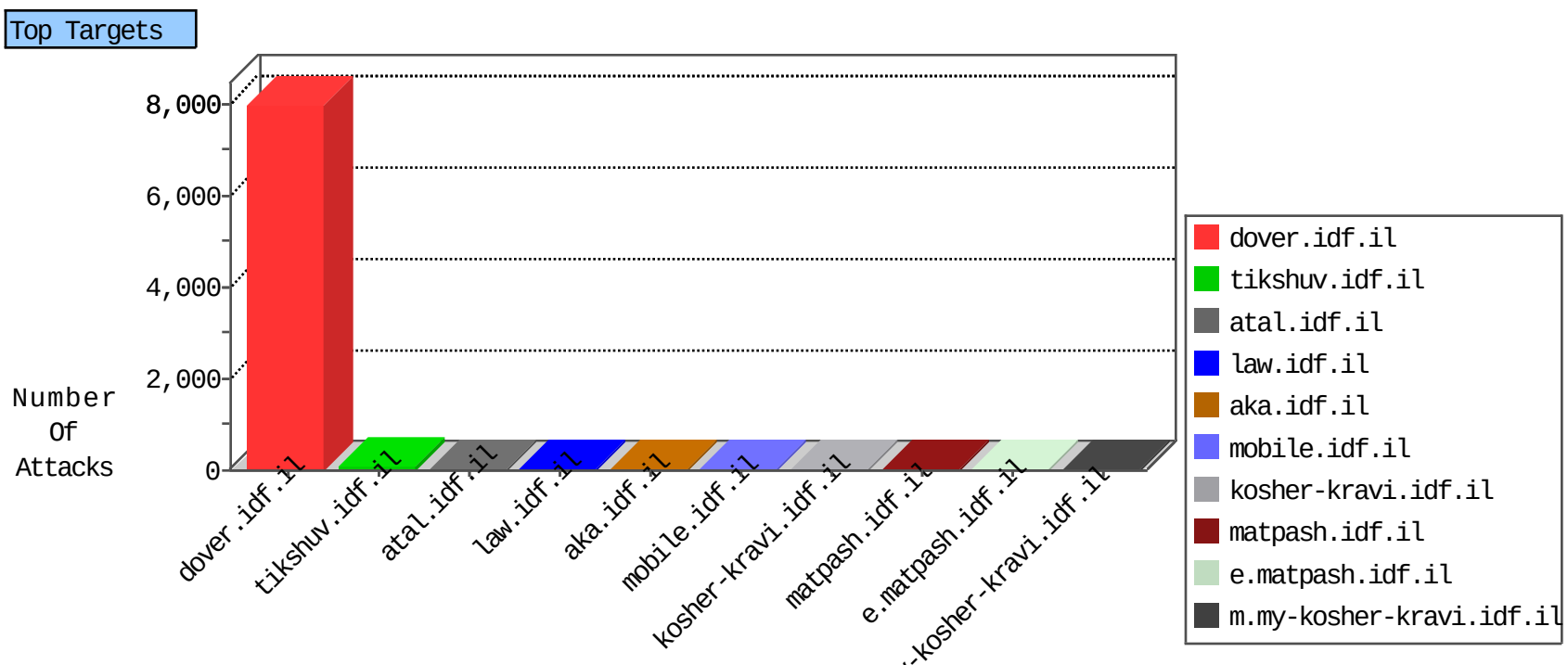
01-17-2016-04:04:08 to 01-17-2016-05:04:08

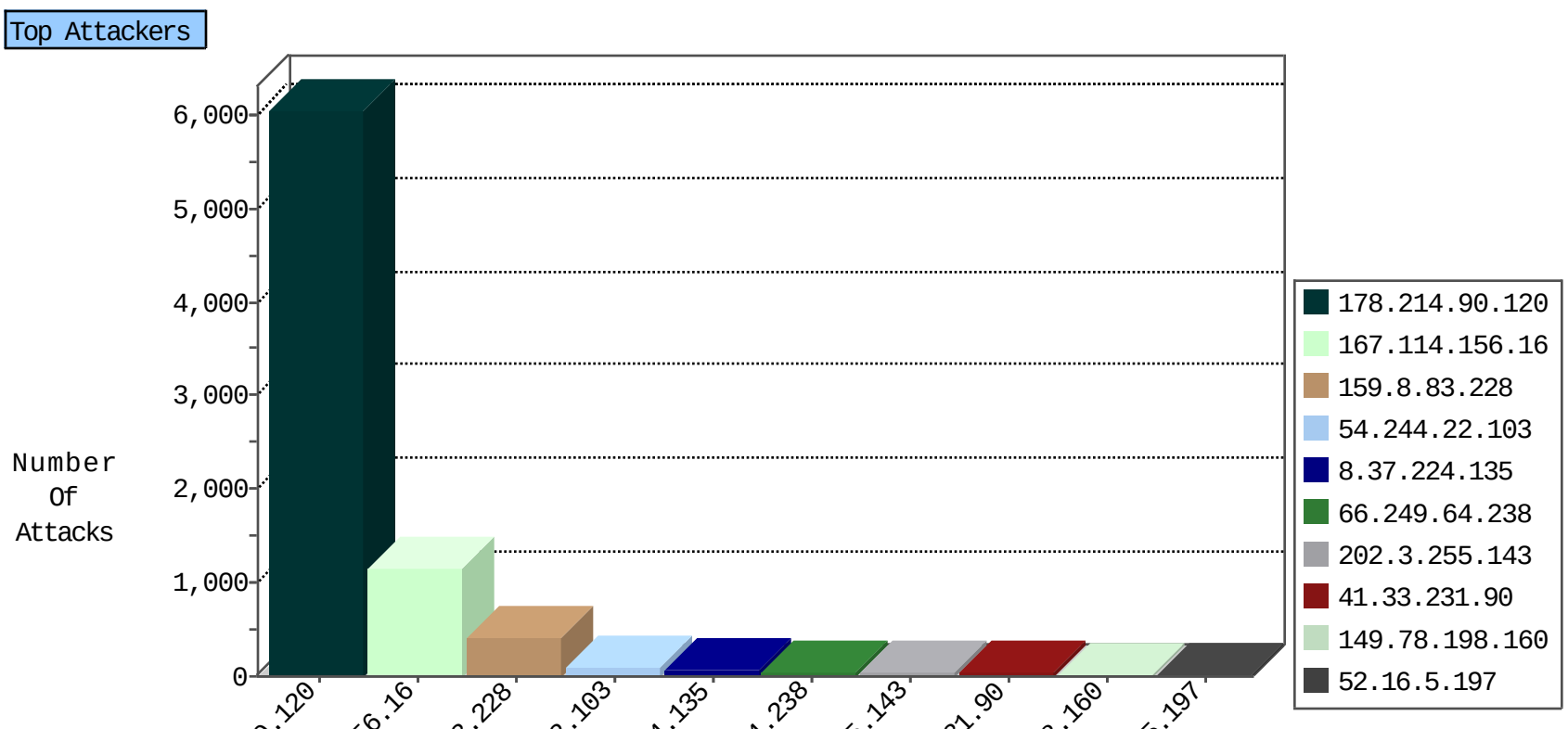
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-17-2016-04:04:08 to 01-17-2016-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.214.90.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6585
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3377
0.0.0.0		147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	740
8.37.224.135	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	55
66.249.64.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
178.214.90.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
66.249.89.119	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
83.137.1.200	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
91.108.167.53	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
107.178.194.79	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.70.77	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
104.131.240.186	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
178.255.215.87	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
178.214.90.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
207.46.13.147	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
157.55.39.171	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
199.30.24.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
178.255.215.87	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
96.56.10.27	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
8.37.224.135	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
157.55.39.155	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
162.248.100.195	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
91.108.167.53	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
199.30.24.112	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
157.55.2.177	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
207.46.13.147	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
157.55.2.177	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
162.248.100.195	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
183.20.216.73	China	147.237.76.196	e.sviva.idf.i	Block_Udp_All_Nets	drop	1

01-17-2016-04:04:08 to 01-17-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
98.19.222.133	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-17-2016-04:04:08 to 01-17-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
159.203.103.36	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

01-17-2016-04:04:08 to 01-17-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.214.90.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5529
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	348
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	90
178.214.90.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
8.37.224.135	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
149.78.198.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
149.78.198.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
24.47.130.40	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
96.56.10.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.174.17.171	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
72.9.148.10	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
66.249.64.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	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
66.249.64.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.155	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.56		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.171	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
207.46.13.58	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.147	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
91.108.167.53	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.255.215.87	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
8.37.224.135	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.112	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
45.35.64.142		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.38	United States	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.96	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.89.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.2.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
54.244.22.103	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1

01-17-2016-04:04:08 to 01-17-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.8.83.228	Netherlands	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning	Block	18
184.168.200.165	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.62.161.53	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
184.168.200.49	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 66.249.78.80	None	1
37.48.80.101	Netherlands	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
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.120	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/sip_storage/files/8/69778.xls/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
207.46.13.36	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
184.168.200.129	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
40.77.167.18	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.18	Block	1
198.51.75.165	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/logo.jpg	Block	1
217.69.136.208	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/	Block	1
184.168.200.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
40.77.167.25	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	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
159.203.103.36	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
184.168.200.165	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	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
50.62.161.53	United States	147.237.77.74	law.idf.il	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/1133-22638-he/dover.aspx.	Block	1
184.168.200.49	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1

01-17-2016-04:04:08 to 01-17-2016-05:04:08