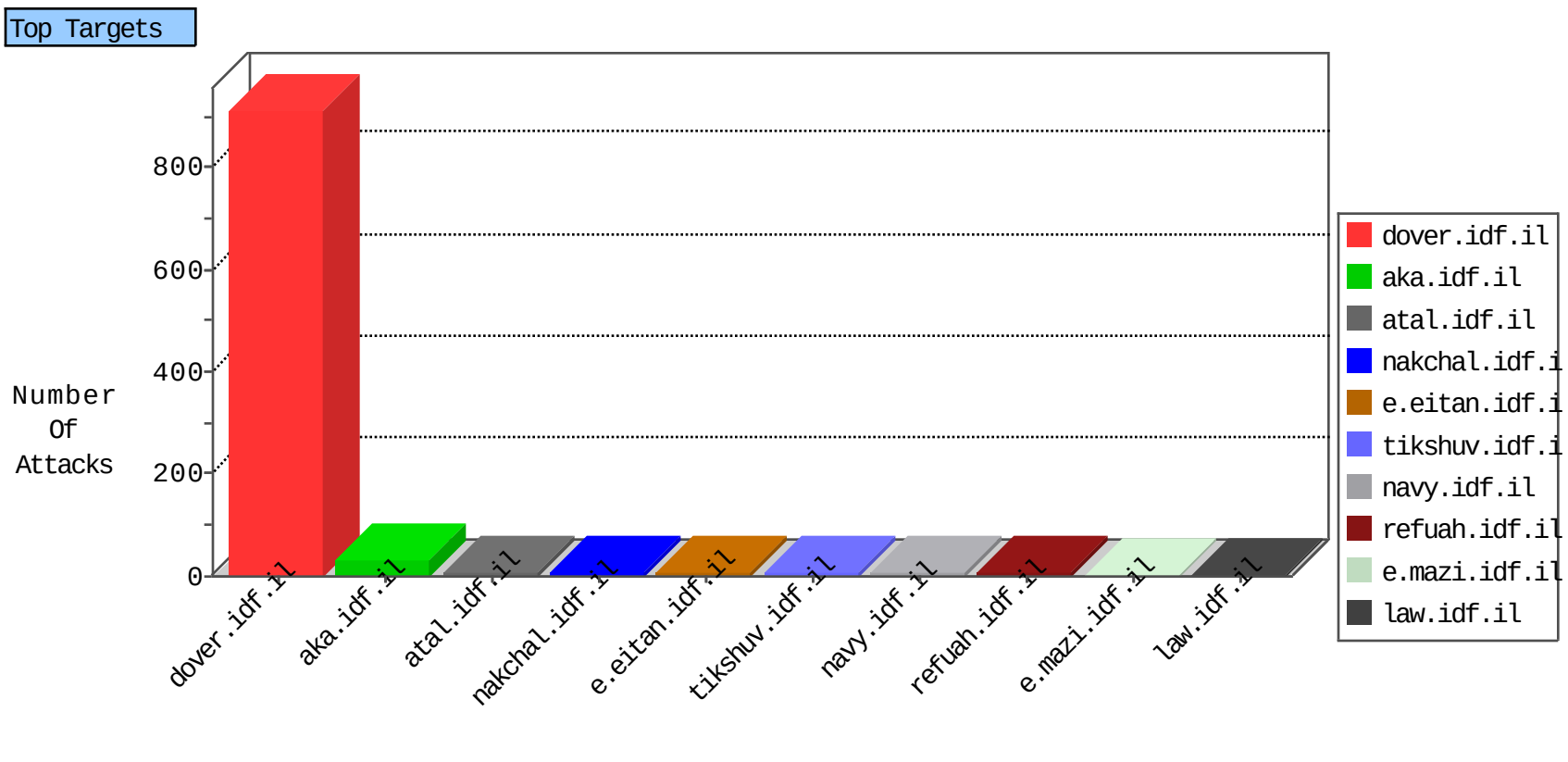
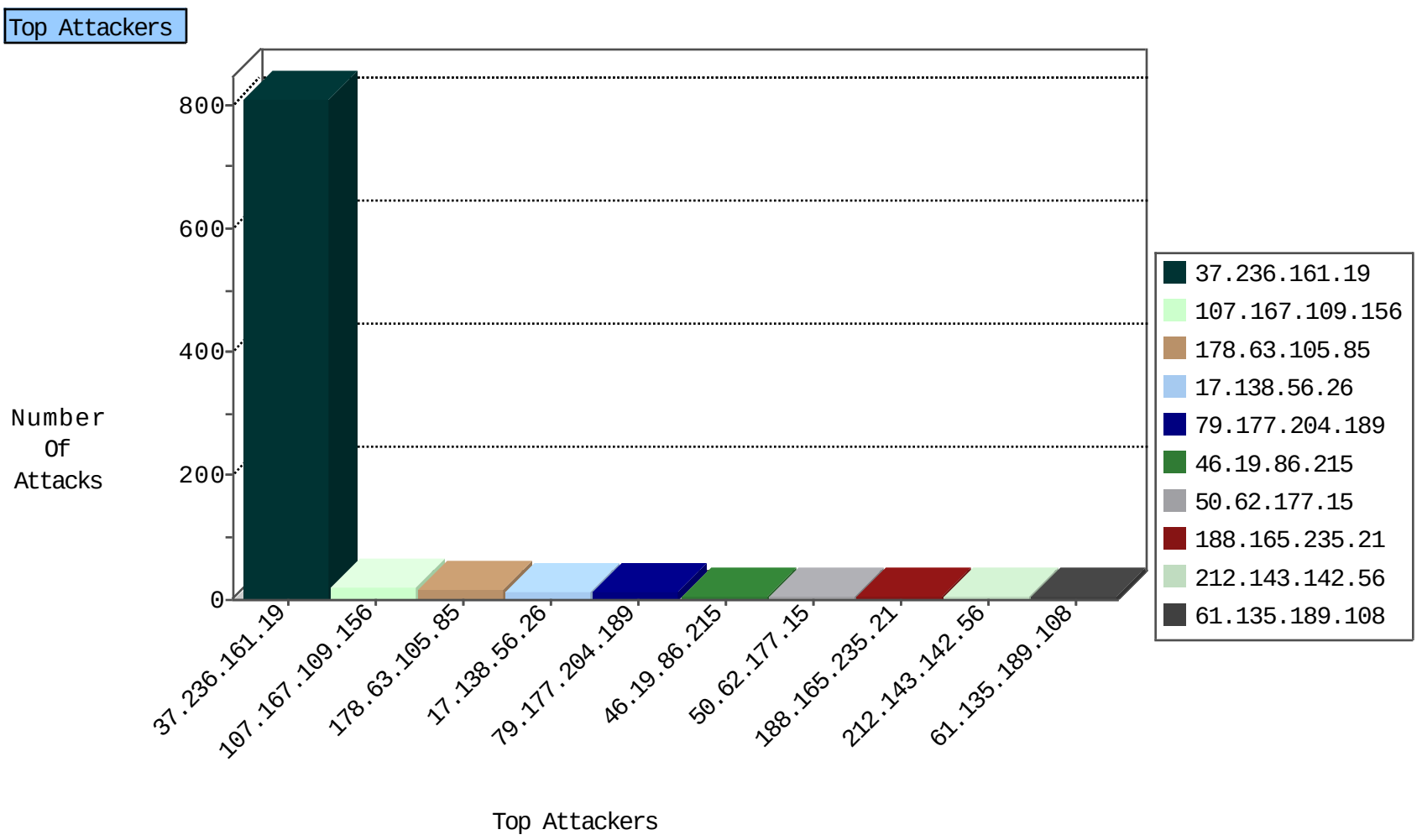
03-07-2016-02:04:03 to 03-07-2016-03:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-07-2016-02:04:03 to 03-07-2016-03:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	798
188.165.235.21	France	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.77.216	dover.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
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
223.146.114.114	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
4.15.125.104	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
223.146.114.114	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-02:04:03 to 03-07-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
199.30.24.231	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.207.27	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.241	France	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-02:04:03 to 03-07-2016-03:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.108.132.58	147.237.76.44	China	e.refuah.idf.i	ET SCAN NMAP -sS window 1024	1
89.163.145.38	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
82.166.184.187	147.237.77.61	Israel	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
5.97.104.158	147.237.76.30	Italy	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.145.38	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-02:04:03 to 03-07-2016-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.109.156	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
79.177.204.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.126.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.53.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	3
2.54.2.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
2.54.3.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.189.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
61.135.189.108	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
91.200.12.143	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.32.182.189		147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.134	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.174	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
129.12.214.94	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.164	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.175	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
136.0.98.17	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.178.11.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.241.237.224	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.165	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
74.71.87.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.32.182.189		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.178.150.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.169	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.32.182.189		147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.117	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1

03-07-2016-02:04:03 to 03-07-2016-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	10
50.62.177.15	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.62.177.15	Block	5
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.236.161.19	Block	2
17.138.56.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.29	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
219.74.36.175	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
112.209.149.103	Philippines	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
46.107.246.96	Hungary	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.24.76.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
77.224.7.171	Spain	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal URL Path Encoding www.law.idf.il/templates/getfile/getfile.aspx?filenamem	Block	1
220.255.148.65	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.237.51.59	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
117.78.13.54	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/894-he	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.255.253.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.224.7.171	Spain	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
41.237.51.59	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
141.212.122.129	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
50.62.177.15	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
207.241.229.224	United States	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
89.139.229.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.83.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.50.179.44		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
183.206.173.115	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/includes/fckeditor/editor/	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.66.26	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
112.209.149.103	Philippines	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
67.247.20.181	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.107.246.96	Hungary	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.24.76.132	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

03-07-2016-02:04:03 to 03-07-2016-03:04:03