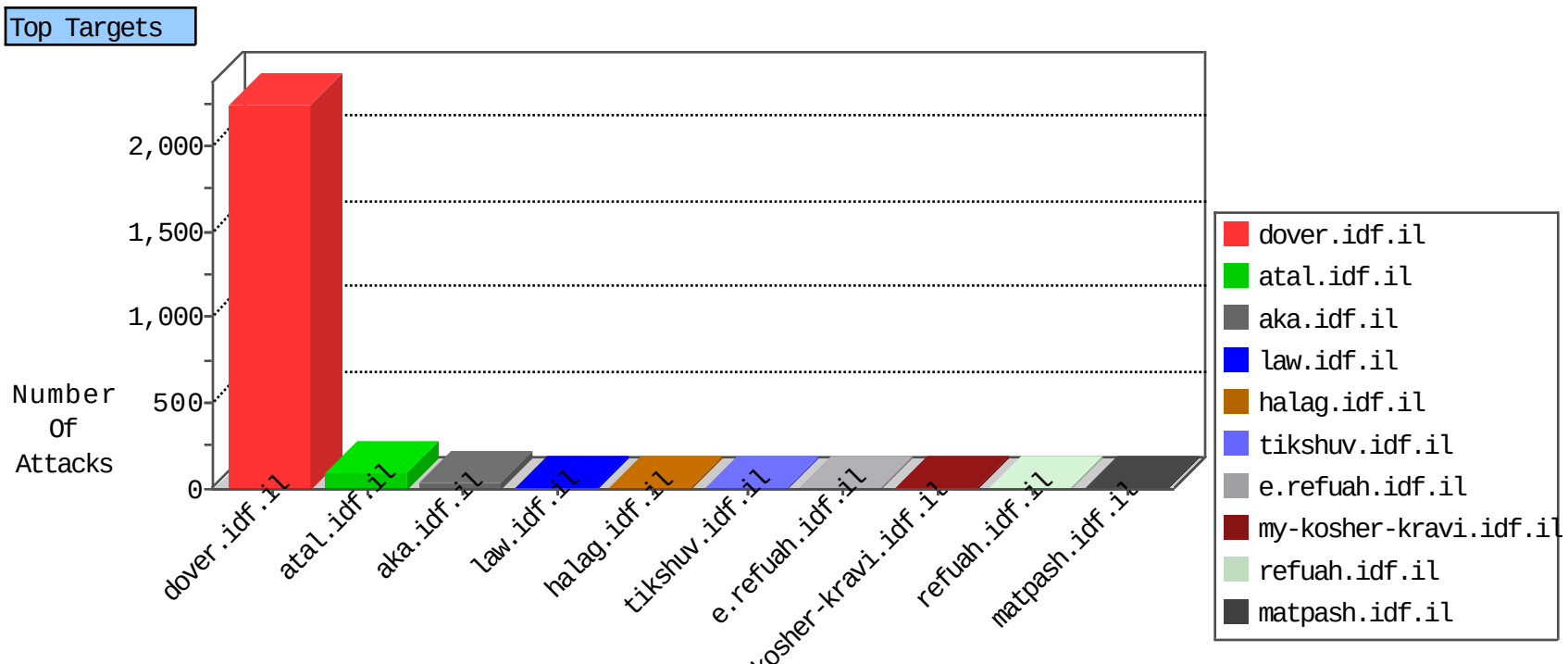
12-06-2015-04:04:04 to 12-06-2015-05:04:04

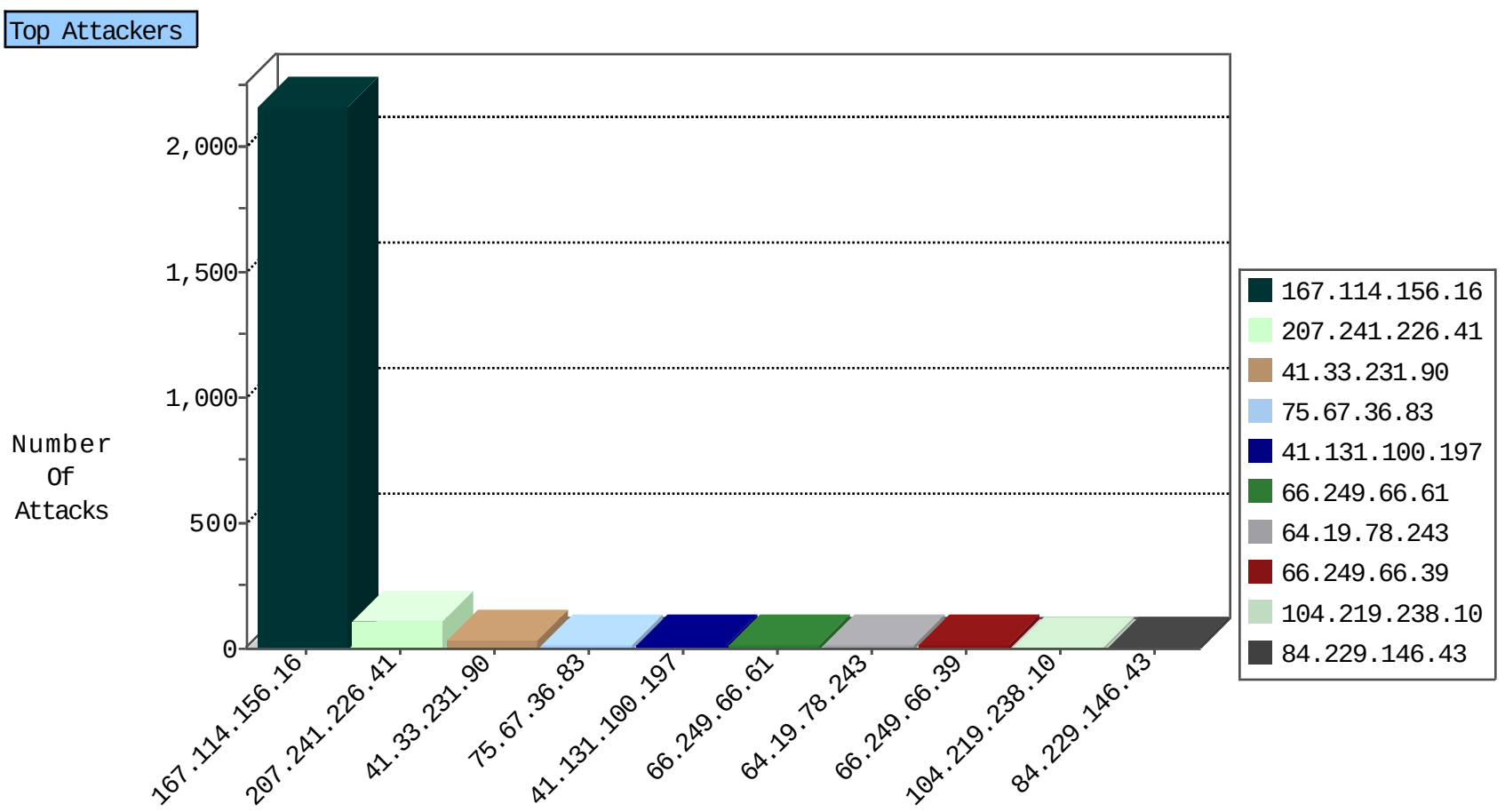
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-06-2015-04:04:04 to 12-06-2015-05:04:04

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	3491
183.4.238.105	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
183.4.238.105	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-06-2015-04:04:04 to 12-06-2015-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-06-2015-04:04:04 to 12-06-2015-05:04:04

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
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.174	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.77.243	Cote D'Ivoire	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.0.33	India	idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.0.33	India	idf.il	ET SCAN NMAP -f -sS	1
104.219.238.10	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.90.244.179	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.243	Cote D'Ivoire	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.0.33	India	idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

12-06-2015-04:04:04 to 12-06-2015-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
75.67.36.83	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.71.4.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.146.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.191.33.191	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.44.226	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
27.227.162.113	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.143.232.37	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.68.38.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.8	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.227	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.227.162.113	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.13.12.99	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.152	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.188.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.16	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.248	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.12.99	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.153	United States	147.237.0.33	idf.il	drop		drop	1
81.7.16.13	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.124	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.150	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.16	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
181.189.139.22	Guatemala	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.153	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.224	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.151	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.28	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.153	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.90.244.179	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.224	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.12.141.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.152	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.36	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.75	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-06-2015-04:04:04 to 12-06-2015-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.41	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	55
207.241.226.41	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 207.241.226.41	Block	28
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	9
210.157.22.73	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 210.157.22.73	Block	5
207.241.226.41	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	4
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	3
41.131.100.197	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	3
75.67.36.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 75.67.36.83	Block	3
207.241.226.41	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	2
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	2
207.241.226.41	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
41.131.100.197	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
176.13.4.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
75.67.36.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	2
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	2
40.77.167.8	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	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	1
76.69.6.148	Canada	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18762-he/dover.aspx	Block	1
41.131.100.197	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
159.203.78.203	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for list.ips.gov.il/	Block	1
93.103.140.121	Slovenia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	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
5.255.253.114	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
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	1
76.69.6.148	Canada	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
159.203.127.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/blog	Block	1
93.103.140.121	Slovenia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
207.241.226.41	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/a	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
61.135.190.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
5.255.253.164	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	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
78.128.92.193	Bulgaria	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
207.241.226.41	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
95.108.158.154	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69861.jpg	Block	1
37.140.141.34	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
157.55.39.204	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
210.157.22.73	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
84.52.86.5	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
178.154.243.93	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

12-06-2015-04:04:04 to 12-06-2015-05:04:04