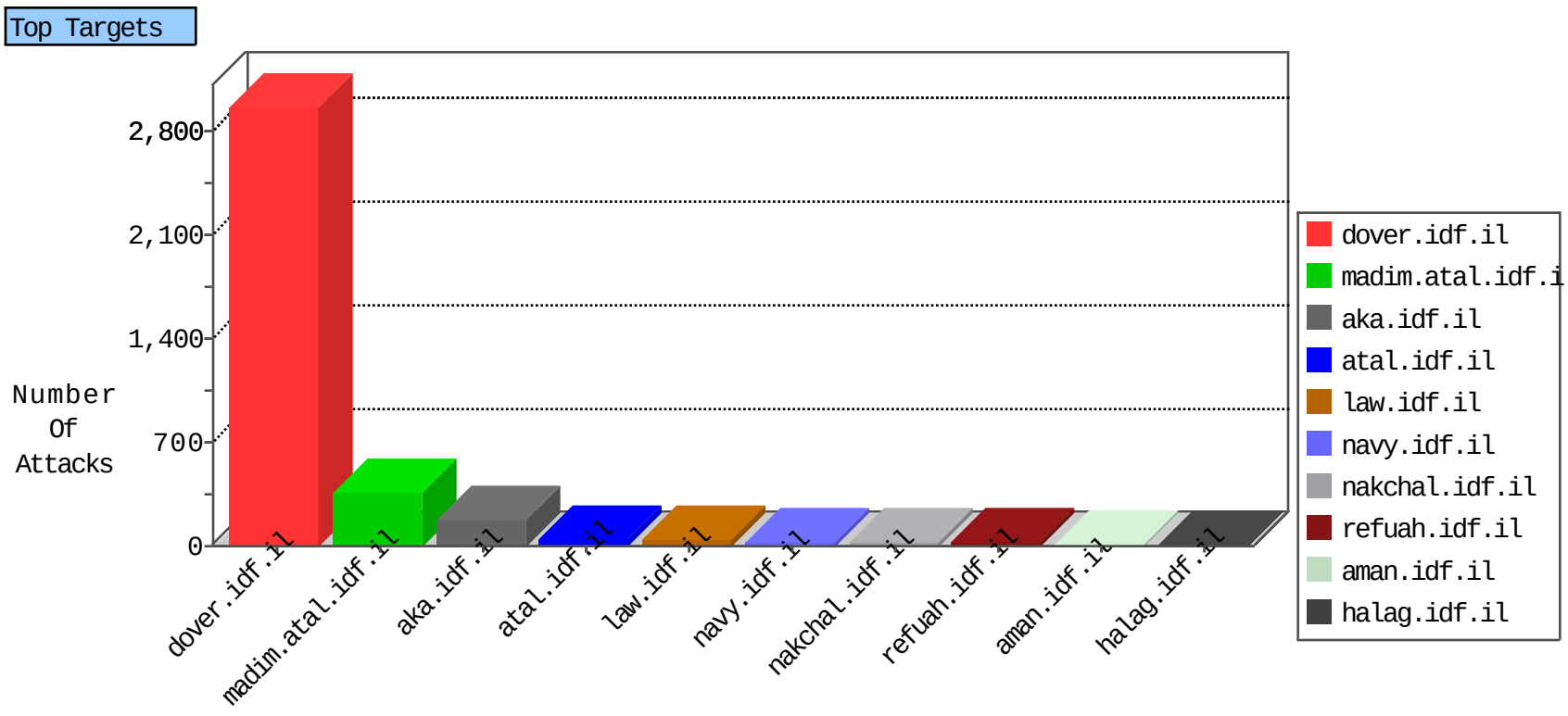
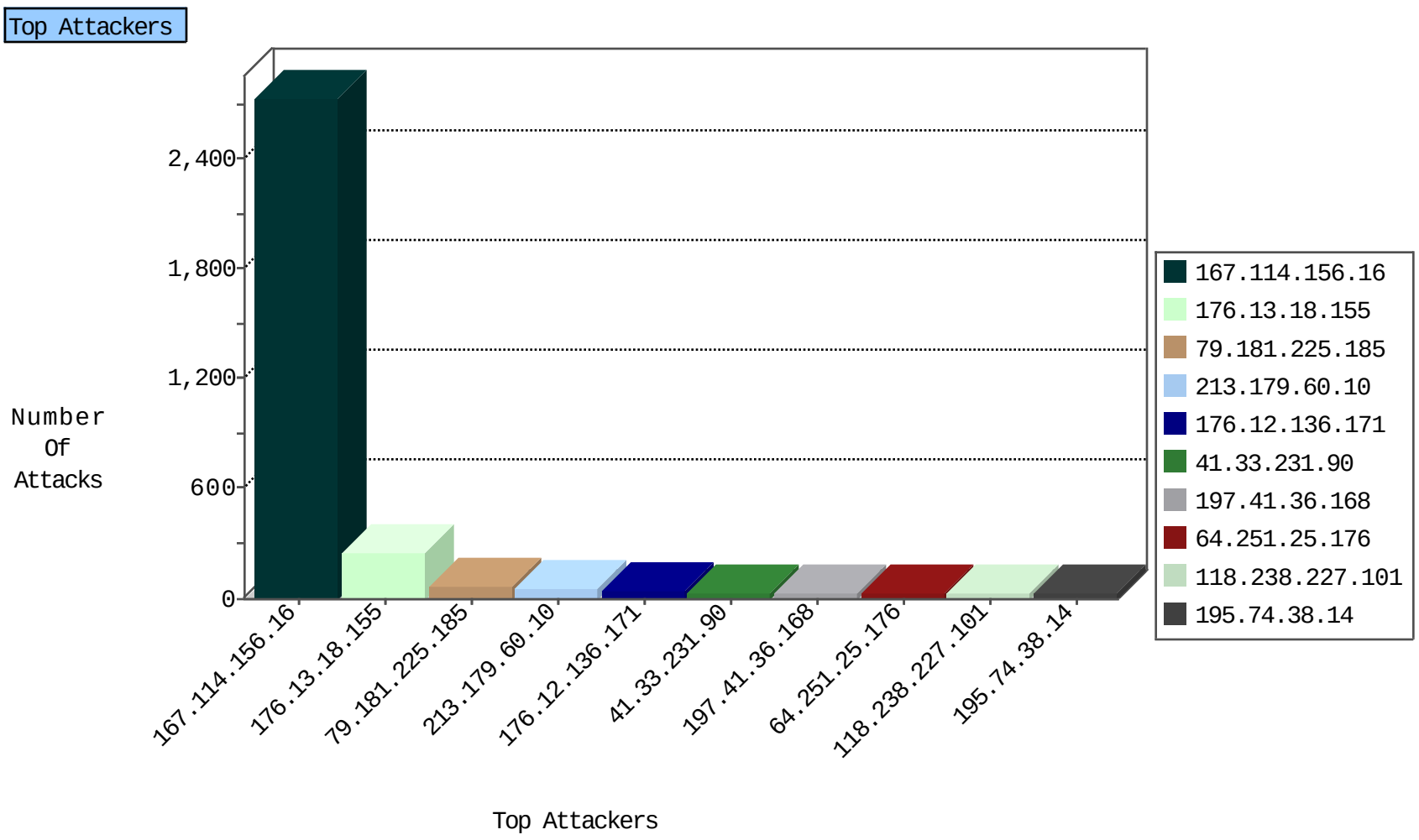
12-04-2015-18:04:04 to 12-04-2015-19:04:04

IDF Under Attack Daily Report





12-04-2015-18:04:04 to 12-04-2015-19:04:04

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	3340
123.234.227.204	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
202.112.51.96	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
51.254.212.184	United Kingdom	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
192.129.227.26	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
123.151.149.222	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
202.112.51.96	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1

12-04-2015-18:04:04 to 12-04-2015-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.59.255.19	France	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
64.251.25.176	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.135.63.82	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
161.202.41.12	Netherlands	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
161.202.41.12	Netherlands	147.237.77.234	halag.idf.il	C003: HTTP: phpMyAdmin access	Block	1
195.74.38.14	Sweden	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

12-04-2015-18:04:04 to 12-04-2015-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.179.60.10	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	42
64.251.25.176	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	24
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
37.59.255.19	147.237.77.74	France	law.idf.il	SQL Injection - Select From	10
46.118.155.187	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP Mambo upload.php access	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.74.38.14	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	3
66.249.66.16	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.8.122.170	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
113.240.250.155	147.237.8.45	China	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
222.45.224.183	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
222.45.224.183	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.45.224.183	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
222.45.224.183	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
222.45.224.183	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
222.45.224.183	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
115.47.52.157	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
222.45.224.183	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.155	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
222.45.224.183	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.45.224.183	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

12-04-2015-18:04:04 to 12-04-2015-19:04:04

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	34
176.106.227.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
118.238.227.101	Japan	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	24
195.74.38.14	Sweden	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
197.41.36.168	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	drop	SAM rule	drop	8
118.238.227.101	Japan	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
197.41.36.168	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.25	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.145.19	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
197.41.36.168	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.25	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.121.93		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.170.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.63.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.41.36.168	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.130.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
87.68.158.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
77.125.82.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.254.182	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.6.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.8.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.50.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
186.64.155.138	Costa Rica	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
73.42.171.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.1.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.43.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.36.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.207.130	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
81.218.133.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.204.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.178.163.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.29.226.56	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
100.100.15.0		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.121.192	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.81.209	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.138.236.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
213.57.130.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
2.54.168.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

12-04-2015-18:04:04 to 12-04-2015-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
176.13.18.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	117
79.181.225.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.12.136.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.118.155.187	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	9
46.118.155.187	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.187	Block	8
176.13.0.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.0.117	None	7
46.116.173.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.3.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.72.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.70.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.64.16	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
98.80.189.213	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
2.54.159.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.41.36.168	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gen_204	Block	1
79.183.151.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
69.171.230.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
98.80.189.213	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ 6Â°Ã¿â€š×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×ž Â¶[[#25]]lÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
87.68.158.221	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
37.142.118.25	Israel	147.237.72.156	aman.idf.il	Cross-site scripting on parameter ctl00$ctl00$cphMain$CPHMainContent$ctl72$ctl05$ctl03$txtField in www.aman.idf.il/modiin/questionnaires.aspx	Block	1
213.233.85.244	Romania	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.71.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.190.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.118.155.187	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/editor/filemanager/upload/php/upload.php	Block	1
98.80.189.213	United States	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.87.98	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
79.183.226.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
176.13.0.117	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
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
98.80.189.213	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Â¬[[#0]][[#0]][[#0]]BÂ¦ Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡ ^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â’ Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
89.138.194.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.144.69	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.1.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.66.236.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
61.135.190.71	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
98.80.189.213	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]BÂ¦ Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡ ^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â’ Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
5.29.180.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.136.139	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.125.145.19	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
98.80.189.213	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]BÂ¦ Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡ ^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â’ Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
2.54.34.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-04-2015-18:04:04 to 12-04-2015-19:04:04