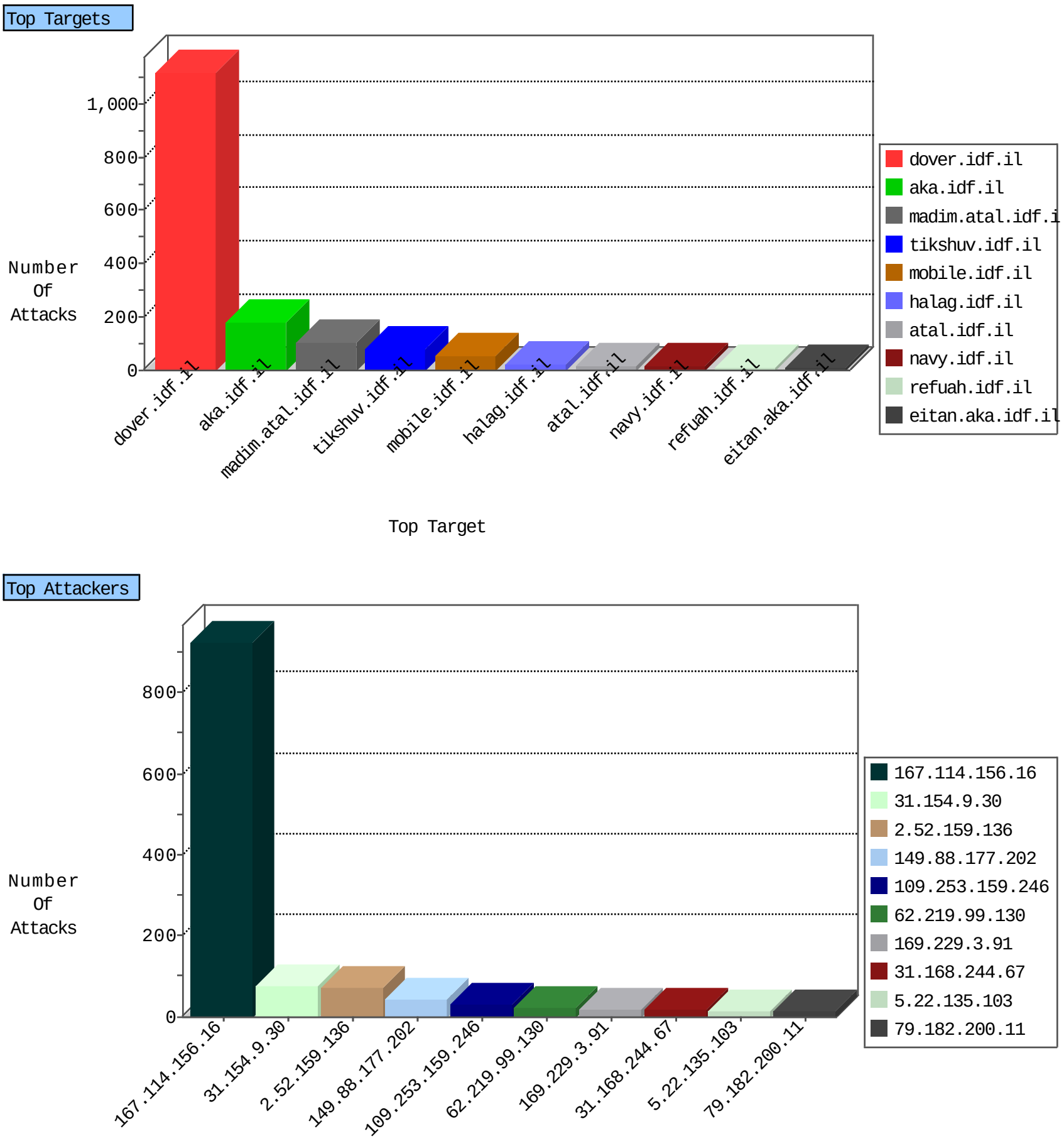
03-11-2016-11:04:03 to 03-11-2016-12:04:03

IDF Under Attack Daily Report



03-11-2016-11:04:03 to 03-11-2016-12:04:03

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	3779
82.145.222.28	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
212.88.63.206	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.206	Netherlands	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.251	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.211	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

03-11-2016-11:04:03 to 03-11-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.38.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
89.139.183.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.215.118	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.118	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.79.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-11-2016-11:04:03 to 03-11-2016-12:04:03

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
193.105.134.220	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.243	Austria	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
178.63.11.208	147.237.76.34	Germany	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1

03-11-2016-11:04:03 to 03-11-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.9.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.182.200.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.219.99.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.22.135.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack		reject	9
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
31.168.244.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.168.244.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.250.128.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.154.9.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.154.9.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.72	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.9.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.22.135.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.9.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.137.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.159.136	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
58.34.131.80	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.159.136	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
95.86.66.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.244.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
85.130.244.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.141	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
85.130.244.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.94.75.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.159.136	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.51	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.215.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.7	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.5.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.16.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.12.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.159.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.184.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.189.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-11-2016-11:04:03 to 03-11-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.177.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
109.253.159.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
212.76.123.50	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 212.76.123.50	Block	6
87.69.192.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.76.123.50	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.232.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.99.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
89.139.184.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.150.69	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.99.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
2.54.9.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
58.34.131.80	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method [[#11]]uCÃÃqœ[[#0]]°³•§ôŠ¼<[[#26]]B¶½'7´LHwìd¢‹Ýzê††[[#23]]§O[[#27]][[#27]]«£2	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
212.179.80.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 212.179.80.54	Block	1
178.152.72.85	Qatar	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/70005.doc	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method 5Ôˆ M[[#15]]-s/#012ÄÚúÊ+w²“ÎJè]ò[[#8]]ã#¦±¾Û-rU¨[[#17]]›j[[#0]]gSä %B^®˜+¢	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
176.13.7.144	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
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	NULL Character in Method [[#11]]uCÃÃqœ[[#0]]°³•§ôŠ¼<[[#26]]B¶½'7´LHwìd¢‹Ýzê††[[#23]]§O[[#27]][[#27]]«£2	Block	1
31.168.244.67	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.204.13	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
87.69.222.24	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
178.152.72.85	Qatar	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in URL	Block	1
2.52.150.69	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.150.69	Block	1
176.13.7.144	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.7.144	None	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Unknown HTTP Request Method [[#11]]uCÃÃqœ[[#0]]°³•§ôŠ¼<[[#26]]B¶½'7´LHwìd¢‹Ýzê††[[#23]]§O[[#27]][[#27]]«£2 in URL	Block	1
37.26.146.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.253.180.221	Australia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
181.16.17.57	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method 5Ôˆ M[[#15]]-s/#012ÄÚúÊ+w²“ÎJè]ò[[#8]]ã#¦±¾Û-rU¨[[#17]]›j[[#0]]gSä %B^®˜+¢	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.94.203.12	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
212.76.123.50	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
176.13.9.177	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Abnormally Long Request	Block	1
37.26.146.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.223.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
46.117.109.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1

03-11-2016-11:04:03 to 03-11-2016-12:04:03