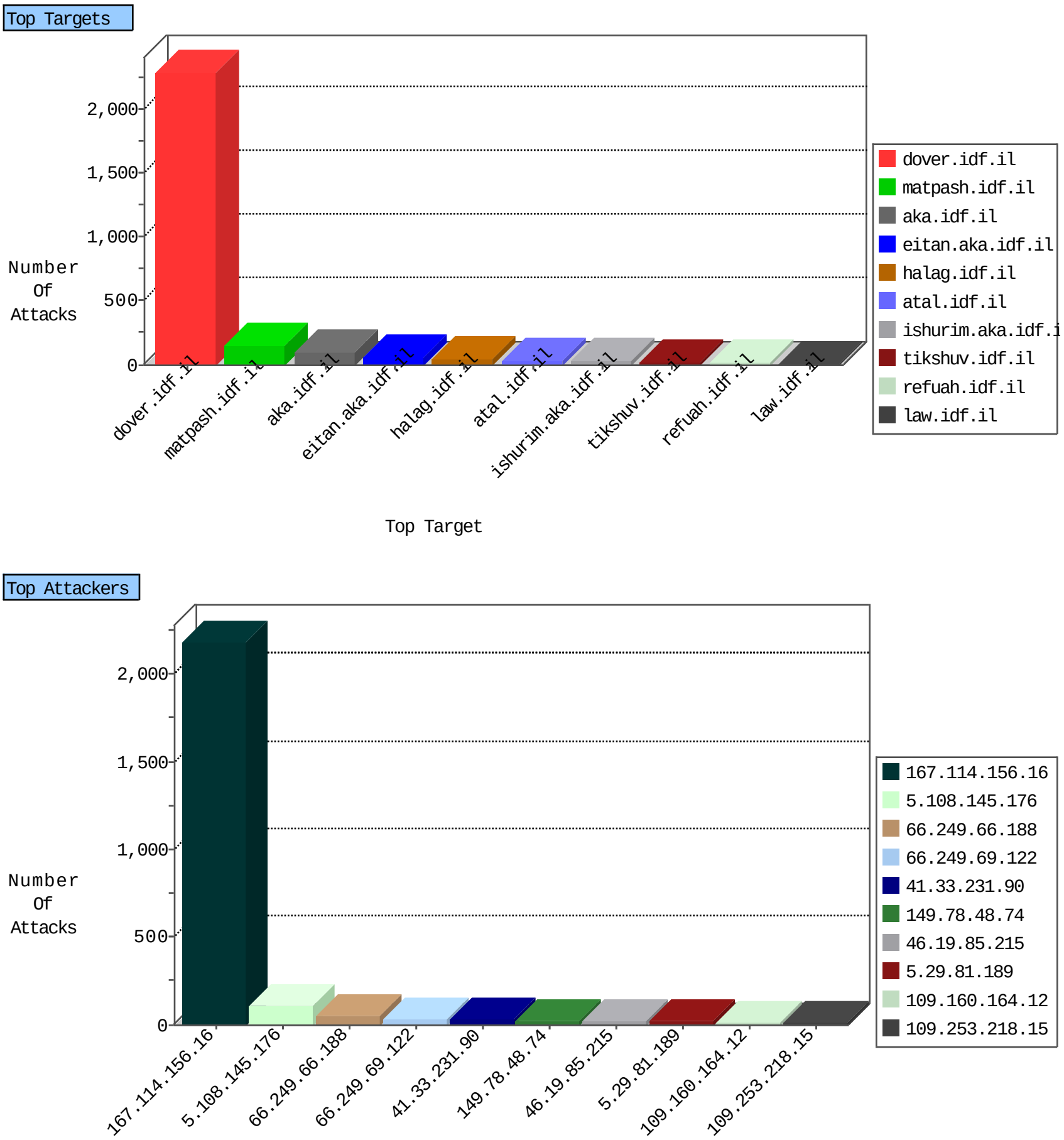
01-23-2016-01:04:09 to 01-23-2016-02:04:09

IDF Under Attack
Daily Report



01-23-2016-01:04:09 to 01-23-2016-02:04:09

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	3038
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
119.123.168.84	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
119.123.168.84	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
149.78.48.74	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

01-23-2016-01:04:09 to 01-23-2016-02:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

01-23-2016-01:04:09 to 01-23-2016-02:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.78.48.74	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
187.160.158.5	147.237.77.19	Mexico	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.139.133.222	147.237.8.27	Brazil	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.8.109.19	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
119.81.188.158	147.237.77.243	Hong Kong	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.15.202	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
210.23.18.244	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
187.160.158.5	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.72.109.162	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
173.167.243.19	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.167.118.67	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.15.202	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1

01-23-2016-01:04:09 to 01-23-2016-02:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.108.145.176	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	105
66.249.66.188	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.69.122	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
79.183.21.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.67.221.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.193.51.64	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
5.29.81.189	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
109.253.218.15	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.160.164.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.218.15	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.164.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.126.86.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.164.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.29.81.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
66.249.69.16	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.29.81.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.145.211.109	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.255.253.77	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.29.81.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.37.23	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
79.176.169.108	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.130.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.34.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.148	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
109.253.213.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
60.225.115.91	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.255.253.122	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
130.193.51.80	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
65.55.210.129	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.136.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
130.193.51.98	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.136	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.255.253.59	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.218.15	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
109.66.173.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.195.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.218.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.199.231.214	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.66.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/916-en/eitan.aspx	None	1
94.189.150.223		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/983-en/eitan.aspx	None	1
157.55.39.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
105.197.172.237	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.81.221	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in eitan.aka.idf.il/938-en/eitan.aspx	None	1
104.192.0.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/gadna	Block	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in eitan.aka.idf.il/938-en/eitan.aspx	None	1
46.19.85.214	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
157.55.39.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
105.197.172.237	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.109.113.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.62.53.168	Russian Federation	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /login	Block	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in eitan.aka.idf.il/938-en/eitan.aspx	None	1
104.194.26.204	United States	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	1
66.249.69.122	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-he	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
162.247.72.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.250.112.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.69.74	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1012-en/eitan.aspx	None	1
37.142.68.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
109.253.218.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
104.194.26.204	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
66.249.66.33	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
176.13.12.44	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
94.189.150.223		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.66.188	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1013-en/eitan.aspx	None	1
157.55.39.1	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
104.236.8.231		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/govermment/pages/tikshoret1.aspx	Block	1