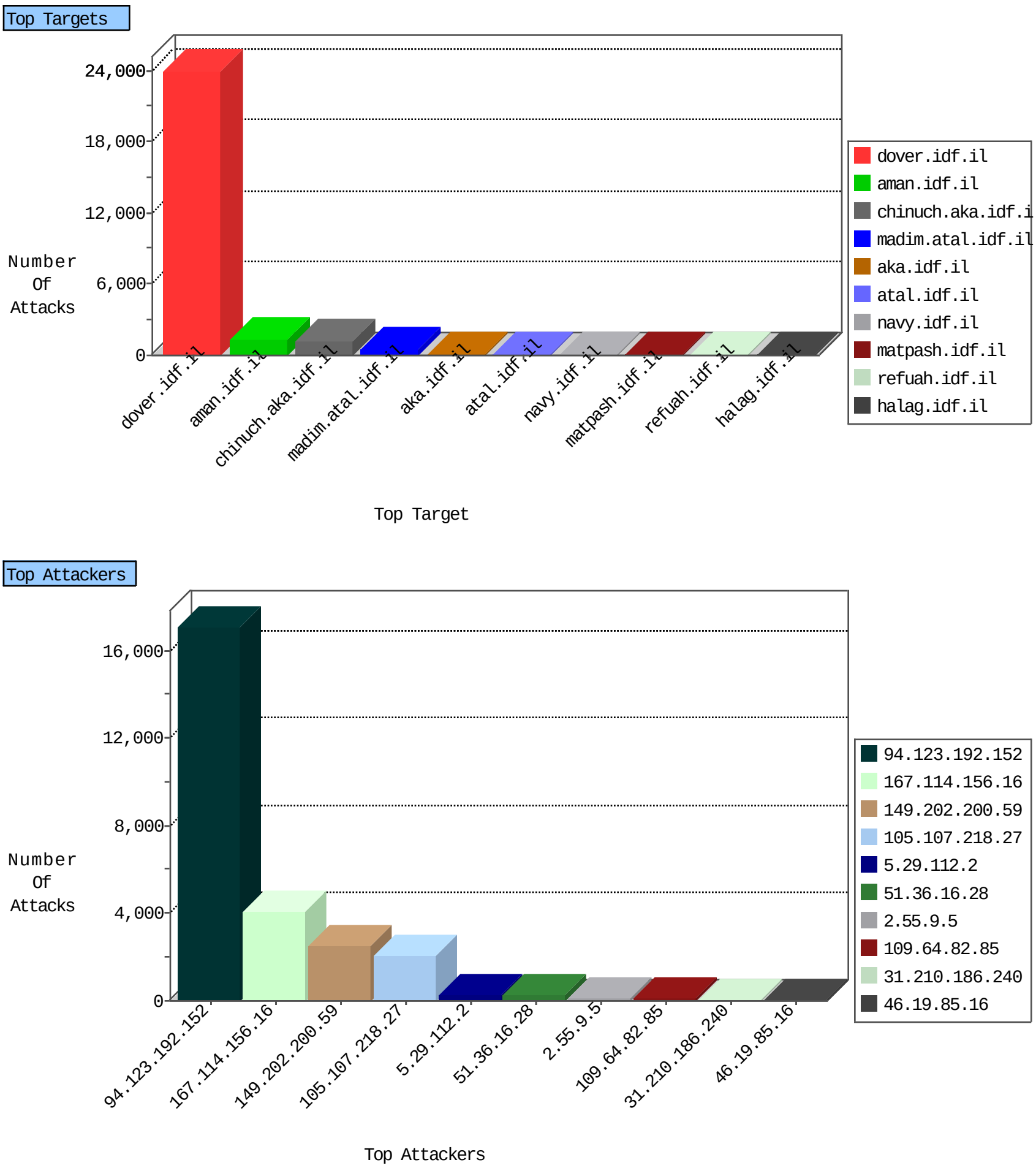
04-13-2016-23:04:04 to 04-14-2016-00:04:04

IDF Under Attack Daily Report



04-13-2016-23:04:04 to 04-14-2016-00:04:04

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	Block_Ip_Web_In	drop	4089
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	208
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	32
104.148.71.133	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	12
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	12
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.94.111.1	Russian Federation	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-13-2016-23:04:04 to 04-14-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.252.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-23:04:04 to 04-14-2016-00:04:04

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
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.177	Kazakstan	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
85.65.120.145	147.237.0.33	Israel	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.4.79.76	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
23.102.168.255	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.22.8.247	147.237.72.167	Portugal	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
88.204.187.90	147.237.76.177	Kazakstan	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
84.200.15.174	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
51.36.16.28	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
46.4.79.76	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
23.102.168.255	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
195.22.8.247	147.237.8.14	Portugal	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

04-13-2016-23:04:04 to 04-14-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2023
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1836
149.202.200.59	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1235
149.202.200.59	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1231
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	325
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	298
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	155
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	126
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	125
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
31.210.186.240	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
5.29.112.2	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
149.200.203.138	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
5.29.209.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	16
90.224.77.235	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
94.230.86.214	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.16	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.16	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.172.183.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.42	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	11
2.55.143.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.210.186.240	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.53.165.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
72.42.102.179	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	SYN Attack		reject	7
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.189	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.196.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.189	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.172.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.66.33.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
72.42.102.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	4727
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	4727
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	4727
5.29.112.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	212
2.55.9.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
109.64.82.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
5.29.112.2	Israel	147.237.0.19	madim.atal.idf.i	Automated Vulnerability Scanning V1	Block	46
8.37.230.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
5.28.166.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
131.253.25.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
149.78.172.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
209.140.44.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
213.151.35.212	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/resources/common/styles/aka.css	Block	1
157.55.39.58	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.178.177.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
50.62.137.87	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-content/plugins/complete-gallery-manager/frames/upload-images.php	Block	1
197.242.100.32	Nigeria	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/163-6958-en/patzar.aspx	Block	1
84.94.174.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cellcom	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
31.168.22.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.10.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
94.230.86.214	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.192.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
207.241.237.226	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/685.pdf,	Block	1
84.108.46.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/resources/common/topakamenu/styles/homepage.css	Block	1
40.77.167.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
176.13.20.185	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
104.148.71.133	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.proxy-listen.de/azenv.php	Block	1
2.53.36.53	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.53.36.53 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
79.179.50.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.66.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/120209.aspx	Block	1
75.111.88.75	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
46.121.232.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.120.126.56	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.36.53	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.181.195.175	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dov.	Block	1
75.111.88.75	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
50.62.137.87	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
197.242.100.32	Nigeria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
124.73.11.78	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-ar/idfg.aspx/trackback/	Block	1
2.53.59.62	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.182.138.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1