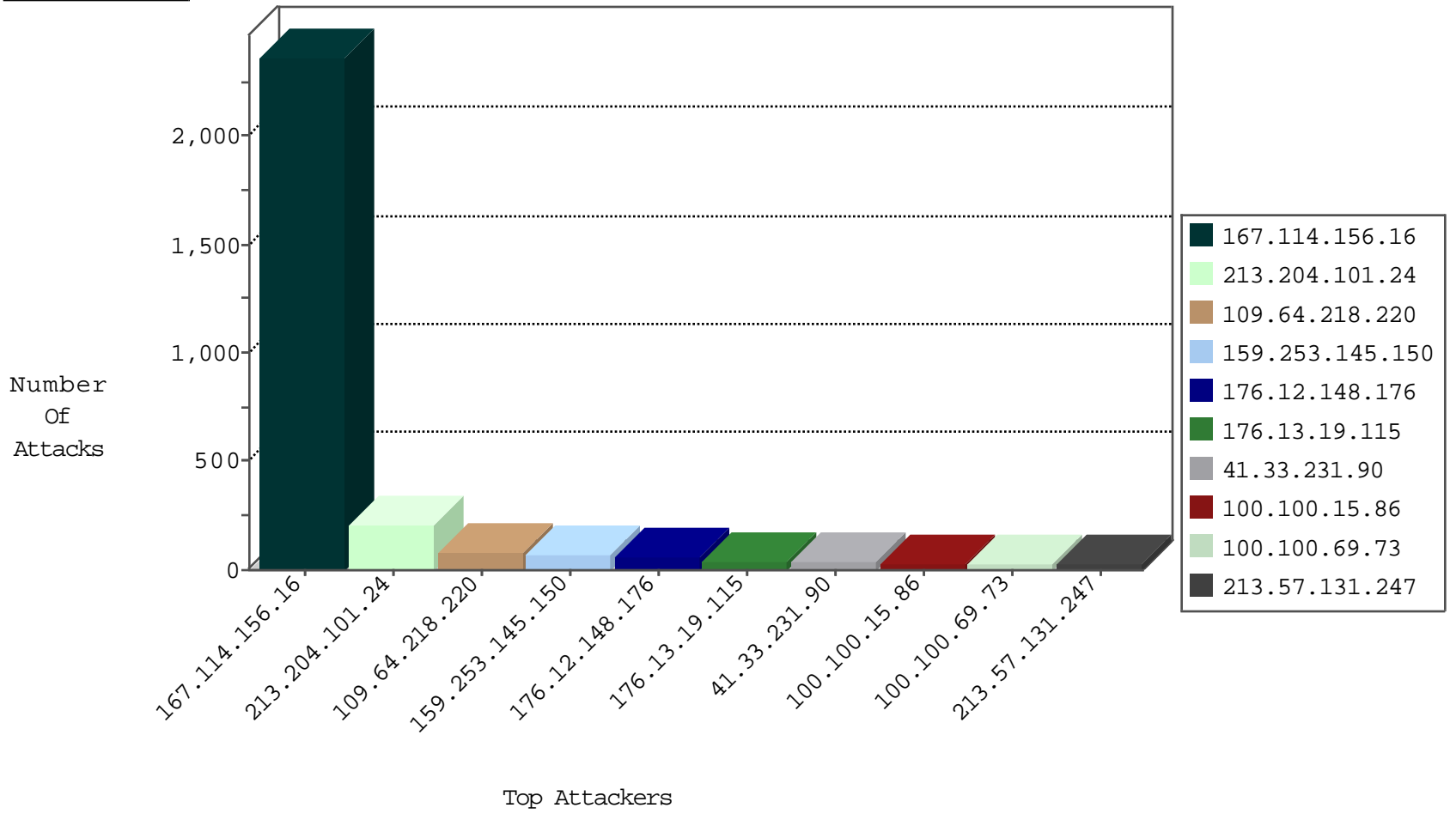
# IDF Under Attack Daily Report



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	3712
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	30
79.180.58.69	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.176.42.43	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
45.63.17.42		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
45.63.17.42		147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.77.233	atal.idf.il	C095: Suspicious Addresses MFA	Permit	38
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	4
37.48.65.47	Netherlands	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
136.243.73.82	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	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	4
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
74.208.221.217	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
194.50.116.59	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.122.238.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.18.73.1	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.182.17.13	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
31.6.71.154	147.237.77.243	Poland	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 3072	1
74.208.221.217	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
74.208.221.217	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
74.208.221.217	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
223.242.109.88	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.208.221.217	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
125.67.229.114	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.172.71.252	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.182.17.13	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
74.208.221.217	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
74.208.221.217	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
74.208.221.217	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	62
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
100.100.15.86		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
100.100.69.73		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.40.191		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.65.199.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
141.0.15.152	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
213.204.101.24	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
14.141.19.126	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
78.109.28.144	Ukraine	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.133.45.4	Papua New Guinea	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.133.45.2	Papua New Guinea	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.183.211.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
100.100.52.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
213.57.128.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
159.253.145.150	United States	147.237.77.233	atal.idf.il	drop		drop	12
100.100.72.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
100.100.45.4		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
41.77.138.90	Egypt	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.241.229.70	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	12
46.19.86.103	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.29.197.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
207.46.13.74	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
159.253.145.150	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	9
40.77.167.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.254.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
107.6.123.226	Singapore	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.177.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.145.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.147.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.2.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.177.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.147.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.48		147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
182.72.157.226	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.245.68	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.218.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
176.12.148.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
176.13.19.115	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	38
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
207.241.226.41	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	8
89.139.57.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.147.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	5
46.121.91.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.91.173	Block	4
93.172.187.243	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	3
2.52.169.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.120.132.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.22.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.54.47.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.99.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
93.172.71.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.2.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.0.102.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	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
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
149.78.22.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
109.67.186.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.51.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.29.197.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
198.103.104.11	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
176.13.1.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.29.182	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
41.45.126.171	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.112	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/imagevideogallerylobby/	Block	1
84.109.145.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
77.87.48.136	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.183.152.26	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
176.106.226.210	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
85.64.189.62	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.12.140.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
114.97.54.36	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1026-ar/idfg.aspx/trackback/	Block	1
79.181.66.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.57.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.161.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.91.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1232-he/refuah.aspx&sa=u&ved=0ahukewiopc2qy7djahxjobokhrwebvcqfggimaa&usq=afqjcneazqhko4kbponcau_zluafeow9hq	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
46.117.62.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
89.139.29.182	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
84.111.137.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1