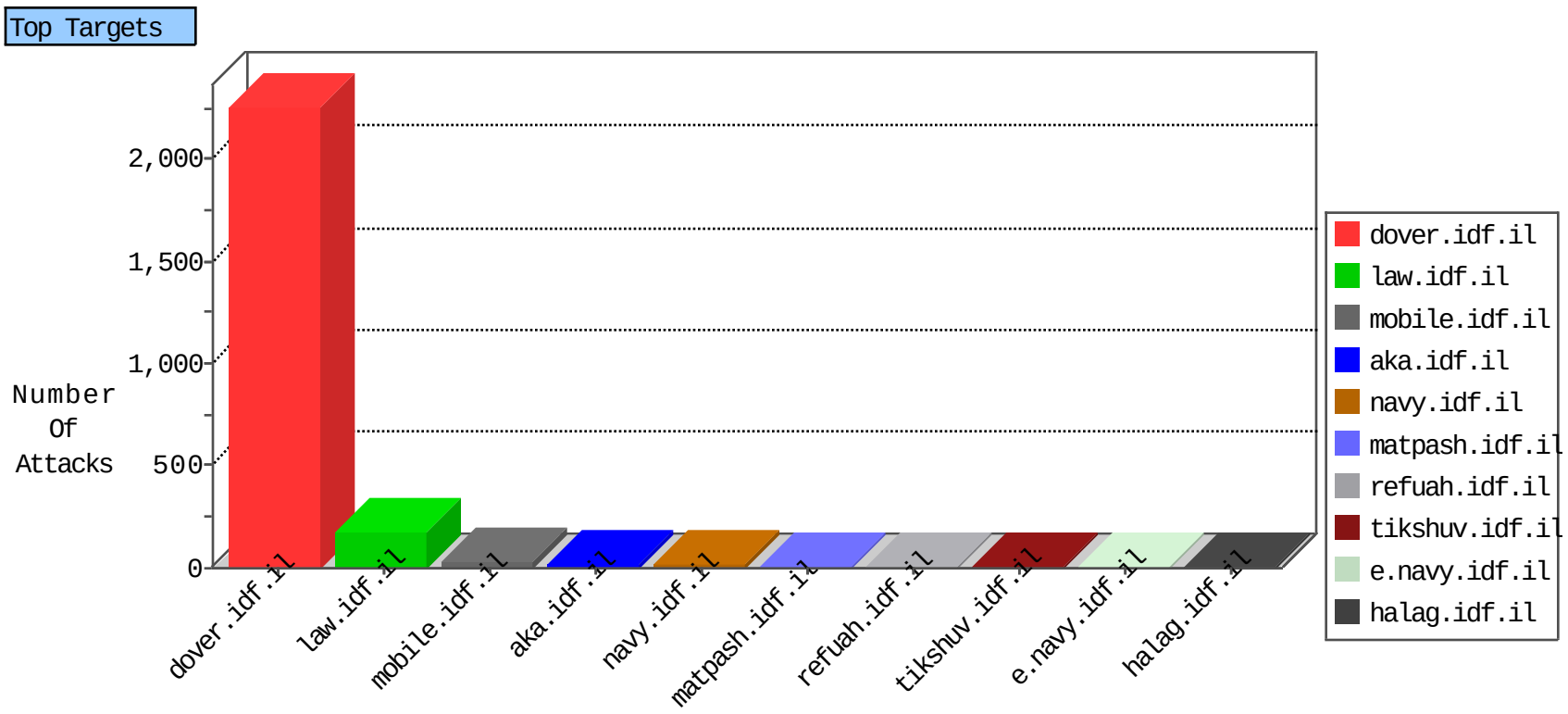
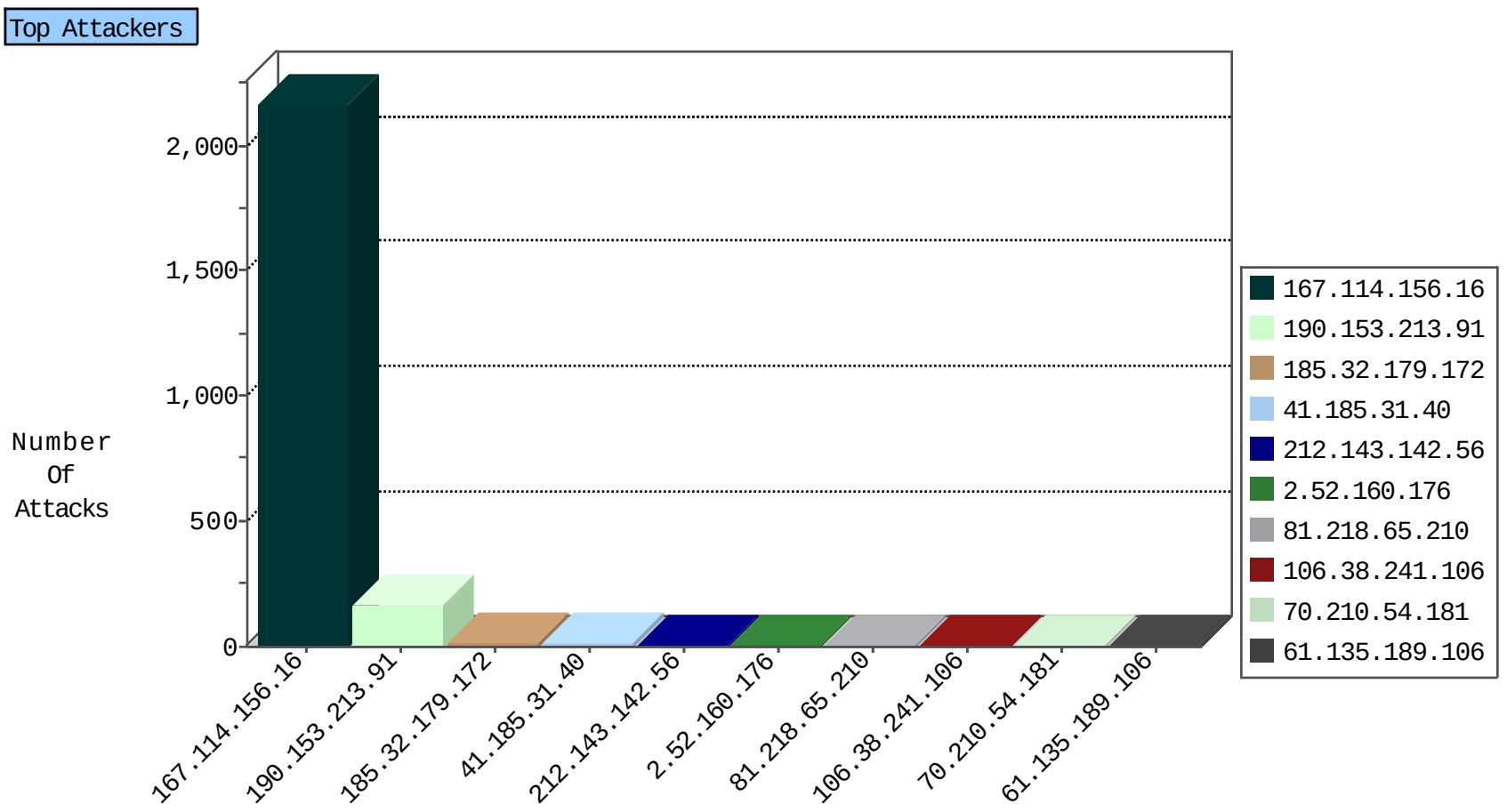
03-15-2016-03:04:08 to 03-15-2016-04:04:08

IDF Under Attack Daily Report





03-15-2016-03:04:08 to 03-15-2016-04:04:08

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	DOS-Tool-SwitchbladG	dest-reset	3269
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

03-15-2016-03:04:08 to 03-15-2016-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-15-2016-03:04:08 to 03-15-2016-04:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.153.213.91	147.237.77.74	Chile	law.idf.il	Tehila - Perl LWP with fake user agent	47
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
45.63.0.76	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.198.210	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.194	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
89.216.119.94	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -f -sS	1
89.163.145.38	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
209.162.248.93	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.11	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.95.73	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
89.163.145.38	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1

03-15-2016-03:04:08 to 03-15-2016-04:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
185.32.179.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.160.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.210.54.181	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
72.219.231.127	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.65.133	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.64.19.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.250.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.50.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.197.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.230.43	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
219.92.106.130	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.236.225.168		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.253.26.225	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.64.96.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
190.148.78.29	Guatemala	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.135.189.106	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.226.95.66	China	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
139.162.146.165	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.204	United States	147.237.0.33	idf.il	drop		drop	1
38.229.1.15	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.214	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.26.252	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.90.244.226	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
190.148.78.29	Guatemala	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
62.194.127.23	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
139.162.146.165	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
120.132.68.87	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.94	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.251	United States	147.237.0.33	idf.il	drop		drop	1
45.63.0.76		147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.215	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.36.202	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.90.245.74	United Kingdom	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.52.172.34	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
139.162.222.24	Netherlands	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.38	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.106	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.52	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.147.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.63.0.76		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
139.162.143.192	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
85.90.245.74	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.98	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.211	United States	147.237.72.167	ishurim.aka.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
190.153.213.91	Chile	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	48
190.153.213.91	Chile	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 190.153.213.91	Block	46
190.153.213.91	Chile	147.237.77.74	law.idf.il	Multiple Admin Blocking from 190.153.213.91	Block	23
5.107.9.189	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	3
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
190.153.213.91	Chile	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/administrator/components/com_civicrm/civicrm/packages/openflashchart/php-ofc-library/ofc_upload_image.php	Block	2
173.254.236.52	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
109.64.80.202	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
213.57.224.195	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.117	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
173.254.236.52	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
109.64.80.202	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
68.180.229.124	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
199.30.24.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.148.155	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
85.250.68.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
173.247.228.10	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
109.64.80.202	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
52.87.206.37	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
190.153.213.91	Chile	147.237.77.74	law.idf.il	Admin Blocking	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
197.52.172.34	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
173.247.228.10	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
109.64.80.202	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
213.57.224.195	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
52.87.206.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	1
157.55.12.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
197.52.172.34	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1