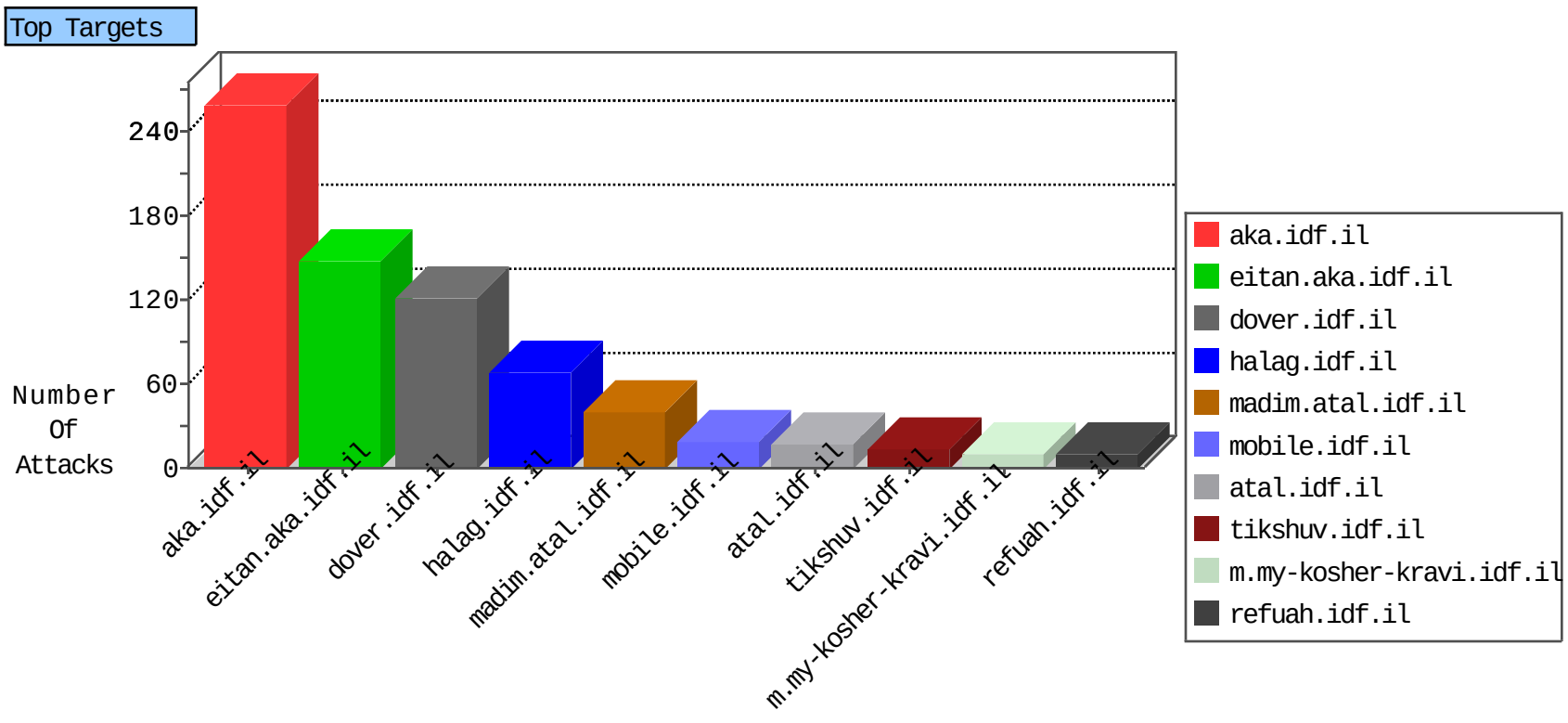
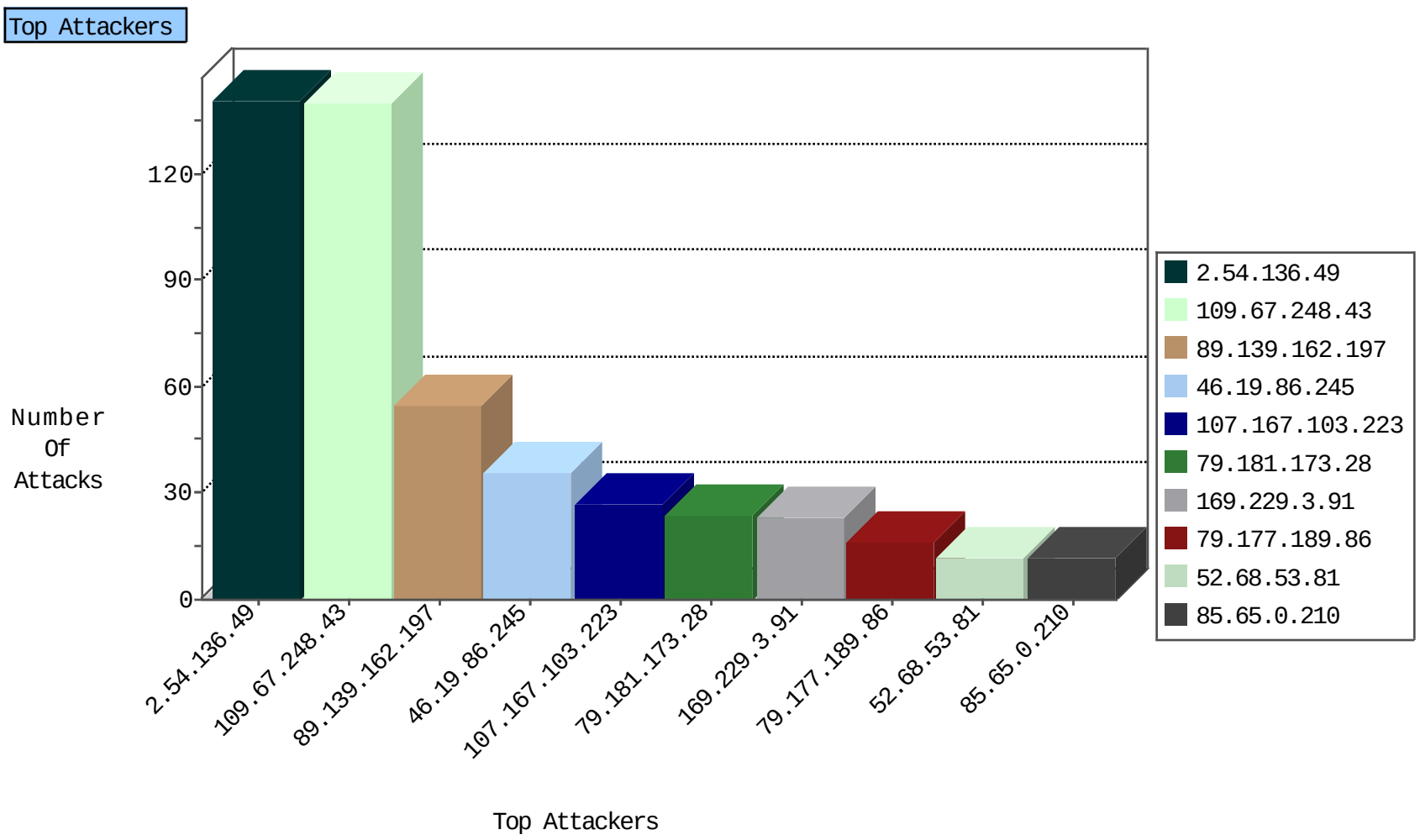
03-05-2016-12:04:05 to 03-05-2016-13:04:05

IDF Under Attack Daily Report





03-05-2016-12:04:05 to 03-05-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	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	1

03-05-2016-12:04:05 to 03-05-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
79.179.221.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.68.249.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.247	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.149	Italy	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
31.154.249.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-05-2016-12:04:05 to 03-05-2016-13:04:05

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
104.128.144.131	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.72.217	Switzerland	e.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

03-05-2016-12:04:05 to 03-05-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.136.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
89.139.162.197	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
109.67.248.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
109.67.248.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
107.167.103.223	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	20
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
85.65.0.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.177.189.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
149.78.156.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.22.135.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.135.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.172.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.41.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.115.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.5.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.32.179.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.189.86	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.65.147.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.96	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.3	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
52.68.53.81	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	5
37.46.38.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.138.97.231	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
103.244.13.108	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.117.62.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
52.68.53.81	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.32.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.153.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.64.175.89	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.135.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.14.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.159.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.1.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.102.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.64.175.89	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.100.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.2.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.201.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.0.84.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-05-2016-12:04:05 to 03-05-2016-13:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.166.102.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.3.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.189.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.22.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.99.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/109290.pdf	Block	2
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	2
95.185.201.50	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
82.102.221.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/php	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in URL /•b[[#11]]8d¸%	Block	1
46.120.145.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in URL ••)>iÙıı3€«ßiÿ¦Œ″¸6˙žß-^ j[[#1]]Þaʊ¦	Block	1
87.70.68.166	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
173.247.228.10	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
5.164.192.16	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method f.ž³ÑžÞ«ˆ•	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.240.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal URL Path Encoding /•b[[#11]]8d¸%	Block	1
62.84.70.202	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Malformed URL ••)>iÙıı3€«ßiÿ¦Œ″]]1#[[j¸6˙žß-^ Þaʊ¦	Block	1
89.137.180.5	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
173.247.228.10	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
31.168.16.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL	Block	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″ ×•×ª×¨	Block	1
85.65.0.210	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.241.237.223	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteyerua	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
89.138.97.231	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.176.115.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.161 (Open Mode)	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method f.ž³ÑžÞ«ˆ• in URL	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
213.204.93.10	Lebanon	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.250.92.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14880-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
89.139.162.197	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.189.86	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
185.32.179.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Query String on /•b[[#11]]8d¸%	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
213.204.93.32	Lebanon	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
86.62.174.218	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method [[#31]]"Ü'Tš"[[#18]]†{œêàÝ#mçlå¶°[[#30]]¡$ÓŒ in URL /•b[[#11]]8d¸%	Block	1
66.249.66.188	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Unknown HTTP Request Method [[#20]][[#16]]HÈò¥…žÿ¿#[[#31]]ëï·7″?bÂqö*°ãâ\[[#19]]«Â,´ in URL ••)>iÙıı3€«ßiÿ¦Œ″]]1#[[j¸6˙žß-^ Þaʊ¦	Block	1