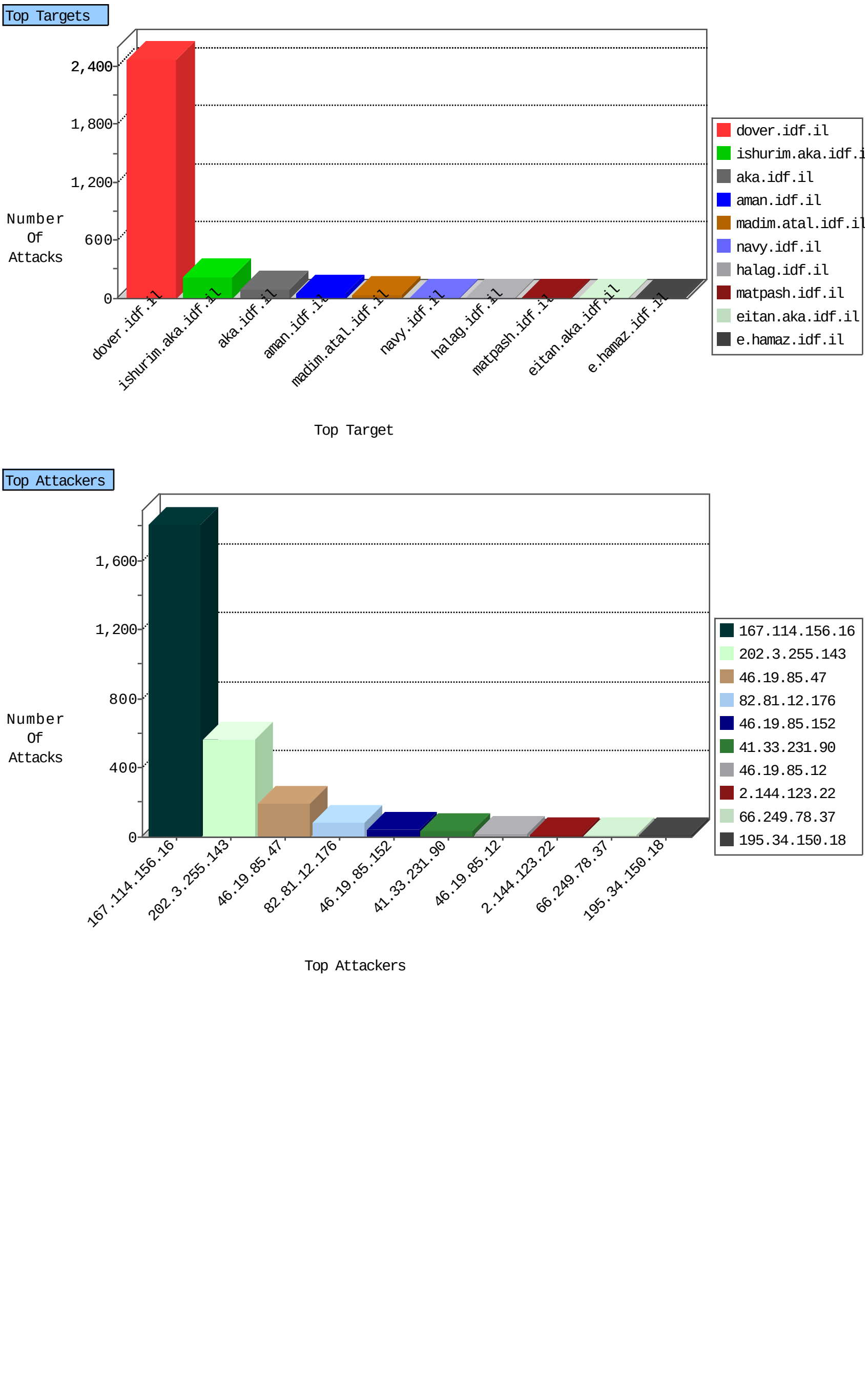
01-19-2016-05:04:02 to 01-19-2016-06:04:02

IDF Under Attack Daily Report



01-19-2016-05:04:02 to 01-19-2016-06:04:02

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	3003
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	80

01-19-2016-05:04:02 to 01-19-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	5
149.202.54.50	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-19-2016-05:04:02 to 01-19-2016-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	532
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
114.79.169.197	147.237.77.227	India	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
114.79.169.197	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.77.61	India	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
220.130.153.76	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.7	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
175.6.228.149	147.237.76.34	China	yohalan.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
114.79.169.197	147.237.77.243	India	mobile.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.77.212	India	e.dover.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.77.170	India	maarachot.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
162.13.88.58	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-19-2016-05:04:02 to 01-19-2016-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.47	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.12	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.144.123.22	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.12	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.144.123.22	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.185.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
157.55.2.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.33	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.2.168	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.52	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.37	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
60.179.60.253	China	147.237.72.166	aka.idf.il	Directory Traversal	directory traversal overflow	monitor	1
191.240.136.5	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
98.235.34.47	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.99	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.174	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
61.135.190.71	China	147.237.0.35	akaws.idf.il	drop		drop	1
191.240.136.5	Brazil	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.205.127.20	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
137.226.113.7	Germany	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.78.66	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.34	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.232	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.74.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
191.240.136.5	Brazil	147.237.76.202	e.halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.167	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
191.240.136.5	Brazil	147.237.76.198	e.yohalan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.79	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
191.240.136.5	Brazil	147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.42	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	41
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
14.1.194.250	Malaysia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
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	2
14.1.194.250	Malaysia	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
187.45.193.166	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
85.65.19.101	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.65.19.101 (sigalgs DoS Attack)	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
208.109.236.182	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
162.144.94.102	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.196.184.4	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
198.1.70.245	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
95.110.205.27	Italy	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
92.53.96.78	Russian Federation	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
192.99.98.54	Canada	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.44	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
213.136.76.107	Germany	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
179.188.17.23	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	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
37.122.211.142	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	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
2.54.27.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.111.139.216	Germany	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
94.23.59.136	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
187.45.195.183	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
85.65.19.101	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
162.144.94.102	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
198.1.70.245	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
95.211.0.114	Netherlands	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
92.53.96.78	Russian Federation	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
192.99.98.54	Canada	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
179.188.17.23	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
72.167.190.179	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
213.136.76.107	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.150.195.212	Sweden	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
195.67.74.166	Sweden	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
94.23.59.136	France	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
190.95.243.229	Ecuador	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
85.65.236.192	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
212.48.81.89	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
162.144.222.195	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
95.211.0.114	Netherlands	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
198.1.94.193	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
94.23.6.148	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
192.169.202.14	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
185.26.122.4	Russian Federation	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
79.96.139.9	Poland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1