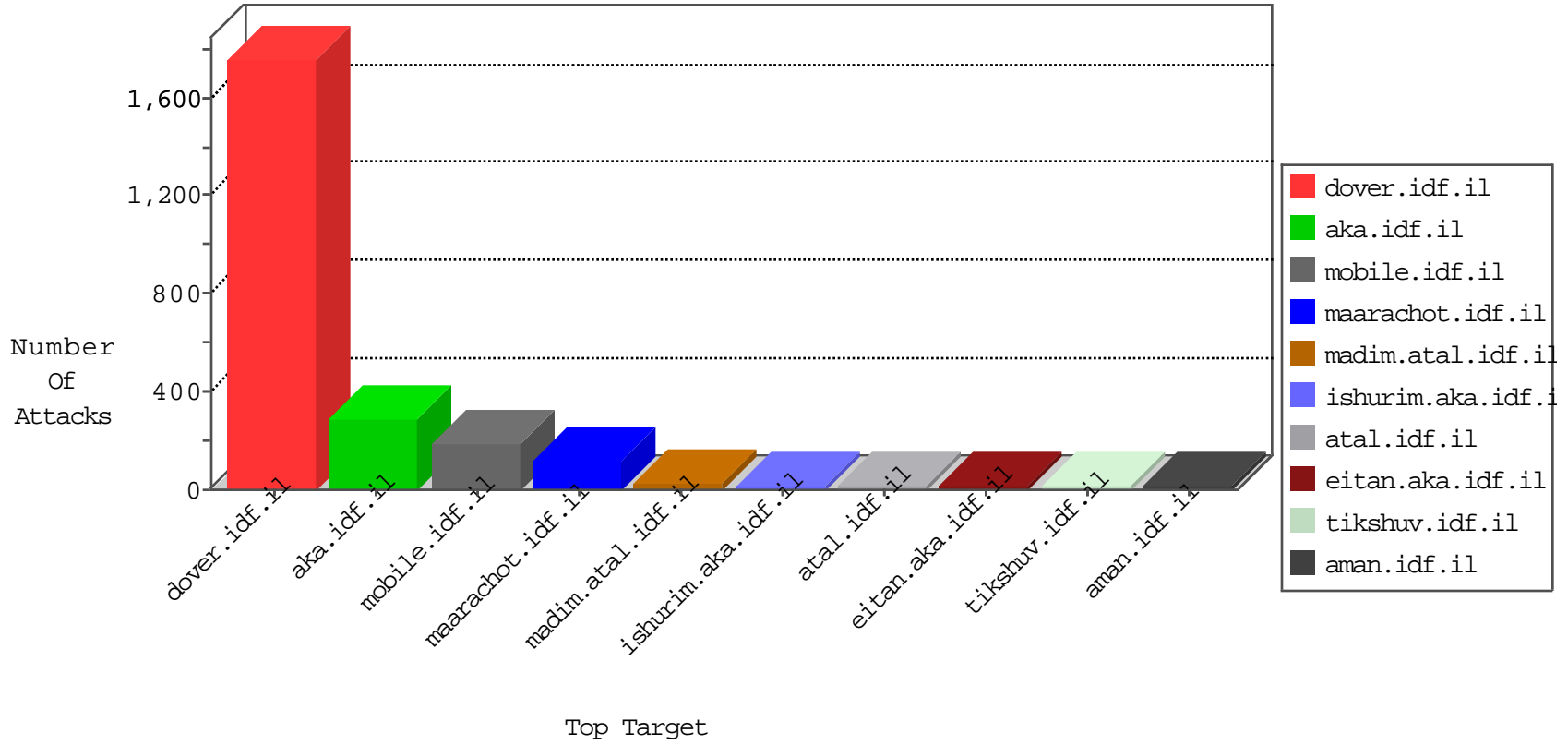


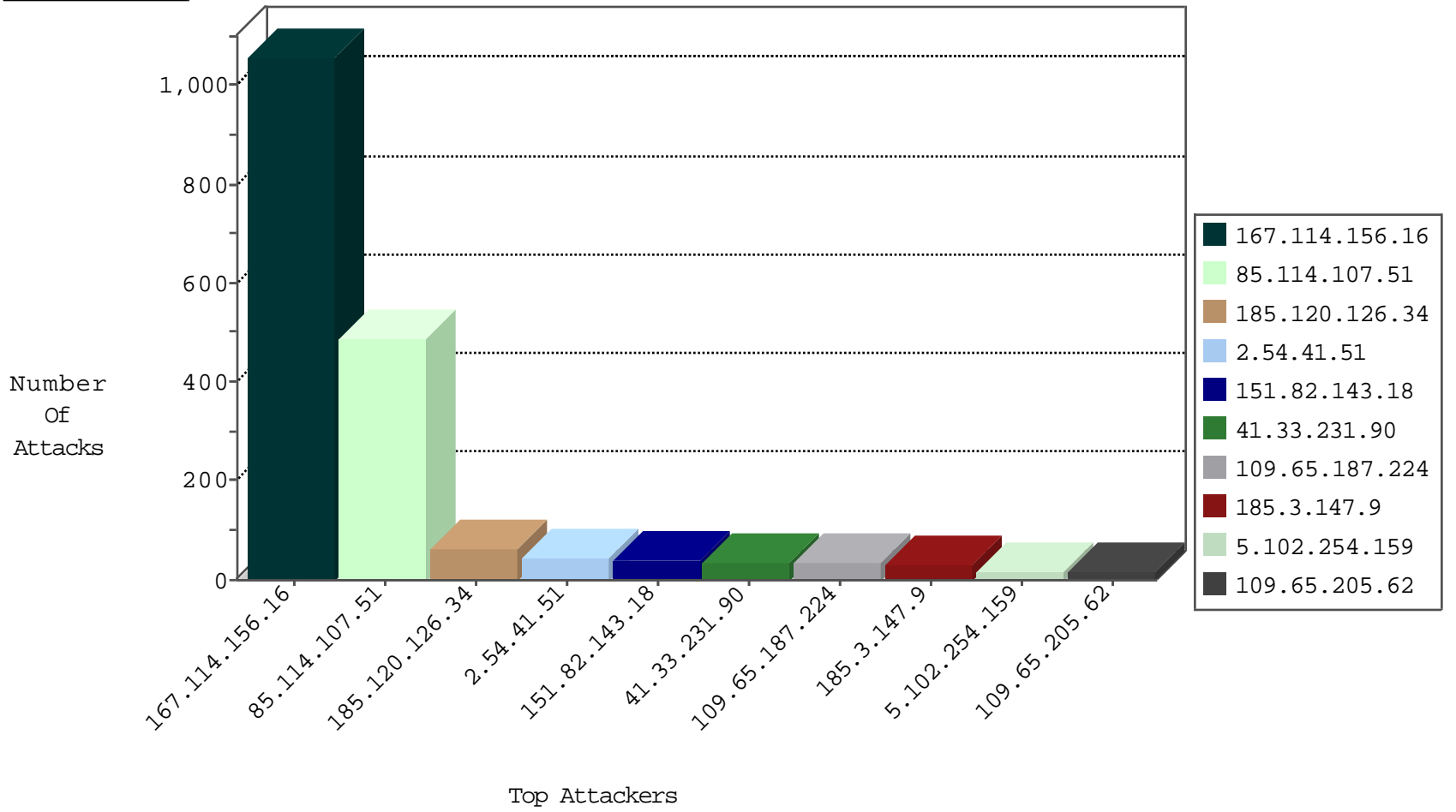
# IDF Under Attack Daily Report



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	3536
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	391
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
208.67.1.66	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.66	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
208.67.1.66	United States	147.237.76.198	e.yochalan.idf.il	Block_Udp_All_Nets	drop	1

01-01-2016-17:04:03 to 01-01-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	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
2.54.141.156	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.66.23	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
128.127.0.45	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -f -sS	1
190.249.184.162	147.237.77.243	Colombia	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
120.199.111.137	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.235	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
120.194.193.15	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.235	147.237.76.148		ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
120.194.193.15	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.235	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.72.156	France	aman.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.235	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
54.205.120.75	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.64.31.170	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
168.62.238.153	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
208.64.31.170	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.227.7	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
120.199.111.137	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
190.249.184.162	147.237.77.243	Colombia	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
120.194.193.15	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.235	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
120.194.193.15	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.235	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
85.114.107.51	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL Injection - Select From	1
185.130.5.235	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.161.252.88	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.64.31.170	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
12.139.41.189	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.114.107.51	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	84
185.120.126.34		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
151.82.143.18	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
185.3.147.9	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
109.65.187.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.65.205.62	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
5.102.254.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
109.64.108.40	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.67.42.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.32.179.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.10.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.230.157	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.185	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
151.82.143.18	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.127.91.85	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.22.130.139	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.125.4.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.168.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.174	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.228.51.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.143	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.129.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.5.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.217.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.213.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.0.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.69.16.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
67.55.90.132	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.46.39.21	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.129.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.13.131	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
5.29.0.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
31.154.7.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
77.125.102.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.148.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.26.43	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.41.51	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.41.51	Block	40
185.120.126.34		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	8
185.27.105.73	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
89.139.165.67	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	7
109.65.187.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.16.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.173.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
207.46.13.144	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.144	Block	3
157.55.39.137	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
176.13.15.221	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
2.54.36.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.106.176	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	2
109.253.159.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.22.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.191.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.64.194.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.131.167	Block	2
5.102.254.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.51.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.106.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	2
207.46.13.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.175.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.245	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.65.54	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.210.189.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.129.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.49.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.0.29	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.57.130.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.133.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.41.51	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
162.234.184.148	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.234	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/gyus/general.aspx	Block	1
109.64.140.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
84.94.90.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.227.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
176.228.51.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.211.67	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
141.212.122.160	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1