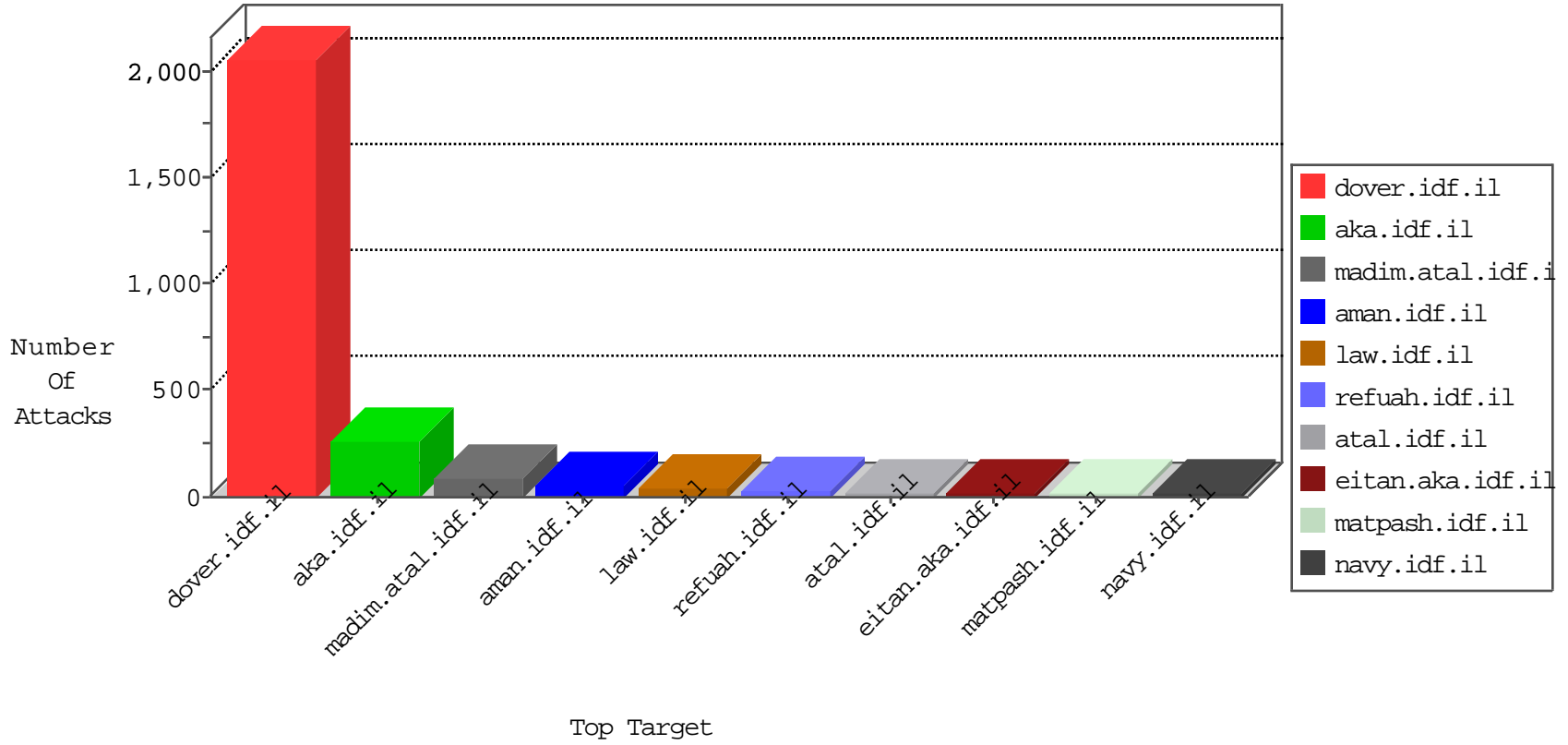


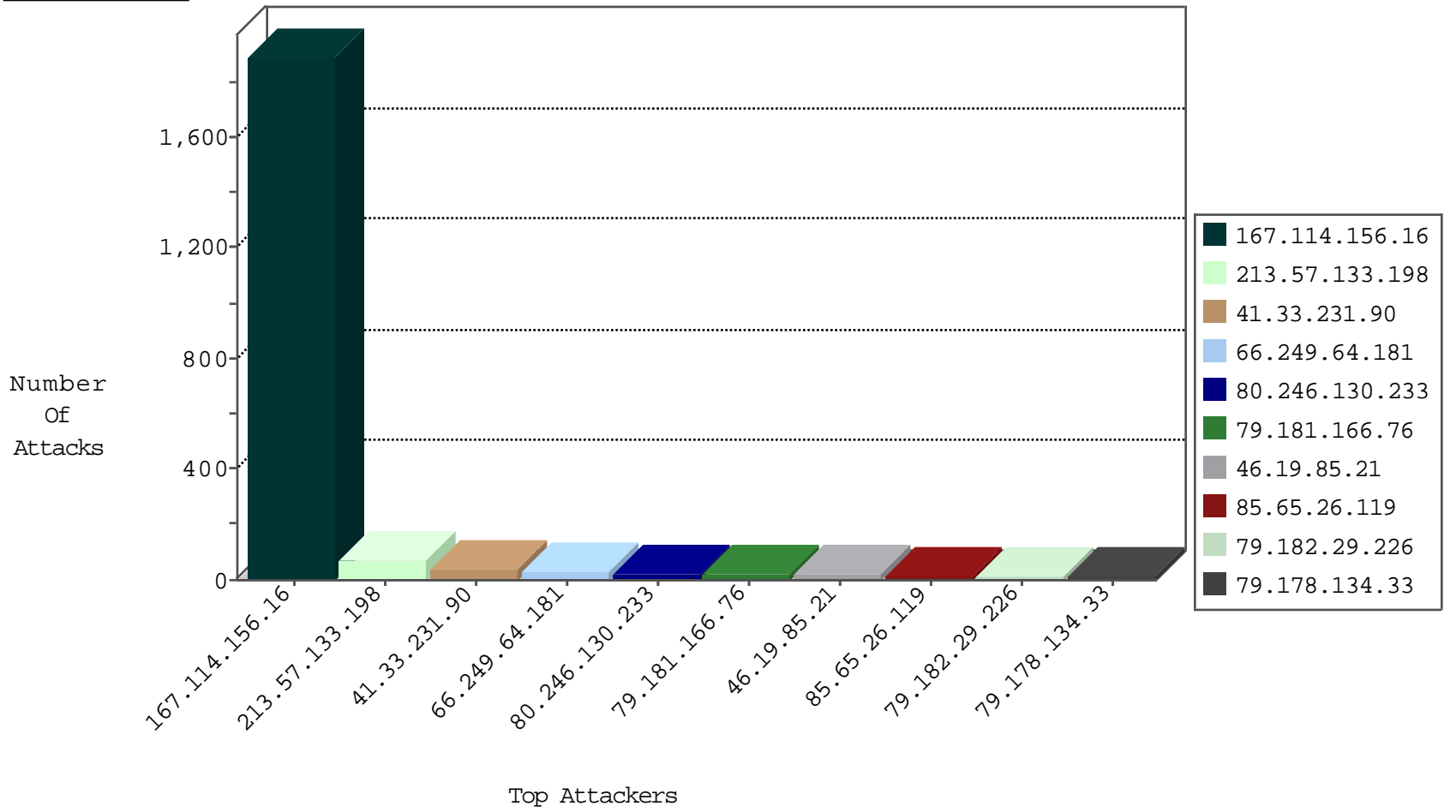
# IDF Under Attack Daily Report



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	3444
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1666
168.235.207.129	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
94.102.56.238	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.56.238	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.36.86	United Kingdom	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
158.69.214.109	United States	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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	20
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
199.19.105.111	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
80.246.130.62	147.237.76.31	Israel	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
190.213.109.118	147.237.77.176	Trinidad and Tobago	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.126.212.181	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
93.158.215.45	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.45	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.93.88.114	147.237.0.35	Germany	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.199.41.16	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.158.215.45	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.46	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.215.45	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.151.10.118	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
93.158.215.46	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
82.117.208.243	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.45	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.133.198	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
80.246.130.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
79.182.29.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.143.99	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.131.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.144.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.139.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.26.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.12.148.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.179.21.123	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
85.65.26.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.23		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.161.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.245.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.109.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.110.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.166.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.94.221.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.21	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.21	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.94.221.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.204.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.12.82	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.148.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
162.203.2.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.128.149	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.219.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.108.0.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.181.166.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
2.52.167.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.70.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.166.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.134.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.0.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.208.52.72	Austria	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.52.181.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.166.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.29.219.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.177.194.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.46.236	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.134.33	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.178.134.33	Block	13
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
162.203.2.233	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 162.203.2.233	Block	5
173.246.96.76	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.246.96.76	Block	5
31.154.157.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
176.12.148.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.228.28.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.117.18.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
109.226.21.133	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationsevice.aspx/getauthuser	Block	2
89.138.189.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.90.205	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx&sa=u&ved=0ahukewjmjv1_7mtjahxirhgkhy6rbf4qfggrmae&usg=afqjcnf_b016rnmjdjafppqlxngfli8du6w	Block	2
185.3.146.213	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
149.78.94.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
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	1
84.108.53.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/yohalan/main/main.asp	Block	1
173.252.122.122	United States	147.237.72.166	aka.idf.il	Unknown Parameter sandbox in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/shared/main_pict.jpg	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
109.201.154.167	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.205.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.162.250	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.52.181.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.179.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.178	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8832-he/refuah.aspx	Block	1
46.121.111.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
84.111.224.167	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18189-he/dover.aspx	Block	1
46.117.140.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.142.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.19.105.111	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.78.236	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
46.166.190.164	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.174.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
176.13.23.22	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
123.152.228.17	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
93.173.175.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1