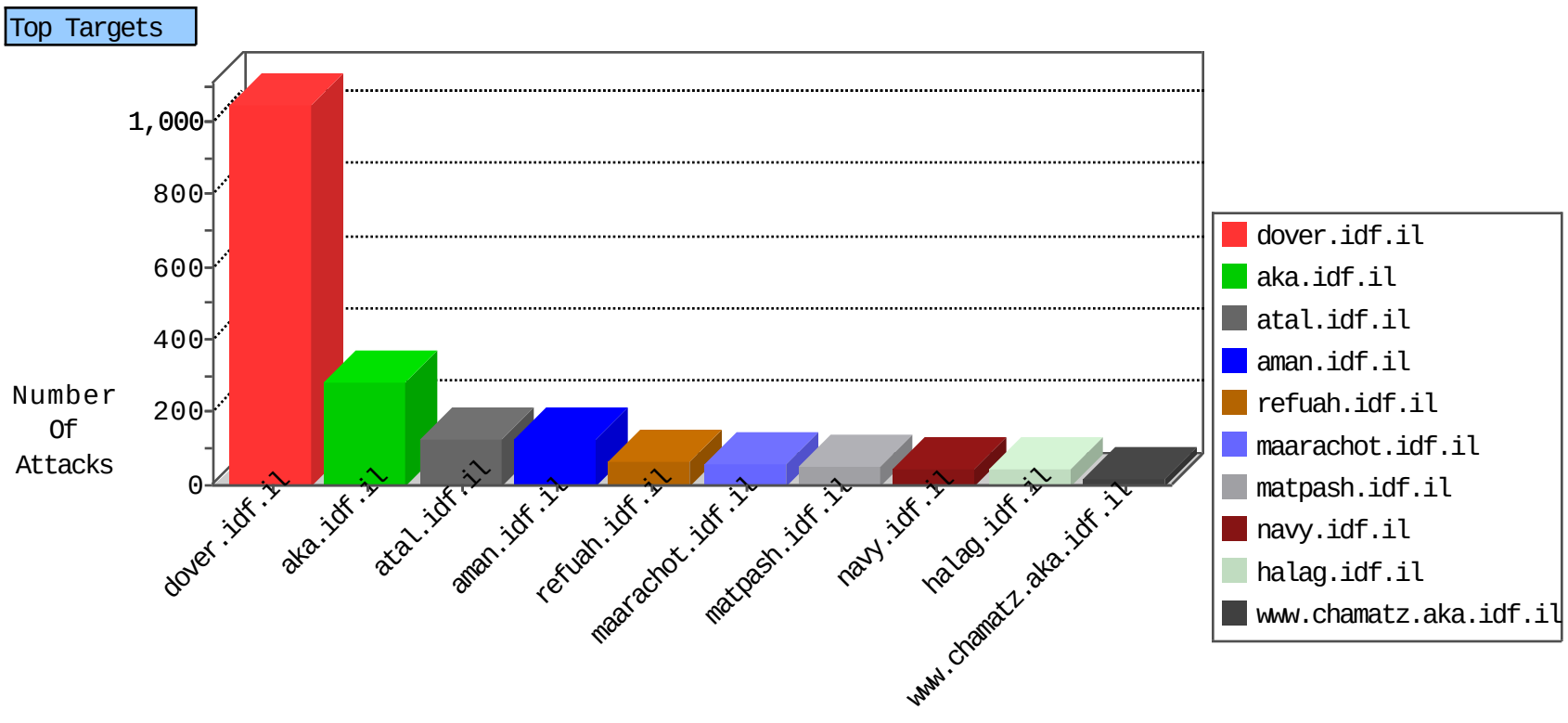
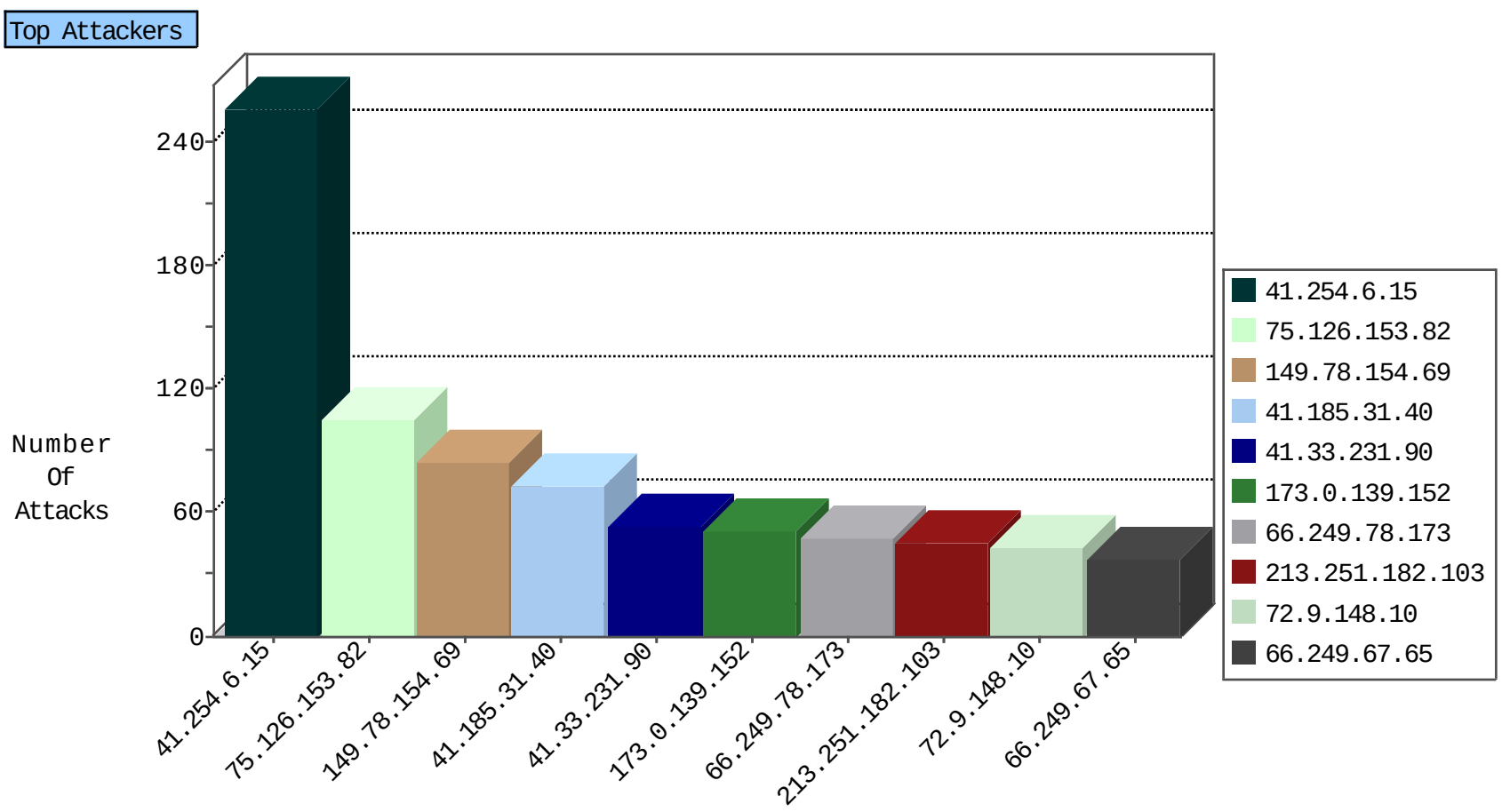
10-30-2015-05:04:04 to 10-30-2015-06:04:04

IDF Under Attack Daily Report



Top Target



Top Attackers

10-30-2015-05:04:04 to 10-30-2015-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3418
66.249.75.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	50
188.138.74.85	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
73.180.88.123	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
188.138.74.85	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
119.239.188.137	Japan	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

10-30-2015-05:04:04 to 10-30-2015-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.8.66.78	Russian Federation	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

10-30-2015-05:04:04 to 10-30-2015-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.8.66.78	147.237.77.216	Russian Federation	dover.idf.il	SERVER-WEBAPP Setup.php access	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.92	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.2	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.75.68	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
222.186.56.115	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
75.126.153.82	147.237.77.233	United States	atal.idf.il	SERVER-WEBAPP admin.php access	1
222.186.56.115	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
192.210.198.226	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
192.210.198.226	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.78	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
192.210.198.226	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
179.178.97.120	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.8.133	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.19	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.115	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.115	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
192.210.198.226	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
192.210.198.226	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
192.210.198.226	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
192.210.198.226	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
179.178.97.120	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.8.133	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

10-30-2015-05:04:04 to 10-30-2015-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.254.6.15	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	257
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
41.185.31.40	South Africa	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
162.157.170.239	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
80.74.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
185.84.70.100		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
173.0.139.152	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
63.149.187.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
220.238.32.14	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.142.248.109	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.67.13	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.54.59.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.183	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.4.10.6	Germany	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.248.109	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.232.110.28	United Kingdom	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
41.185.31.40	South Africa	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
37.26.147.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.6	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

10-30-2015-05:04:04 to 10-30-2015-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	45
75.126.153.82	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 75.126.153.82	Block	30
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
75.126.153.82	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	15
188.42.240.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/	Block	15
46.116.206.159	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	15
75.126.153.82	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
172.240.96.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	15
66.249.65.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2888.pdf	Block	15
41.185.31.40	South Africa	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
75.126.153.82	United States	147.237.77.233	atal.idf.il	Admin Blocking	Block	15
66.249.73.202	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
188.165.15.241	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	15
79.182.9.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
46.120.182.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	15
173.0.139.152	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	15
66.249.65.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2868.ppt	Block	15
41.185.31.40	South Africa	147.237.72.156	aman.idf.il	Multiple signatures from 41.185.31.40	Block	15
75.126.153.82	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 75.126.153.82	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15769-he/dover.aspx	Block	15
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.67.65	Block	15
207.46.13.95	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/Ã—â€?Ã—Â?Ã—Âª Ã—Â¨	Block	15
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	15
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2821.pdf	Block	15
173.0.139.152	United States	147.237.72.156	aman.idf.il	Multiple signatures from 173.0.139.152	Block	15
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/clientscripts.js	Block	15
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	15
108.192.112.224	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	15
59.41.177.129	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	15
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	15
66.249.69.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	15
176.13.8.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/clientscripts/jquery/jquery-ui.js	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	15
172.240.96.58	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15
59.41.177.129	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112994.pdf/	Block	15
37.142.248.109	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15

10-30-2015-05:04:04 to 10-30-2015-06:04:04