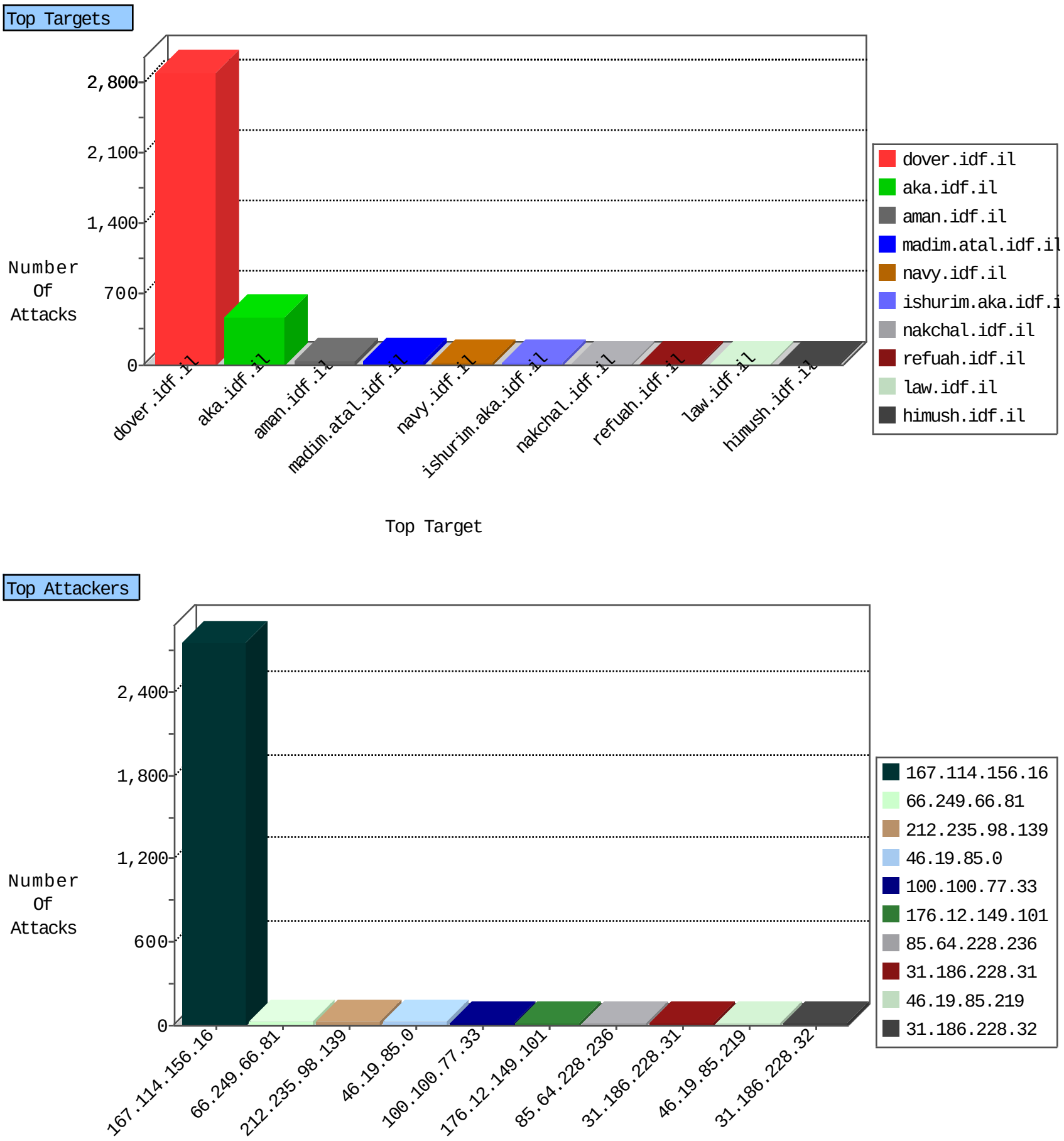
12-01-2015-07:04:04 to 12-01-2015-08:04:04

IDF Under Attack Daily Report



12-01-2015-07:04:04 to 12-01-2015-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	14205
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3615
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
93.174.93.151	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.169	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.169	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
93.158.203.169	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-07:04:04 to 12-01-2015-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-01-2015-07:04:04 to 12-01-2015-08:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.176.170.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.119.220.104	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
125.119.220.104	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.220.104	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.121.120.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.119.220.104	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
45.127.207.216	147.237.0.200		m4u.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.36	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
95.211.117.83	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1
173.160.184.241	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
85.130.130.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.160.184.241	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
2.52.172.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.27	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.220.104	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
77.125.128.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.119.220.104	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.220.104	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.130.145.216	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.220.104	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.119.220.104	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
45.127.207.216	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.37	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
113.160.150.62	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.0.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.134.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.160.184.241	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.93	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
171.232.56.152	147.237.77.216	Vietnam	dover.idf.il	ET SCAN Potential SSH Scan	1

12-01-2015-07:04:04 to 12-01-2015-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
82.166.53.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
31.186.228.32	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
31.186.228.59	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
216.223.27.58	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.54.186.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	9
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
82.80.168.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.181.192.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.75	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.56.188	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.219.198.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.186.228.30	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.65.52.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.52.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.129.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
100.100.87.29		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.132.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.159.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.60.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.101.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.11.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.0.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.125.161.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.17.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.149.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
85.64.228.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.228.236	Block	16
79.176.131.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	8
37.26.149.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	4
79.179.99.94	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
176.12.151.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
84.228.144.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.228.129.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
85.64.228.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
5.22.134.19	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.91	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1271-he/atal.aspx	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.66.31	Block	1
109.66.213.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.99.75	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
37.142.68.73	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
79.177.164.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
195.154.168.82	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.134.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/d	Block	1
79.183.18.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/ http:/www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
176.13.23.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
131.162.130.180	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
37.142.68.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
79.177.225.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	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
176.13.2.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.249	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/1133-22461-he/dover.aspx.	Block	1
79.183.163.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.159.71	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res ources/images/innerpage/goback.gif	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
157.55.39.108	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
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	1
79.178.143.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.173.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.12.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1