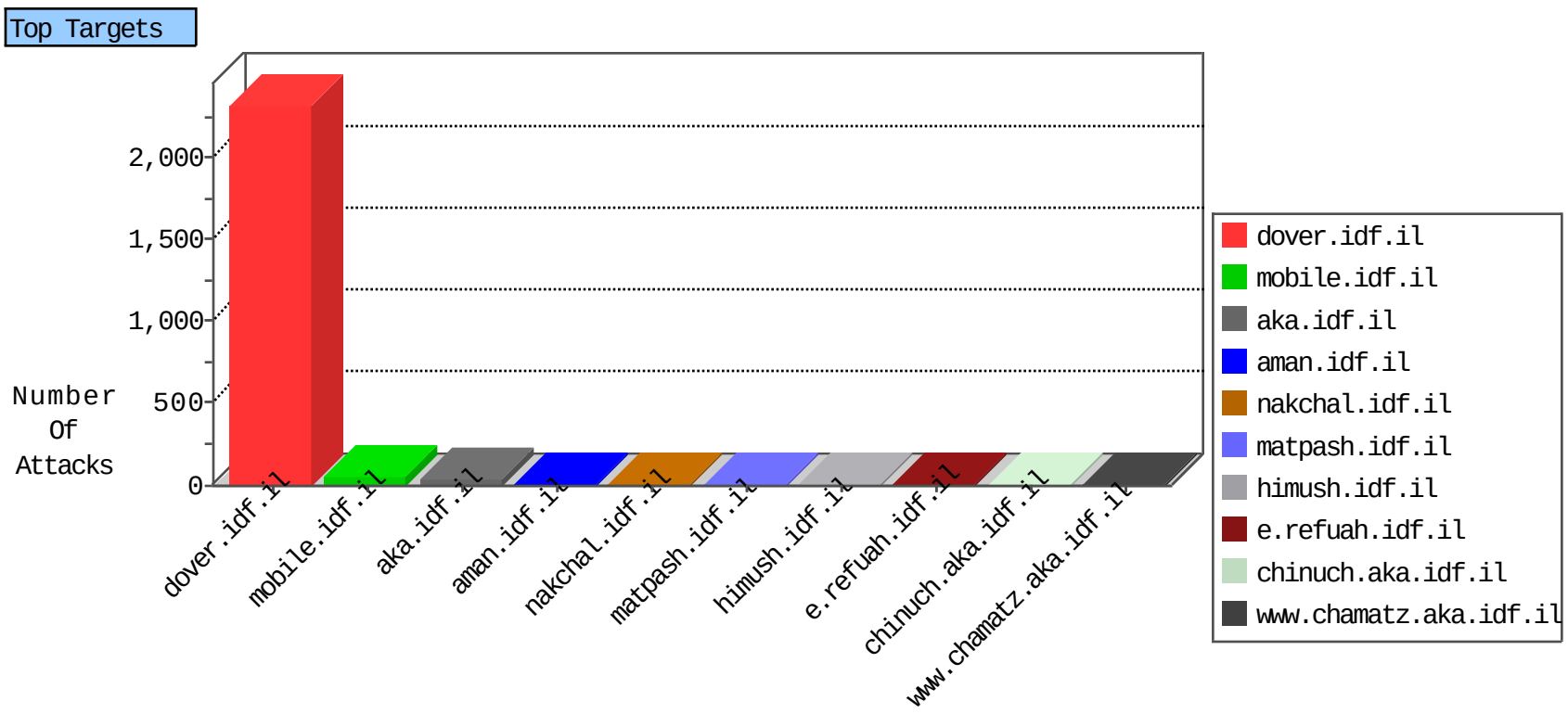
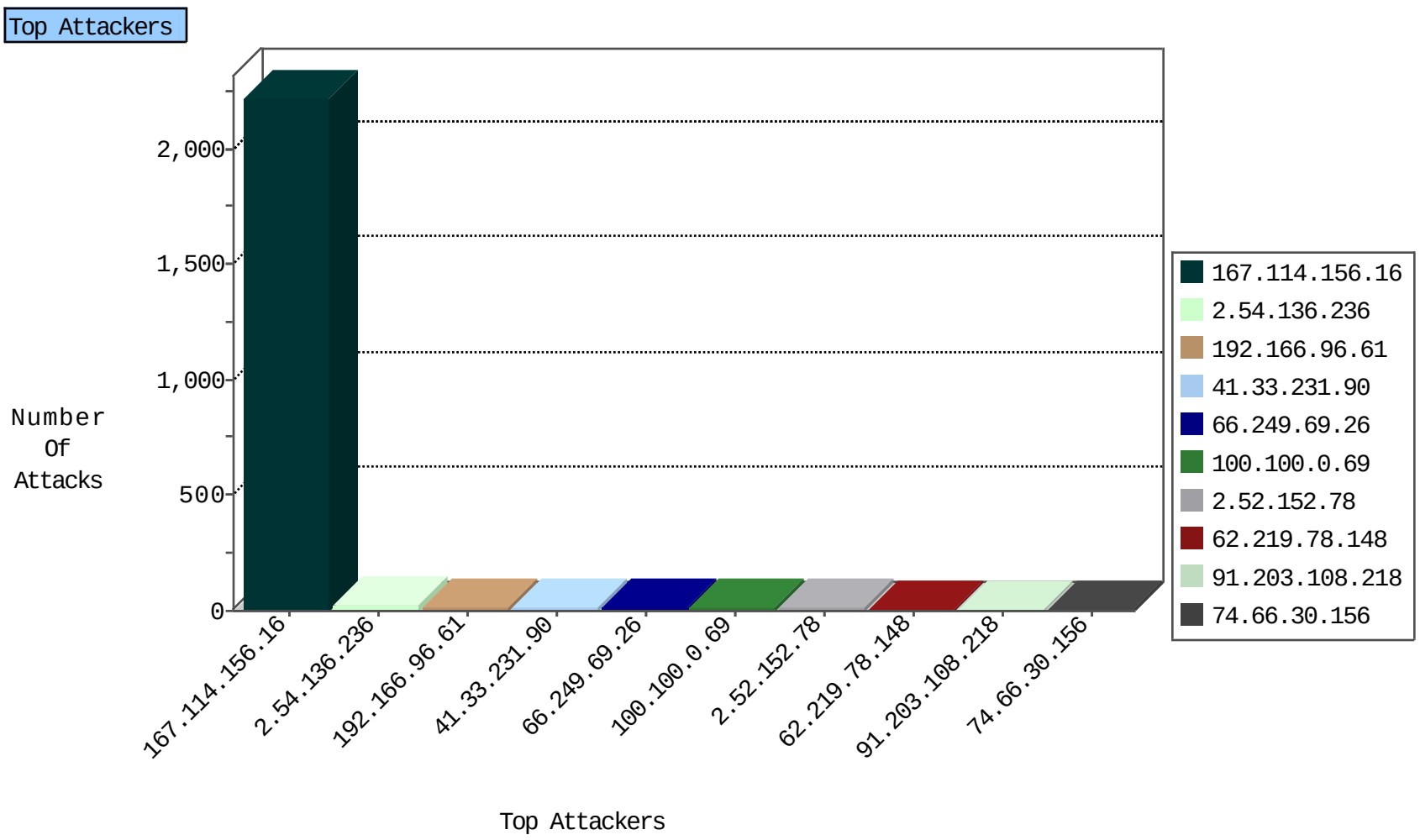
11-29-2015-04:04:00 to 11-29-2015-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-29-2015-04:04:00 to 11-29-2015-05:04:00

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	3260
166.111.105.45	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
62.165.231.216	Hungary	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
113.122.119.225	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-29-2015-04:04:00 to 11-29-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.114	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-29-2015-04:04:00 to 11-29-2015-05:04:00

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
111.93.198.54	147.237.77.235	India	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.27	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.226	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.226.212.78	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

11-29-2015-04:04:00 to 11-29-2015-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.136.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.52.152.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.12	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
74.66.30.156	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.177.48.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
213.57.215.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
23.242.15.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.246.110.40	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.79.13	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.52	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.148.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
112.74.67.109	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.193	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.149.161	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.56.80.138	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
104.192.0.226	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.60	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.94.2		147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
104.192.0.226	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.96	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.131.199.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.138.17.205	France	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.192.0.226	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.6.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.112	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.192.0.226	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.201.154.186	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
85.65.6.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.28	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.56.80.138	Netherlands	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
104.192.0.226	United States	147.237.0.33	idf.il	drop		drop	1

11-29-2015-04:04:00 to 11-29-2015-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.136.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
192.166.96.61	Netherlands	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
66.49.211.78	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
192.166.96.61	Netherlands	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.166.96.61	Block	3
62.219.78.148	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
60.241.215.85	Australia	147.237.76.30	himush.idf.il	PHP Attempt	Block	3
91.203.108.218	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
192.166.96.61	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
79.182.8.237	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
66.49.211.78	Canada	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
62.219.78.148	Israel	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
2.52.152.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.166.96.61	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
213.57.215.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.49.211.78	Canada	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.49.211.78	Block	2
176.13.10.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.203.108.218	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
192.166.96.61	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
149.88.191.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.219.78.148	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.219.78.148	Block	2
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	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
192.166.96.61	Netherlands	147.237.76.31	nakchal.idf.il	Distributed Admin Blocking	Block	2
60.241.215.85	Australia	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/index.php	Block	2
91.203.108.218	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.203.108.218	Block	2
2.52.152.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.226	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
60.241.215.85	Australia	147.237.76.30	himush.idf.il	Admin Blocking	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.196.50.33	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on testp2.czar.bielawa.pl/testproxy.php	Block	1
212.90.148.38	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.64.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
112.199.109.213	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
91.203.108.218	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.227	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
60.241.215.85	Australia	147.237.76.30	himush.idf.il	Multiple Admin Blocking from 60.241.215.85	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.196.50.33	Poland	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
112.199.109.213	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
93.172.124.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar	Block	1
207.46.13.87	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
73.191.251.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.64.207.12	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
60.241.215.85	Australia	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 60.241.215.85	Block	1
216.104.160.96	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.74.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
40.77.167.91	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-29-2015-04:04:00 to 11-29-2015-05:04:00