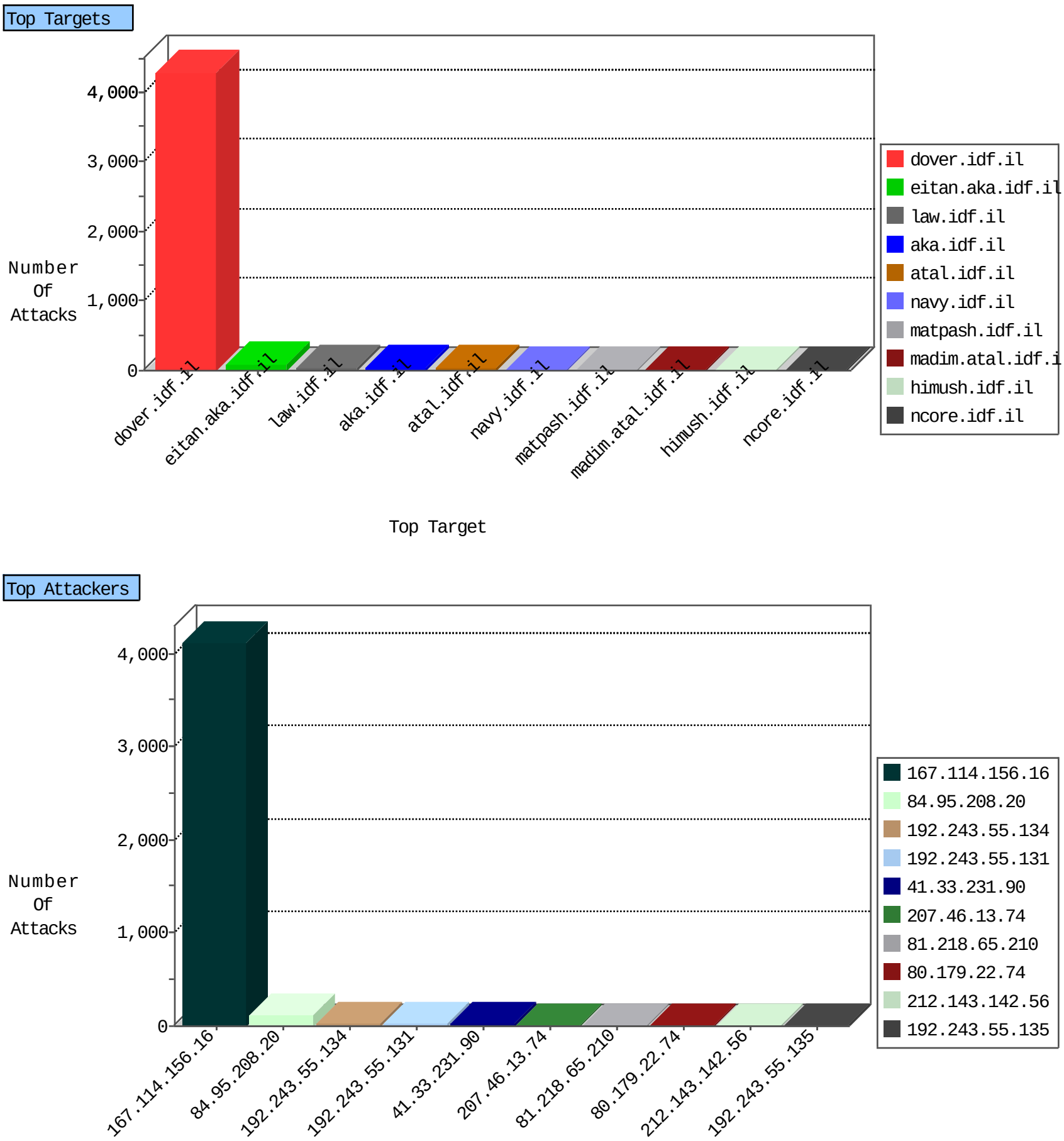
04-12-2016-04:04:08 to 04-12-2016-05:04:08

IDF Under Attack Daily Report



04-12-2016-04:04:08 to 04-12-2016-05:04:08

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	4125
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
120.132.50.135	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	4
209.126.110.5	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
103.44.205.54	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1
43.225.239.22	China	147.237.77.61	e.cogat.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
209.126.110.5	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
103.44.205.54	China	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.168.1.15		147.237.76.177	ncore.idf.il	Invalid L4 Header Length	drop	1
216.218.206.91	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
207.243.129.34	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.237.162	Germany	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1

04-12-2016-04:04:08 to 04-12-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
213.239.205.207	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-04:04:08 to 04-12-2016-05:04:08

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
107.158.255.194	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
89.36.214.115	147.237.77.74	Romania	law.idf.il	ET SCAN Potential SSH Scan	1
13.92.246.145	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
201.164.217.90	147.237.72.14	Mexico	dover.idf.il(old	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.158.255.194	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
89.36.214.115	147.237.77.178	Romania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.36.214.115	147.237.76.31	Romania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
13.92.246.145	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2016-04:04:08 to 04-12-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.74	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	11
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.179.22.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.37.101.13	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.179.22.74	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.44.192.63	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.131.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.8.142.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.24.206.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
209.140.33.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.208	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.249.69.18	Israel	147.237.0.33	idf.il	drop		drop	1
208.100.26.228	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.218	United States	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.148.71.133	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.196.135.21	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.46.13.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

04-12-2016-04:04:08 to 04-12-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	26
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	5
65.55.210.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
65.55.210.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.17	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.199	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
23.81.69.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
198.58.103.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	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
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
131.253.25.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1

04-12-2016-04:04:08 to 04-12-2016-05:04:08