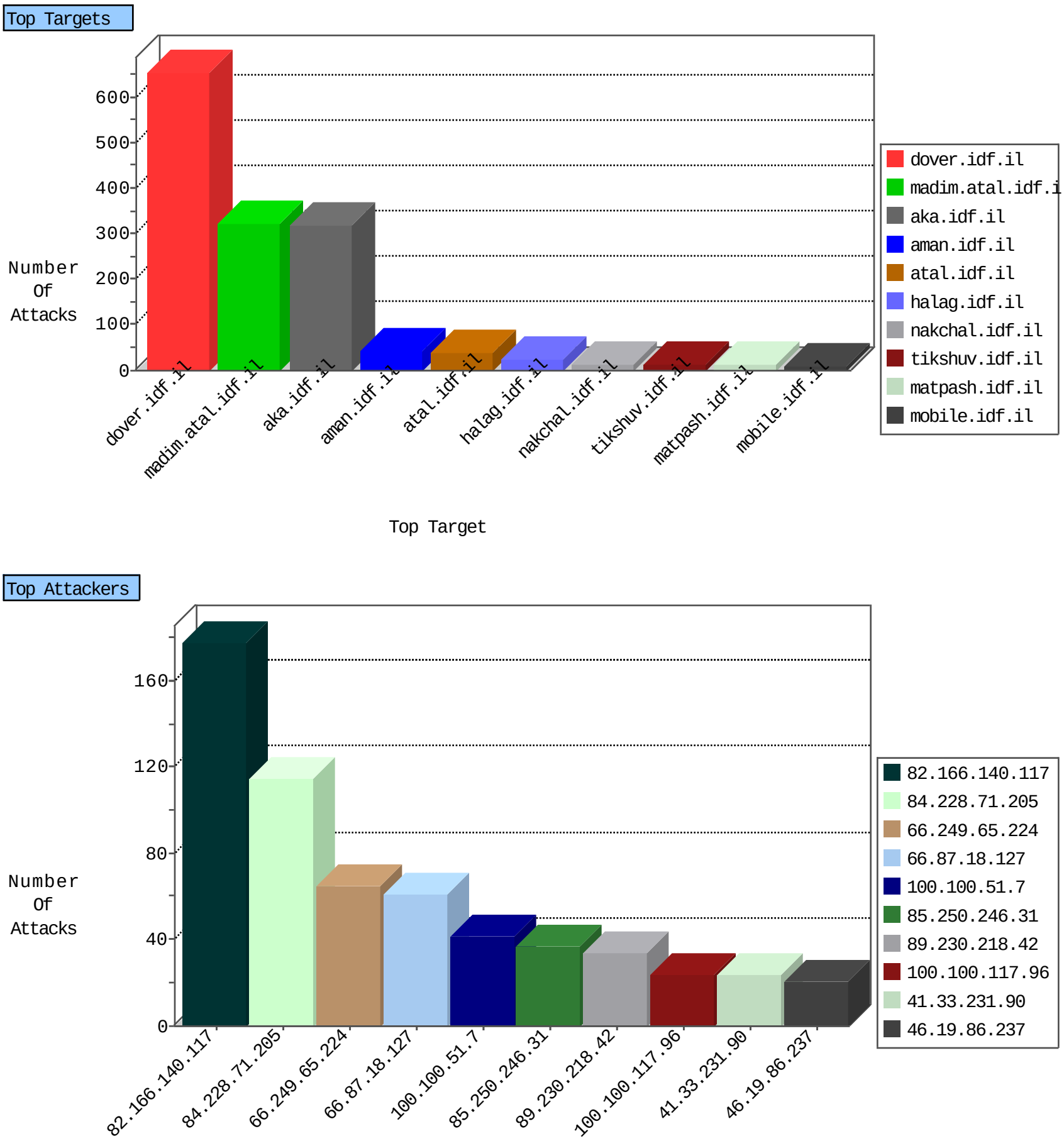
11-21-2015-13:04:00 to 11-21-2015-14:04:00

IDF Under Attack
Daily Report



11-21-2015-13:04:00 to 11-21-2015-14:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
87.68.45.205	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
100.100.85.150		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.178.37.168	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
80.246.136.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
80.246.136.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
157.55.39.229	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
80.246.139.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
85.64.181.229	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
104.192.0.226	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
199.188.205.42	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
85.65.93.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1

11-21-2015-13:04:00 to 11-21-2015-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.236.19.75	China	147.237.0.19	madim.atal.idf.i	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1

11-21-2015-13:04:00 to 11-21-2015-14:04:00

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	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
221.9.77.215	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.124.35.115	147.237.76.199	Nicaragua	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
178.62.126.13	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.108.21.16	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.90.155.19	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.124.35.115	147.237.76.199	Nicaragua	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
114.33.6.2	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.108.21.16	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1

11-21-2015-13:04:00 to 11-21-2015-14:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.18.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
100.100.51.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
89.230.218.42	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.117.96		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
119.173.226.201	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
100.100.122.50		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
100.100.68.243		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
37.26.146.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.108.111.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.77.70.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
151.80.41.176	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.65.21.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.85.150		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.3	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.123	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.250.246.31	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	8
183.79.221.34	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.250.246.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.67.165.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.246.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.137.33	Israel	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.148.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
183.79.221.34	Japan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.125.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.117.205.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.151.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
107.178.194.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.237	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.45.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.122.22		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.154.91.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.250.246.31	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.154.91.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.140.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
84.228.71.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
82.166.140.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
84.228.71.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
82.166.140.117	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 82.166.140.117	Block	6
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	5
149.78.135.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
87.69.107.145	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
109.160.147.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.107.145	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
176.13.20.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
87.68.241.137	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
109.65.19.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
85.250.243.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.3.146.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.165.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.137.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.132	Israel	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
80.246.137.117	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
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	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
221.231.6.246	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
188.225.177.134	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/8	Block	1
85.65.17.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.140.117	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
46.101.51.119	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
157.55.39.164	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
79.178.58.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.46.44.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
212.150.126.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.17.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1489-12652-he/dover.aspx	Block	1
46.19.85.132	Israel	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
149.78.135.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
80.246.137.117	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.1.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	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
50.116.28.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.207	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.180.0.58	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
41.143.110.168	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.201.154.197	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1